The Habiro ring

Jesper de Groot
Student number: 3796582
Utrecht University

June 25, 2014

Contents

1 Introduction **2**
1.1 Structure 2

2 Cyclotomic polynomials **3**
2.1 Elementary properties 3
2.2 Expressions 5
2.3 Cyclotomic polynomials modulo p 6
2.4 Irreducibility 7
2.5 Minimal polynomials of roots of unity 9

3 Quotients of $\mathbb{Z}[q]$ **11**
3.1 Properties of $\mathbb{Z}[q]/(\Phi_n(q)^j)$ 11
3.2 Properties of $\mathbb{Z}[q]/(Q_n(q))$ 13
3.3 Finite Habiro expansions in $\mathbb{Z}[q]/(Q_n(q))$ 15

4 Projective limits **17**
4.1 Formal definitions 17
4.2 Two examples 18
4.3 Constructing the Habiro ring 20
4.4 A mapping from $\mathbb{Z}[q]$ to $\widehat{\mathbb{Z}[q]}$ 24
4.5 A mapping from $\widehat{\mathbb{Z}[q]}$ to $\mathbb{Z}[q]^{\{n\}}$ 26

5 Unique identification with values at the roots of unity **28**
5.1 Injectivity of σ_T 29
5.2 Injectivity of γ_Z 30

1 Introduction

The Habiro ring $\widehat{\mathbb{Z}[q]}$ is named after Kazuo Habiro, a Japanese mathematician from the Kyoto University. In his article 'Cyclotomic Completions of Polynomial Rings' he describes the ring as follows [1]

> The completion $\widehat{\mathbb{Z}[q]} = \lim_{\infty \leftarrow n} \mathbb{Z}[q]/((1-q)(1-q^2)\cdots(1-q^n))$ can be regarded as a 'ring of analytic functions'. This means that an element of $\widehat{\mathbb{Z}[q]}$ vanishes if it vanishes on a certain type of infinite set of roots of unity.

Unless you are an expert on mathematics, you will not directly understand what the Habiro ring is. I would describe the Habiro ring as some kind of extension of $\mathbb{Z}[q]$, the ring of polynomials with integer coefficients over a variable q. $\mathbb{Z}[q]$ only contains elements of the form $a_0 + a_1 q + ... + a_n q^n$, where n is finite. As we will see, the Habiro ring contains certain infinite sums, of the form $a_0 + a_1 q + ...$, with the condition that this sum has a well defined value at the roots of unity. Certainly all elements of $\mathbb{Z}[q]$ are elements of the Habiro ring, since finite sums can be extended to infinite sums by adding infinitely many times 0. The Habiro ring appears to be the so called projective limit of a system of quotient rings $\mathbb{Z}[q]/(Q_n(q))$.
Not much research has been done on the Habiro ring, but it shows up in a few parts of ring theory, such as the study of $\mathbb{F}_1$-geometry, which is about the properties of the so called 'field with one element'. Yu.I. Manin and M. Marcolli contributed much to the knowledge on the Habiro ring, researching this 'field with one element'. Via the so called Witten-Reshetikhin-Turaev invariants, researched by Habiro, there is a surprising link with knot theory. Both topics are beyond the scope of this thesis.

1.1 Structure

We will start to say something about cyclotomic polynomials. They turn out to be important for introducing the Habiro ring. Then we take a look at quotient rings of $\mathbb{Z}[q]$ and (products of) cyclotomic polynomials, also introducing $\mathbb{Z}[q]/(Q_n(q))$. The next section will be devoted to the introduction of the projective limit and the definition of the Habiro ring via this projective limit. It will turn out that we can write each element of the Habiro ring in a unique way as a certain infinite sum, called the Habiro expansion. Finally we will show that an element of the Habiro ring is uniquely determined by its values on (a certain group of) roots of unity.
In most of this thesis we will use integers, and therefore $n \geq 0$ means $n \in \mathbb{Z}$ with $n \geq 0$, unless otherwise specified. We will also use the convention that 0 is not a positive integer, which means that $\mathbb{N} = \{1, 2, 3, ...\}$. The notation $\mathbb{N}_0$ will be used for $\mathbb{N} \cup \{0\}$.

2 Cyclotomic polynomials

2.1 Elementary properties

First I will present some elementary properties of so called cyclotomic polynomials. We will need some of these properties in the next sections. Before we can define the notion of a cyclotomic polynomial, we first need a few definitions and two lemmas.

Definition 2.1. *Let $n \in \mathbb{N}$ and $\zeta \in \mathbb{C}$. If $\zeta^n = 1$ we call ζ an nth root of unity. The smallest $d \in \mathbb{N}$ such that $\zeta^d = 1$ is called the order of ζ and denoted by $ord(\zeta)$. If $ord(\zeta) = n$, ζ is called a primitive nth root of unity.*

Lemma 2.2. *Let $n, k \in \mathbb{N}$ and ζ a nth root of unity. Then $ord(\zeta) \mid k$ if and only if $\zeta^k = 1$. We also have $ord(\zeta) \mid n$.*

Proof. If $ord(\zeta) \mid k$, then obviously we have $\zeta^k = 1$. Moreover, suppose that $\zeta^k = 1$ and $ord(\zeta) \nmid k$. Then $k = p\ ord(\zeta) + q$ for some $p \in \mathbb{N}_0$ and $0 < q < ord(\zeta)$. This results in $\zeta^q = \zeta^k \zeta^{-p\ ord(\zeta)} = 1$, so $ord(\zeta) \leq q$. This is a contradiction and therefore: $ord(\zeta) \mid k$. We now also have $ord(\zeta) \mid n$. □

Lemma 2.3. *Let $n, k \in \mathbb{N}$ and ζ a primitive nth root of unity. Then $gcd(k, n) = 1$ if and only if ζ^k is a primitive nth root of unity.*

Proof. Define $d = ord(\zeta^k)$, then $\zeta^{kd} = 1$. Therefore, by Lemma 2.2 we have $n = ord(\zeta) \mid kd$. If $gcd(k, n) = 1$ we obviously have $n \mid d$. Since ζ^k is also an nth root of unity ($\zeta^{kn} = 1$) we have by the same lemma $d \mid n$. This results in $d = n$ and ζ^k is primitive. If $gcd(k, n) \neq 1$, then let $g = gcd(k, n)$. Then $\zeta^{\frac{kn}{g}} = 1$ and therefore $d = \frac{n}{g} < n$, so ζ^k is not primitive. □

We know that there are n unique nth roots of unity, namely $e^{\frac{2\pi i}{n}}, e^{\frac{4\pi i}{n}}, \ldots, e^{\frac{2n\pi i}{n}}$. For fixed $n \in \mathbb{N}$ we define $\zeta^k = e^{\frac{2k\pi i}{n}}$ for $1 \leq k \leq n$. Since there are by definition $\phi(n)$ numbers satisfying $0 \leq k \leq n-1$ with $gcd(k, n) = 1$ we obtain

Corollary 2.4. *Let $n \in \mathbb{N}$. Then there are $\phi(n)$ primitive nth roots of unity.*

Now we are ready to define the notion of a cyclotomic polynomial.

Definition 2.5. *Let $n \in \mathbb{N}$. Then the nth cyclotomic polynomial Φ_n is defined as the monic polynomial with only the primitive nth roots of unity as its roots, that is*

$$\Phi_n(q) = \prod_{k:ord(\zeta^k)=n} (q - \zeta^k) \tag{2.1}$$

By Corollary 2.4 we see that the nth cyclotomic polynomial has degree $\phi(n)$. From our knowledge of $\mathbb{Z}/n\mathbb{Z}$, we see that if $gcd(k, n) = 1$ then $gcd(n-k, n) = 1$ for $1 \leq k \leq n-1$. Therefore $(q - \zeta^k)(q - \zeta^{n-k}) = q^2 + \zeta^n - q(\zeta^k + \overline{\zeta^k}) = q^2 + 1 - 2Re(\zeta^k)q$. Since this product is real we see that $\Phi_n(q)$ is monic and has real coefficients. We can in fact prove that these coefficients are integers. To do this, we first need to prove the following lemma.

Lemma 2.6. *Let $n \in \mathbb{N}$. Then*

$$q^n - 1 = \prod_{d \mid n} \Phi_d(q) \tag{2.2}$$

Proof. The roots of $q^n - 1$ are by definition exactly the nth roots of unity. Take one root of $q^n - 1$ and call it ζ. Let $d = ord(\zeta)$, then ζ is a primitive dth root of unity and a root of $\Phi_d(q)$. Since $d \mid n$ by Lemma 2.2, ζ is a root of the right hand side.
Furthermore, if we take one root of the right hand side and call it again ζ with $d = ord(\zeta)$, then $\zeta^n = \zeta^{d\frac{n}{d}} = 1$. Thus follows that ζ is a nth root of unity. Since both polynomials are monic and have the same roots, they are equal. □

Example 2.1. We can easily check Lemma 2.6 for $n = 4$. We have $\Phi_1(q) = q - 1$,$\Phi_2(q) = q + 1$ and $\Phi_4(q) = (q + i)(q - i) = q^2 + 1$. Thus follows

$$\Phi_1(q)\Phi_2(q)\Phi_4(q) = (q-1)(q+1)(q^2+1) = (q^2-1)(q^2+1) = q^4 - 1 \tag{2.3}$$

We will use the lemma to prove the next theorem.

Theorem 2.7. *Let $n \in \mathbb{N}$, then the nth cyclotomic polynomial has integer coefficients, that is $\Phi_n \in \mathbb{Z}[q]$. If $n = 1$ the constant term of Φ_n is equal to -1, if $n \geq 2$ the constant term is equal to 1.*

Proof. We will use induction on n. By definition we have $\Phi_1(q) = q - 1 \in \mathbb{Z}[q]$ and $\Phi_2(q) = q + 1 \in \mathbb{Z}[q]$, so the theorem is true for $n = 1, 2$. Now fix $n \geq 3$ and assume that the theorem is satisfied for all $k \mid n$ with $k \neq n$. Denote $m = \phi(n) < n$ then we can express $\Phi_n(q) = q^m + a_{m-1}q^{m-1} + ... + a_1 q + a_0$. By Lemma 2.6, we have

$$q^n - 1 = \Phi_n(q) \prod_{d|n, d\neq n} \Phi_d(q) \tag{2.4}$$

Therefore we can write $\prod_{d|n,d\neq n} \Phi_d(q) = q^{n-m} + b_{n-m-1}q^{n-m-1} + ... + b_1 q + b_0$. This polynomial is a finite product of elements of $\mathbb{Z}[q]$ and therefore also an element of $\mathbb{Z}[q]$, so the coefficients are integers. If we expand Equation 2.4, we get

$$q^n - 1 = q^n + (a_{m-1} + b_{n-m-1})q^{n-1} + ... + (a_1 b_0 + a_0 b_1)q^1 + a_0 b_0 \tag{2.5}$$

Since the constant term on the left side of Equation 2.5 is equal to -1, we should also have $a_0 b_0 = -1$. We know that b_0 is equal to the product of the constant terms of all Φ_d with $d \mid n, d \neq n$. By our induction hypothesis we have that the constant term of Φ_d is equal to -1 if $d = 1$ and equal to 1 if $d \neq 1$. Since $1 \neq n$ we have $b_0 = -1$. Therefore $a_0 = 1$, and the last part of the theorem is proven. We also obtain from Equation 2.5 $a_1 b_0 + a_0 b_1 = 0$, since the coefficient of q^1 is equal to 0 on the left side and $b_0 = -1$. Thus $a_1 = a_0 b_1 = -b_1 \in \mathbb{Z}$. If we define $b_j = 0$ for $j > n - m$, we can go on similarly for $a_2, a_3, ..., a_m$. For $2 \leq k \leq m$ we obtain from Equation 2.5

$$a_k b_0 + a_{k-1} b_1 + ... + a_1 b_{k-1} + a_0 b_k = 0 \tag{2.6}$$

This is because $k \leq m < n$. Since $b_0 = -1$ and $a_j \in \mathbb{Z}$ for $0 \leq j \leq k - 1$, we obtain $a_k = a_{k-1}b_1 + ... + a_1 b_{k-1} + a_0 b_k \in \mathbb{Z}$. Thus all coefficients of Φ_n are integers. Therefore the theorem is proven. □

Lemma 2.6 also gives us another way to express the nth cyclotomic polynomial

$$\Phi_n(q) = \frac{q^n - 1}{\prod_{d|n,d\neq n} \Phi_d(q)} \tag{2.7}$$

We will now discuss a final result of Lemma 2.6. Define for $n \geq 0$ the polynomial Q_n by

$$Q_0(q) = 1 \tag{2.8}$$

$$Q_n(q) = \prod_{j=1}^{n}(1-q^j) = (-1)^n \prod_{j=1}^{n}(q^j - 1) \qquad \text{if } n \geq 1 \tag{2.9}$$

If we fix $1 \leq d \leq n$, we obtain from Equation 2.2 that Φ_d divides $q^k - 1$ exactly once if and only if $d \mid k$, that is if $k = d, 2d, ..., \lfloor \frac{n}{d} \rfloor d, (\lfloor \frac{n}{d} \rfloor + 1)d, ...$ There are exactly $\lfloor \frac{n}{d} \rfloor$ such values of k, such that $q^k - 1$ appears in the product in Equation 2.9. Therefore $\Phi_d(q)^{\lfloor \frac{n}{d} \rfloor}$ is the highest power of Φ_d dividing Q_n. Since the only factors of $q^k - 1$ are cyclotomic polynomials, the next corollary follows.

Corollary 2.8. *Let $n \in \mathbb{N}$. Then we have*

$$Q_n(q) = (-1)^n \prod_{j=1}^{n} \Phi_j(q)^{\lfloor \frac{n}{j} \rfloor} \tag{2.10}$$

2.2 Expressions

We will now derive some explicit expressions for cyclotomic polynomials. The first ones are very obvious using Definition 2.5 or Equation 2.7.

$$\Phi_1(q) = q - 1 \tag{2.11}$$

$$\Phi_2(q) = q + 1 \tag{2.12}$$

$$\Phi_3(q) = q^2 + q + 1 \tag{2.13}$$

$$\Phi_4(q) = q^2 + 1 \tag{2.14}$$

Using Equation 2.7 we can express more cyclotomic polynomials explicitly. First take $n = p$ a prime. Then we have by this equation and the geometric series

$$\Phi_n(q) = \frac{q^n - 1}{q - 1} = 1 + q + ... + q^{n-1} = \sum_{i=0}^{n-1} q^i \tag{2.15}$$

Also, if $n = 2p$ with p an odd prime, we have

$$\begin{aligned} \Phi_n(q) &= \frac{q^n - 1}{\prod_{d|n, d \neq n} \Phi_d(q)} = \frac{q^{2p} - 1}{\Phi_1(q)\Phi_p(q)\Phi_2(q)} = \frac{q^{2p} - 1}{(q^p - 1)(q + 1)} \\ &= \frac{q^p + 1}{q + 1} = \frac{(-q)^p - 1}{-q - 1} = \sum_{i=0}^{p-1} (-q)^i \end{aligned} \tag{2.16}$$

Our next result will turn out to be very useful in the next sections.

Lemma 2.9. *Let p be a prime and $k \in \mathbb{N}$. Then we have for $n = p^k$*

$$\Phi_n(q) = 1 + q^{p^{k-1}} + q^{2p^{k-1}} + ... + q^{(p-1)p^{k-1}} = \sum_{i=0}^{p-1} q^{ip^{k-1}} \tag{2.17}$$

Proof. Again, by Equation 2.7 and the geometric series, we have

$$\begin{aligned}\Phi_{p^k}(q) &= \frac{q^{p^k}-1}{\prod_{d|p^k, d\neq p^k}\Phi_d(q)} = \frac{q^{p^k}-1}{\prod_{d|p^{k-1}}\Phi_d(q)} = \frac{q^{p^k}-1}{q^{p^{k-1}}-1} \\ &= \frac{(q^{p^{k-1}})^p-1}{q^{p^{k-1}}-1} = \sum_{i=0}^{p-1} q^{ip^{k-1}}\end{aligned}$$

□

2.3 Cyclotomic polynomials modulo p

Since $p \nmid j!$ for $1 \leq j \leq p-1$ and $j!\binom{p}{j} = p(p-1)\cdots(p-j+1)$ we have $p \mid \binom{p}{j}$ by the fact that $p \mid p(p-1)\cdots(p-j+1)$ and p is a prime. Therefore we have

$$\binom{p}{0} = 1 \qquad \equiv 1 \pmod{p} \tag{2.18}$$

$$\binom{p}{j} = p\frac{(p-1)\cdots(p-j+1)}{j(j-1)\cdots 1} \qquad \equiv 0 \pmod{p} \qquad \text{if } 1 \leq j \leq p-1 \tag{2.19}$$

$$\binom{p}{p} = 1 \qquad \equiv 1 \pmod{p} \tag{2.20}$$

By the binomial theorem we have

$$(q-1)^p = \sum_{j=0}^{p}\binom{p}{j}(-1)^j q^{p-j} \equiv q^p + (-1)^p \pmod{p} \tag{2.21}$$

If we take $p = 2$, we also see $(q-1)^2 \equiv q^2+1 \equiv q^2-1 \pmod 2$. Therefore we have for all primes p

$$(q-1)^{p-1} = \frac{(q-1)^p}{q-1} \equiv \frac{q^p-1}{q-1} = \sum_{j=0}^{p-1} q^j = \Phi_p(q) \pmod{p} \tag{2.22}$$

Now take $k \in \mathbb{N}$ and p a prime, and consider the prime power p^k. Repeatedly using Equation 2.21 we obtain $(q-1)^{p^k} \equiv (q^p-1)^{p^{k-1}} \equiv ... \equiv (q^{p^k}-1) \pmod p$. Then we obtain similarly to Equation 2.22

$$\begin{aligned}(q-1)^{p^{k-1}(p-1)} &\equiv (q^{p^{k-1}}-1)^{p-1} = \frac{(q^{p^{k-1}}-1)^p}{q^{p^{k-1}}-1} && \pmod p \\ &\equiv \frac{(q^{p^{k-1}})^p-1}{q^{p^{k-1}}-1} = \sum_{j=0}^{p-1} q^{jp^{k-1}} = \Phi_{p^k}(q) && \pmod p \end{aligned} \tag{2.23}$$

From the above discussion these two corollaries follow

Corollary 2.10. *Let p^k be a prime power. Then we have $\Phi_{p^k}(q) \equiv (q-1)^{p^{k-1}(p-1)} = (q-1)^{\phi(p^k)}$ (mod p) where $\phi(p^k)$ is the totient function of p^k.*

Corollary 2.11. *Let p^k be a prime power. Then we have $\Phi_{p^k} \in (p, \Phi_1)$, the ideal containing all elements of the form $f(q)p + g(q)\Phi_1(q)$ with $f, g \in \mathbb{Z}[q]$.*

2.4 Irreducibility

Another important property of a cyclotomic polynomial is its irreducibility over $\mathbb{Z}$ and even over $\mathbb{Q}$. It means that for each $n \in \mathbb{N}$ we cannot write $\Phi_n(q) = f(q)g(q)$ for some $f, g \in \mathbb{Q}[q]$ with both of the polynomials being non-constant. The proof is not very simple, except for $n = p$ a prime. In this case we can just use Eisenstein's criterion. In this section we will prove this statement for each $n \in \mathbb{N}$. For the proof we first need to recapitulate the concept of a primitive polynomial. A primitive polynomial is a polynomial with the greatest common divisor of all its coefficients equal to 1. Gauss stated an important lemma about primitive polynomials.

Lemma 2.12 (Gauss)**.** *Let $f, g \in \mathbb{Z}$ be primitive polynomials, then their product $h(q) = f(q)g(q)$ is also primitive.*

Proof. Suppose to the contrary that h is not primitive, then we can write $h(q) = p \cdot \bar{h}(q)$ with $p > 1$ a prime and $\bar{h}$ a polynomial in $\mathbb{Z}[q]$. Write $f(q) = \sum_{i=0}^{k} f_i q^i$ and $g(q) = \sum_{i=0}^{k} g_i q^i$ with $k \geq deg(f), deg(g)$. Let $f_n q^n$ and $g_m q^m$ be the highest degree terms of f and g respectively with $p \nmid f_n, g_m$. These terms have to exist, since f and g are primitive polynomials. Because the coefficient of the term $h_{n+m} q^{n+m}$ is divisible by p and $h_{n+m} = f_{n+m} g_0 + f_{n+m-1} g_1 + ... + f_n g_m + ... + f_1 g_{n+m-1} + f_0 g_{n+m}$, we see that $p \mid f_n g_m$. This is because all other terms in the expression of h_{n+m} are divisible by p, as is h_{n+m} itself. Since p is a prime dividing $f_n g_m$, we know that p divides f_n or g_m. This is a contradiction. □

Let $h \in \mathbb{K}[q]$, where $\mathbb{K}$ is $\mathbb{Z}$ or $\mathbb{Q}$, be non-zero and not be a unit in $\mathbb{K}[q]$. Recall that the polynomial h is called irreducible in $\mathbb{K}[q]$, if any factorisation $h(q) = f(q)g(q)$ with $f, g \in \mathbb{K}[q]$ implies that f or g is a unit in $\mathbb{K}[q]$. With this definition we can prove the following lemma.

Lemma 2.13. *Let h be a primitive polynomial in $\mathbb{Z}[q]$, then h is irreducible in $\mathbb{Z}[q]$ if and only if it is irreducible in $\mathbb{Q}[q]$.*

Proof. First suppose $deg(h) = 0$. Then, since $h(q) = \sum_{i=0}^{deg(h)} h_i q^i$ is a primitive polynomial and h_0 is the only non-zero coefficient of h, we have $h(q) = \pm 1$. Since ± 1 is a unit in $\mathbb{Z}[q]$ and $\mathbb{Q}[q]$, h is reducible in both rings. Thus the lemma is true for h with $deg(h) = 0$.
Now suppose $deg(h) \geq 1$ and h is irreducible in $\mathbb{Q}[q]$. Since the units of $\mathbb{Q}[q]$ are the constants, the elements of $\mathbb{Q}$, we have that h cannot be factorized in a product of non-constant polynomials with lower degree in $\mathbb{Q}[q]$. Therefore h cannot be factorized in a product of non-constant polynomials with lower degree in $\mathbb{Z}[q]$. Since all elements of $\mathbb{Z} \backslash \{-1, 0, 1\}$ are non-units in $\mathbb{Z}[q]$, the only possible factorization of h in $\mathbb{Z}[q]$ is given by: $h(q) = cf(q)$ where $c \in \mathbb{Z} \backslash \{-1, 0, 1\}$ and $f \in \mathbb{Z}[q]$. But then: $|c| > 1$ and $|c| \mid h(q)$, which is a contradiction with the fact that h is primitive.
Now suppose h is reducible in $\mathbb{Q}[q]$. Then we have $f(q) = g(q)h(q)$ with $g, h \in \mathbb{Q}[q]$ non-constant polynomials. Let d_f, d_g be the smallest numbers such that $d_f f(q)$, $d_g g(q) \in \mathbb{Z}[q]$ respectively. Define $\bar{f}(q) = d_f f$ and $\bar{g}(q) = d_g g$. Then $\bar{f}(q)$ and $\bar{g}(q)$ are both primitive polynomials, since if for example f is not, we can find a smaller d_f such that $d_f f \in \mathbb{Z}[q]$. By Lemma 2.12 we also have that $\bar{f}(q)\bar{g}(q) = d_f d_g h(q)$ is a primitive polynomial. Since h is also a primitive polynomial, we can only have $d_f d_g = \pm 1$.
Therefore we have a factorization $h(q) = \pm \bar{f}(q)\bar{g}(q)$ with $\bar{f}$ and $\bar{g}$ non-constant polynomials in $\mathbb{Z}[q]$ and therefore non-units. Thus h is reducible in $\mathbb{Z}[q]$. □

Example 2.2. Consider the polynomial $bq^2 - a$ with $a, b \in \mathbb{N}_0$ and $gcd(a, b) = 1$. Since this polynomial is primitive, Lemma 2.13 tells us that it is irreducible in $\mathbb{Z}[q]$ if and only if it is irreducible in $\mathbb{Q}[q]$. We cannot factor the polynomial into a non-unit constant and a polynomial of degree 2, by the fact that $bq^2 - a$ is primtive. Therefore, the only possible factorization in $\mathbb{Q}[q]$ and $\mathbb{Z}[q]$ is into two linear polynomials. Suppose that this is possible, and we have $bq^2 - a = (c_1q + d_1)(c_2q + d_2)$. By the fact that $bq^2 - a$ could not be factored in a non-unit constant and a polynomial of degree 2, we should have that c_1 and d_1 are coprime as well as c_2 and d_2. If we take $q = -\frac{d_1}{c_1}$ we see that the right hand side of this equation is equal to zero. Therefore we have $b\frac{d_1^2}{c_1^2} - a = 0$. This results in $\frac{d_1^2}{c_1^2} = \frac{a}{b}$. We know that a and b are coprime. Furthermore d_1^2 and c_1^2 are also coprime. We now claim $d_1^2 = a$ and $c_1^2 = b$. This is true, since if $d_1^2 = ma$ for some non-unit $m \in \mathbb{Z}$, we also have $c_1^2 = mb$, which is a contradiction with the fact that d_1^2 and c_1^2 are coprime. Also, if $a = nd_1^2$ for some non-unit $n \in \mathbb{N}$, we also have $b = nc_1^2$, which is again a contradiction. Therefore we obtain $d_1 = \pm\sqrt{a}$ and $c_1 = \pm\sqrt{b}$. By taking $q = -\frac{d_2}{c_2}$ we obtain similarly $d_2 = \pm\sqrt{a}$ and $c_2 = \pm\sqrt{b}$. One possible factorization is $bq^2 - a = (\sqrt{b}q + \sqrt{a})(\sqrt{b}q - \sqrt{a})$. We see that c_1, c_2, d_1 and d_2 are elements of $\mathbb{Z}$ if and only if a and b are squares. Therefore we can factor $bq^2 - a$ in $\mathbb{Z}[q]$ if and only if a and b are squares. If a or b is not a square, the value $\sqrt{a}$ or $\sqrt{b}$ is irrational and therefore not an element of $\mathbb{Q}$. So, we can also factor $bq^2 - a$ in $\mathbb{Q}[q]$ if and only if a and b are squares. Thus the lemma holds for this polynomial.

We are now ready to prove the next theorem.

Theorem 2.14. *For each $n \in \mathbb{N}$ the nth cyclotomic polynomial Φ_n is irreducible over $\mathbb{Q}$.*

Proof. Suppose that Φ_n is reducible over $\mathbb{Q}$. By Lemma 2.13 Φ_n is also reducible over $\mathbb{Z}$ and we can write $\Phi_n(q) = f(q)g(q)$ with $f, g \in \mathbb{Z}[q]$ non-units. Since Φ_n is monic, we can choose both of these polynomials monic, since the product of their leading coefficients should equal 1.
Define $\zeta = e^{\frac{2\pi i}{n}}$. Clearly this is a root of Φ_n, and therefore also a root of f or g or possibly both. We can choose ζ to be a root of f by possibly exchanging the functions f and g. Now define the mapping $N_\zeta : \mathbb{Z}[q] \to \mathbb{Z}[\zeta]$ by $h(q) \mapsto h(\zeta)$. We will show that N_ζ is an ring homomorphism. Obviously, the function 1 in $\mathbb{Z}[q]$ is mapped to 1. Furthermore, take $k, l \in \mathbb{Z}[q]$, then we have

$$N_\zeta(k + l) = (k + l)(\zeta) = k(\zeta) + l(\zeta) = N_\zeta(k) + N_\zeta(l) \tag{2.24}$$
$$N_\zeta(kl) = (kl)(\zeta) = k(\zeta)l(\zeta) = N_\zeta(k)N_\zeta(l) \tag{2.25}$$

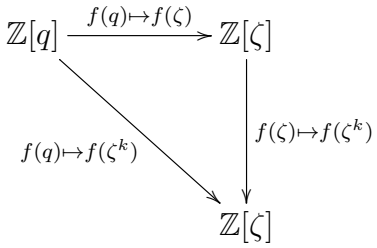
by the fact that we have for all polynomials with $q \in \mathbb{C}$ that $k(q)l(q) = (kl)(q)$ and $(k + l)(q) = k(q) + l(q)$. The kernel of this homomorphism in $\mathbb{Z}[q]$ consists precisely of the polynomials with ζ as a root.
Now take $1 \leq k \leq n - 1$ coprime with n. Then we know by Lemma 2.3 that ζ^k is also a primitive nth root of unity and therefore ζ^k is also a zero of Φ_n. We now define a new mapping $M_k : \mathbb{Z}[\zeta] \to \mathbb{Z}[\zeta]$ by $h(\zeta) \mapsto h(\zeta^k)$ for all such k. Since $ord(\zeta) = n$, we know that every element of $\mathbb{Z}[\zeta]$ can be represented as a polynomial in ζ with degree $< n$, that is $h(\zeta) = h_0 + h_1\zeta + h_2\zeta^2 ... + h_{n-1}\zeta^{n-1}$ with $h_i \in \mathbb{Z}$ for each i, by the fact that $\zeta^n = 1$. Therefore, if we map ζ to ζ^k as above, we see $M_k(h) = h_0 + h_1\zeta^k + h_2\zeta^{2k} + ... + h_{n-1}\zeta^{k(n-1)}$. By the fact that k and n are coprime,

we have that there is no $0 \leq i \leq n-1$ such that $\zeta^{ik} = 1$. As a matter of fact, we know that k has a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$, that is, there is a $1 \leq j \leq n-1$ with $gcd(j,n) = 1$ such that $jk \equiv 1 \pmod{n}$. Therefore $\zeta^{jk} = \zeta$. If $j < \frac{n}{2}$, we then also see $\zeta^{2jk} = \zeta^2$. If $j > \frac{n}{2}$ we see $\zeta^{(2j-n)k} = \zeta^2$, and so on. We therefore see that for each $0 \leq i \leq n-1$ we have $\zeta^{ik} = \zeta^l$ for some $0 \leq l \leq n-1$. Therefore the mapping M_k is well defined.
Now we will proceed with the proof of the fact that this mapping is a homomorphism. Again, the element 1 of $\mathbb{Z}[\zeta]$ is mapped by M_k to 1. Furthermore, take $r(\zeta), s(\zeta) \in \mathbb{Z}[\zeta]$, then we have

$$M_k(r+s) = (r+s)(\zeta^k) = r(\zeta^k) + s(\zeta^k) = M_k(r) + M_k(s) \tag{2.26}$$

$$M_k(rs) = (rs)(\zeta^k) = r(\zeta^k)s(\zeta^k) = M_k(r)M_k(s) \tag{2.27}$$

again by the fact that we can multiply and add polynomials as usual. Therefore M_k is also a ring homorphism.
Now take another zero of Φ_n and name it ω. By the fact that ω is a primitive nth root of unity, we have by Lemma 2.3 that there is a $1 \leq k \leq n-1$ coprime with n such that $\omega = \zeta^k$, where ζ is still equal to $e^{\frac{2\pi i}{n}}$. Therefore $N_\omega = M_k \circ N_\zeta$. Since M_k is a ring homomorphism, it maps 0 to 0. Therefore $ker(N_\zeta) \subset ker(N_\omega)$.
We can see this in the following diagram



Since $f \in ker(N_\zeta)$, we also have that ζ^k is a zero of f for all $1 \leq k \leq n-1$ with k coprime with n. Since these are exactly the roots of Φ_n and both are monic, we have $\Phi_n = f$, which is a contradiction. □

A direct result of the last part of this proof is

Corollary 2.15. *Let $f \in \mathbb{Z}[q]$ be a polynomial with ζ, an primitive nth root of unity, as root. Then $f(\zeta') = 0$ for all primitive nth roots of unity ζ'.*

2.5 Minimal polynomials of roots of unity

We can use the results of the previous section to prove that in fact the nth cyclotomic polynomial is the minimal polynomial of a primitive nth root of unity. Therefore we also have that all polynomials with a primitive nth root of unity as root, are divisible by Φ_n. We will start with a short example.

Example 2.3. Consider the polynomial $f(q) = q^6 + 2q^4 + q^2$. We clearly have $f(i) = 0$ and $f(-i) = 0$. Therefore $f(q) = (q^2+1)(q^2+q^4) = (q^2+1)g(q)$. Since also $g(i) = 0$ and $g(-i) = 0$, we have $f(q) = (q^2+1)^2q^2$. Since i and $-i$ are primitive fourth roots of unity, we see as expected $q^2 + 1 = \Phi_4(q) \mid f(q)$.

Now we state a preliminiary result to prove our expectation.

Lemma 2.16. *Let $f \in \mathbb{Q}[q]$ be the minimal polynomial of an element $\zeta \in \mathbb{C}$. Then, for every $g \in \mathbb{Q}[q]$ with zero ζ we have $f \mid g$.*

Proof. By definition is f the polynomial in $\mathbb{Q}[q]$ of smallest degree and leading coefficient 1 such that ζ is a zero. We have by the Euclidean division algorithm for polynomials

$$g(q) = h(q)f(q) + r(q) \text{ with } deg(r) < deg(f) \text{ or } r(q) = 0 \tag{2.28}$$

where $h, r \in \mathbb{Q}[q]$ are unique. Since ζ is a root for both f and g we also have $(q-\zeta) \mid r$. Since $deg(r) < deg(f)$, ζ is a zero of r and r is an element of $\mathbb{Q}[q]$, this is a contradiction with the fact that f is a minimal polynomial. Therefore $r(q) = 0$ and $f \mid g$, as was to be proven. □

The big question is now if this lemma will also hold if we take f, g, h and r in $\mathbb{Z}[q]$. The answer is 'yes' if we could let f be monic in $\mathbb{Z}[q]$, that is, the minimal polynomial of ζ in $\mathbb{Q}[q]$ should be also an element of $\mathbb{Z}[q]$.

Lemma 2.17. *Let $\zeta \in \mathbb{C}$ be such that its minimal polynomial f over $\mathbb{Q}$, is an element of $\mathbb{Z}[q]$. Then, for every $g \in \mathbb{Z}[q]$ with zero ζ we have $f \mid g$.*

Proof. Since f is monic, we can again use the Euclidean division algorithm.

$$g(q) = h(q)f(q) + r(q) \text{ with } deg(r) < deg(f) \text{ or } r(q) = 0 \tag{2.29}$$

where $h, r \in \mathbb{Z}[q]$ are unique. This is clearly possible, since if g_m is the leading coefficient of g and the degree of f is equal to $k < m$ we can substract $g_m q^{m-k} f(q)$ from $g(q)$ to get a polynomial of degree $m-1$ and so on until the degree of g is smaller than k. If already $k > m$, then we can obviously choose $h(q) = 0$ and $r(q) = g(q)$.
Since ζ is a root for both f and g we also have $(q - \zeta) \mid r$. Since $deg(r) < deg(f)$ and ζ is a zero of r, this is a contradiction with the fact that f is a minimal polynomial. Therefore $r(q) = 0$ and $f \mid g$, as was to be proven. □

Now we can prove a final lemma.

Lemma 2.18. *Let f be a monic irreducible polynomial in $\mathbb{Q}[q]$. Then it is the minimal polynomial of its roots.*

Proof. Let ζ be a root of f, then the minimal polynomial $m(q)$ of ζ over $\mathbb{Q}$ clearly divides f. The polynomial m is not a unit, since it has a root and the degree of m is greater than or equal to 1. Since f is irreducible in $\mathbb{Q}[q]$, we must have $f(q) = a \cdot m(q)$ where a is a unit. Both f and m are monic and therefore $a = 1$, which results in $f(q) = m(q)$. □

Lemmas 2.17 and 2.18 have two important consequences.

Corollary 2.19. *Let ζ be a root of unity with order n. Then the nth cyclotomic polynomial is the minimal polynomial of ζ. For every polynomial $f \in \mathbb{Z}[q]$ with a root of unity ζ, we have $\Phi_n \mid f$ for $n = ord(\zeta)$.*

3 Quotients of $\mathbb{Z}[q]$

After our discussion of cyclotomic polynomials, I would like to devote a section to quotients of the ring $\mathbb{Z}[q]$ and ideals generated by polynomials, in particular by (specific products of) cyclotomic polynomials. First we take a look at $\mathbb{Z}[q]/(\Phi_n(q)^j)$ for arbitrary $n, j \in \mathbb{N}$ and after that at $\mathbb{Z}[q]/(Q_n(q))$ where Q_n is defined as in Equation 2.9.
First I would like to say something about quotient rings in general, since I made a lot of mistakes while investigating this topic. The elements of a quotient ring are in fact equivalence classes. If we, for example take $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 2$, the quotient ring contains the congruence classes $0, 1, ..., n-1$. These are in fact the remainders of the division of elements in $\mathbb{Z}$ by n. It is maybe tempting to regard $\mathbb{Z}/n\mathbb{Z}$ as a subset of $\mathbb{Z}$, but these are two completely different rings. $\mathbb{Z}$ consists of numbers and the quotient ring of congruence classes containing numbers. Each congruence class in $\mathbb{Z}/n\mathbb{Z}$ can be uniquely represented by a number between 0 and $n-1$, but also by a number between $2n$ and $3n-1$, since $mn+k$ belongs to the same congruence class as k for $m \in \mathbb{N}_0$ and $0 \leq k \leq n-1$.

3.1 Properties of $\mathbb{Z}[q]/(\Phi_n(q)^j)$

Let us first consider the elements of the quotient ring $\mathbb{Z}[q]/(\Phi_n(q))$. As already stated the degree of Φ_n is equal to $\phi(n)$. Recall that all elements of a quotient ring are congruence classes. We claim that each element of $\mathbb{Z}[q]/(\Phi_n(q))$ can be uniquely represented as a polynomial of degree smaller than $\phi(n)$, that is, each congruence class contains precisely one polynomial of degree smaller than $\phi(n)$. If this was false, we could take a congruence class only consisting of polynomials of degree $\geq \phi(n)$ Take an element f with the smallest degree k in this congruence class and denote this element by $f(q) = f_k q^k + f_{k-1}q^{k-1} + ... + f_0$. Since Φ_n is monic, the polynomial $g(q) = f(q) - f_k q^{k-\phi(n)}\Phi_n(q)$ has degree $k-1$ and belongs to the same congruence class as f, which is a contradiction. By the Euclidean division algorithm from Equation 2.28, we see that two polynomials of degree $< \phi(n)$ cannot be equivalent modulo a polynomial of degree $\phi(n)$ and therefore every element of $\mathbb{Z}[q]/(\Phi_n(q))$ is a congruence class uniquely determined by the polynomial of degree $< \phi(n)$ in that congruence class. This results in the next corollary.

Corollary 3.1. *For each $n \in \mathbb{N}$, the quotient ring $\mathbb{Z}[q]/(\Phi_n(q))$ consists of all congruence classes in $\mathbb{Z}[q]$ modulo $\Phi_n(q)$ and each congruence class contains a unique polynomial of degree $< \phi(n)$. Furthermore two different polynomials of degree $< \phi(n)$ in $\mathbb{Z}[q]$ belong to different congruence classes.*

Example 3.1. If we take $n = 1$, the quotient ring is given by $\mathbb{Z}[q]/(q-1)$. By our discussion above we know that all congruence classes in $\mathbb{Z}[q]/(q-1)$ contain one unique constant in $\mathbb{Z}$. This does not surprise us, since $\mathbb{Z}[q]/(q-1) \cong \mathbb{Z}$ by the fact that $(q-1)$ is the kernel of the homomorphism $f : \mathbb{Z}(q) \to \mathbb{Z}$ given by $P(q) \mapsto P(1)$. The same happens for $n = 2$, where the quotient ring is $\mathbb{Z}[q]/(q+1) \cong \mathbb{Z}$.
If we take $n = 3$ or $n = 4$ we obtain $\mathbb{Z}[q]/(q^2+q+1)$ and $\mathbb{Z}[q]/(q^2+1)$ respectively as quotient rings. In both rings each congruence class contains only one polynomail with degree ≤ 1, which is therefore a constant or a linear polynomial.

Now we take arbitrary $j \in \mathbb{N}$. Obviously the degree of $\Phi_n(q)^j$ equals $j\phi(n)$. Therefore we have by the same argument as above

Corollary 3.2. *For all $n, j \in \mathbb{N}$, the quotient ring $\mathbb{Z}[q]/(\Phi_n(q)^j)$ consists of all congruence classes in $\mathbb{Z}[q]$ modulo $\Phi_n(q)^j$ and each congruence class contains a unique polynomial of degree $< j\phi(n)$. Furthermore two different polynomials of degree $< j\phi(n)$ in $\mathbb{Z}[q]$ belong to different congruence classes.*

This is not quite a surprise. The next theorem is much less obvious.

Theorem 3.3. *Let $n, j \in \mathbb{N}$. Then for each $f \in \mathbb{Z}[q]$ there are unique polynomials f_i for $0 \leq i \leq j-1$ with $deg(f_i) \leq (\phi(n)-1)$ such that*

$$f(q) - f_0(q) - \sum_{i=1}^{j-1} f_i(q)\Phi_n(q)^i \equiv 0 \ (mod\ \Phi_n(q)^j) \tag{3.1}$$

Proof. We can use the Euclidean division algorithm for polynomials given by Equations 2.28 and 2.29, since the nth cyclotomic polynomial is monic for each $n \in \mathbb{N}$. Take $f \in \mathbb{Z}[q]$ and define r_j with help of the Euclidean division algorithm where we divide the polynomial f by the jth power of the nth cyclotomic polynomial, that is, $r_j(q) \equiv f(q) \pmod{\Phi_n(q)^j}$. The remainder r_j should have $deg(r_j) \leq j\phi(n) - 1$. Now again use the Euclidean division algorithm, which results in

$$r_j(q) = f_{j-1}(q)\Phi_n(q)^{j-1} + r_{j-1}(q) \tag{3.2}$$

with $deg(r_{j-1}) \leq (j-1)\phi(n) - 1$. We therefore also have $deg(f_{j-1}) = deg(r_j) - deg(\Phi_n^{j-1}) \leq j\phi(n) - 1 - (j-1)\phi(n) = \phi(n) - 1$. We can do this again repeatedly obtaining

$$r_k(q) = f_{k-1}(q)\Phi_n(q)^{k-1} + r_{k-1}(q) \tag{3.3}$$

with $deg(r_{k-1}) \leq (k-1)\phi(n)-1$ and again $deg(f_{k-1}) \leq \phi(n)-1$ for each $1 \leq k \leq j-1$. We therefore see that

$$r_j(q) = f_0(q) + \sum_{i=1}^{j-1} f_i(q)\Phi_n(q)^i \tag{3.4}$$

with $deg(f_i) \leq (\phi(n)-1)$ for $0 \leq i \leq j-1$, with the polynomials f_i uniquely determined by the Euclidean division algorithm. Since $r_j(q) \equiv f(q) \pmod{\Phi_n(q)^j}$, we have $f(q) - r_j(q) \equiv 0 \pmod{\Phi_n(q)^j}$, as required to prove the theorem. □

We will call Equation 3.4 the finite Φ_n-adic expansion of r_j. In general each polynomial f with integer coefficients has a finite Φ_n-adic expansion, since there is always a $j \in \mathbb{N}$ such that $deg(f) < j\phi(n)$. Therefore the polynomial f is the unique polynomial of degree $< j\phi(n)$ in a congruence class belonging to the ring $\mathbb{Z}[q]/(\Phi_n(q)^j)$. By the procedure used in the proof of the previous theorem we can obtain its finite Φ_n-adic expansion, given by Equation 3.4 with $f(q) = r_j(q)$.

Example 3.2. If we again take $n = 4$ and take a look at the quotient ring $\mathbb{Z}[q]/(\Phi_4(q)^3) = \mathbb{Z}[q]/((q^2+1)^3)$. Observe that each element of this ring can be identified with a unique polynomial with integer coefficients and degree ≤ 5. Let us take such a polynomial, for example $f(q) = 4q^4 - 3q^3 + 1$. Since $\Phi_4(q)^2 = q^4 + 2q^2 + 1$, we have $f(q) = 4\Phi_4(q)^2 - 11q^3 - 3$ and therefore $f_2(q) = 4$. Here we used again the

Euclidean division algorithm with $h(q) = f_2(q)$ and $r_1(q) = -11q^3 - 3$. We use r_1 to determine the other coefficients, again by the Euclidean division algorithm. We have $r_1(q) = -11q\Phi_4(q) + 11q - 3$. Therefore $f_1(q) = -11q$ and $f_0(q) = 11q - 3$. Therefore the finite Φ_4-adic expansion of f is given by

$$4q^4 - 3q^3 + 1 = -3 + 11q - 11q\Phi_4(q) + 4\Phi_4(q)^2 \tag{3.5}$$

3.2 Properties of $\mathbb{Z}[q]/(Q_n(q))$

We now stop our discussion of cyclotomic polynomials and recall the definition of the polynomials Q_n for $n \in \mathbb{N}_0$ given in Equations 2.8 and 2.9

$$Q_0(q) = 1 \tag{3.6}$$

$$Q_n(q) = \prod_{j=1}^{n}(1 - q^j) = (-1)^n \prod_{j=1}^{n}(q^j - 1) \qquad \text{if } n \geq 1 \tag{3.7}$$

Observe that for $n \leq m$ we have $Q_n \mid Q_m$ and

$$Q_m(q) = Q_n(q) \prod_{j=n+1}^{m} (1 - q^j) \tag{3.8}$$

The main goal of this thesis is to understand more about the Habiro ring, which is some kind of limit for $n \to \infty$ of the quotient rings $\mathbb{Z}[q]/(Q_n(q))$, described in the next section. First we would like to see some properties of $\mathbb{Z}[q]/(Q_n(q))$. Since $deg(Q_n) = deg(1-q) + deg(1-q^2) + ... + deg(1-q^n) = 1 + 2 + ... + n = \frac{n(n+1)}{2}$, we know by the same discussion as in the proof of Corollary 3.1 that the quotient ring $\mathbb{Z}[q]/(Q_n(q))$ consists of congruence classes, which contain exactly one polynomial of degree $< \frac{n(n+1)}{2}$ and each polynomial of degree $< \frac{n(n+1)}{2}$ belongs to an element (congruence class) of $\mathbb{Z}[q]/(Q_n(q))$.
If we take $n = 1$, we obtain the quotient ring $\mathbb{Z}[q]/(1-q)$, which is isomorphic to $\mathbb{Z}$ and $\mathbb{Z}[q]/(q-1)$, by the fact that $(1-q)$ is the kernel of the homomorphism $f : \mathbb{Z}[q] \to \mathbb{Z}$ given by $P(q) \mapsto P(1)$. This is not quite interesting. If we take $n = 2$, we obtain the quotient ring $\mathbb{Z}[q]/(1 - q - q^2 + q^3)$. Apart from the fact that every element of this ring can be identified with a polynomial of degree less than or equal to 2, we cannot directly say anything interesting about this ring. We can try to find an isomorphism from $\mathbb{Z}[q]/(Q_2(q))$ to another 'easier' ring or a product of rings. The first guess would be to use the Chinese Remainder Theorem.

Theorem 3.4 (Chinese Remainder Theorem)**.** *Let R be a commutative ring and I_1, ..., I_k ideals of R which are all pairwisely relative prime, that is $I_i + I_j = R$ for $i \neq j$. Then we have $R/\prod_{i=1}^{k} I_i \cong R/I_1 \times R/I_2 \times \cdots \times R/I_k$*

If we take $n = 2$ we have $Q_2(q) = (1-q)^2(1+q)$, so we could try to prove the relation $\mathbb{Z}[q]/(Q_2(q)) \cong \mathbb{Z}[q]/((1-q)^2) \times \mathbb{Z}$. Unfortunately, we cannot use the Chinese Remainder Theorem in this case. If we take $I_1 = ((1-q)^2)$ and $I_2 = (1+q)$, we have to show that these two ideals are relative prime, that is, there are $x \in I_1$ and $y \in I_2$ such that $x + y = 1$. These x, y are not so easy to find, in fact it turns out to be impossible.

We first assume that there is in fact an isomorphism f from $\mathbb{Z}[q]/(Q_2(q))$ to $\mathbb{Z}[q]/((1-q)^2)\times\mathbb{Z}$. Every element of $\mathbb{Z}[q]/(Q_2(q))$ can be identified with a polynomial $a+bq+cq^2$ and every element of $\mathbb{Z}[q]/((1-q)^2)\times\mathbb{Z}$ with $(\alpha+\beta q,\gamma)$. Therefore we could express α, β and γ as functions of the variables a, b and c.
By the fact that $f(x+y)=f(x)+f(y)$ for all x, y we see that α, β and γ have to be linear combinations of a, b and c.

$$\begin{pmatrix}\alpha\\ \beta\\ \gamma\end{pmatrix}=\begin{pmatrix}a_1 & a_2 & a_3\\ b_1 & b_2 & b_3\\ c_1 & c_2 & c_3\end{pmatrix}\begin{pmatrix}a\\ b\\ c\end{pmatrix}=M\begin{pmatrix}a\\ b\\ c\end{pmatrix} \tag{3.9}$$

In the above equation, all entries of the matrix M have to be elements of $\mathbb{Z}$. If some entry is not in $\mathbb{Z}$, for example b_2, then we could take $a=c=0$ and $b=1$, which gives $\beta=b_2\notin\mathbb{Z}$. Since f is a an isomorphism we have $f(1)=(1,1)$ and therefore $a_1=1$, $b_1=0$ and $c_1=1$. If we want to obtain the other six coefficients, we have to use the third condition for an isomorphism, which is $f(xy)=f(x)f(y)$ for all x, y. Therefore we have to determine how to multiply elements in $\mathbb{Z}[q]/(Q_2(q))$ and $\mathbb{Z}[q]/((1-q)^2)\times\mathbb{Z}$.

$$\begin{aligned}(a+bq+cq^2)(d+eq+fq^2)&\equiv(ad-ce-bf-cf)+q(bd+ae+ce+bf)\\ &\quad+q^2(cd+be+ce+af+bf+2cf)\ (\mathrm{mod}\ \mathbb{Z}[q]/Q_2)\\ (\alpha+\beta q,\gamma)(\alpha'+\beta' q,\gamma')&\equiv((\alpha\alpha'-\beta\beta')+q(\alpha\beta'+\beta\alpha'+2\beta\beta'),\gamma\gamma')\\ &\quad(\mathrm{mod}\ \mathbb{Z}[q]/(1-q)^2\times\mathbb{Z})\end{aligned}$$

We take α', β' and γ' as functions of d, e and f, given by

$$\begin{pmatrix}\alpha'\\ \beta'\\ \gamma'\end{pmatrix}=M\begin{pmatrix}d\\ e\\ f\end{pmatrix} \tag{3.10}$$

Then we see, by the above equations and the third condition of an isomorphism.

$$\begin{aligned}\alpha\alpha'-\beta\beta'&=a_1(ad-ce-bf-cf)+a_2(bd+ae+ce+bf)+\\ &\quad a_3(cd+be+ce+af+bf+2cf)\\ \alpha\beta'+\alpha'\beta+2\beta\beta'&=b_1(ad-ce-bf-cf)+b_2(bd+ae+ce+bf)\\ &\quad+b_3(cd+be+ce+af+bf+2cf)\\ \gamma\gamma'&=c_1(ad-ce-bf-cf)+c_2(bd+ae+ce+bf)\\ &\quad+c_3(cd+be+ce+af+bf+2cf)\end{aligned}$$

We can even obtain 9 easy solvable equations chosing $a=d=1$ and all other coefficients zero, $b=e=1$ and all other coefficients zero or $c=f=1$ and all other coefficients zero. We can solve this with help of a computer and obtain several sets of coefficients. Most of them contain coefficients which are not elements of $\mathbb{Z}$, so they are not the right solutions. The solutions that satisfy the conditons are

$$M=\begin{pmatrix}a_1 & a_2 & a_3\\ b_1 & b_2 & b_3\\ c_1 & c_2 & c_3\end{pmatrix}=\begin{pmatrix}1 & 1-\tau & 1-2\tau\\ 0 & \tau & 2\tau\\ 1 & \pm1 & 1\end{pmatrix} \tag{3.11}$$

We have now obtained our matrix M, depending on some τ that we still have to determine, but is definitely an integer. If we rearrange Equation 3.9 we see

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} = M^{-1} \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} \tag{3.12}$$

Of course all entries of M^{-1} also have to be elements of $\mathbb{Z}$. By the fact that MM^{-1} has to be equal to the identity matrix I_3, we have $det(M)det(M^{-1}) = det(I_3) = 1$. Obviously the determinant of a matrix with solely integer entries has to be an integer. Therefore we have $det(M) = det(M^{-1}) = \pm 1$. We can easily calculate the determinant of M

$$det(M) = \tau + 2\tau(1-\tau) - \tau(1-2\tau) \mp 2\tau = 2\tau \mp 2\tau \tag{3.13}$$

If we take the minus sign in the above equation we see $det(M) = 0$, which is for sure a contradiction. If we take the plus sign, we see $det(M) = 4\tau$ and therefore $\tau = \pm\frac{1}{4}$, which is not an integer and therefore also a contradiction.
Since we cannot find an M which satisfies Equations 3.9 and 3.12 with the entries of both M and M^{-1} in $\mathbb{Z}$, there is no isomorphism f between $\mathbb{Z}[q]/(Q_2(q))$ and $\mathbb{Z}[q]/((1-q)^2) \times \mathbb{Z}$.
In the same way we can prove that $\mathbb{Z}[q]/(Q_2(q)) \ncong \mathbb{Z}[q]/(1-q^2) \times \mathbb{Z}$ and $\mathbb{Z}[q]/(Q_2(q)) \ncong (\mathbb{Z}[q]/(1-q))^2 \times \mathbb{Z}$. So we cannot find an isomorphism between $\mathbb{Z}[q]/(Q_2(q))$ and a product of some 'smaller', known rings. The same thing holds for $\mathbb{Z}[q]/(Q_3(q))$, but the proof is much longer and not interesting to cover in this thesis.

3.3 Finite Habiro expansions in $\mathbb{Z}[q]/(Q_n(q))$

Similarly to the finite Φ_n-adic expansion of all elements of $\mathbb{Z}[q]/(\Phi_n(q)^j)$ introduced in Section 3.1, we can a introduce a concept I call the finite Habiro expansion in $\mathbb{Z}[q]/(Q_n(q))$.

Theorem 3.5. *Let $n \in \mathbb{N}$. Then for each $f \in \mathbb{Z}[q]$ there are unique polynomials f_i for $0 \leq i \leq n-1$ with $deg(f_i) \leq i$ such that*

$$f(q) - \sum_{i=0}^{j-1} f_i(q)Q_i(q) \equiv 0 \ (mod\ Q_n(q)) \tag{3.14}$$

Proof. We can use again the Euclidean division algorithm for polynomials given by Equations 2.28 and 2.29, since Q_n is monic for n even and $-Q_n$ is monic for n odd. Take $f \in \mathbb{Z}[q]$ and define r_n with help of the Euclidean division algorithm where we divide the polynomial f by the polynomial Q_n, that is, $r_n(q) \equiv f(q) \pmod{Q_n(q)}$. The remainder r_n should have $deg(r_n) \leq \frac{n(n+1)}{2} - 1$.
Now again use the Euclidean division algorithm, which results in

$$r_n(q) = f_{n-1}(q)Q_{n-1}(q) + r_{n-1}(q) \tag{3.15}$$

with $deg(r_{n-1}) \leq \frac{(n-1)n}{2}$. We therefore also have $deg(f_{n-1}) = deg(r_n) - deg(Q_{n-1}) \leq \frac{n(n+1)}{2} - 1 - \frac{(n-1)n}{2} = \frac{n^2+n-n^2+n}{2} - 1 = n-1$.

We can do this again repeatedly obtaining

$$r_k(q) = f_{k-1}(q)Q_{k-1}(q) + r_{k-1}(q) \tag{3.16}$$

with $deg(r_{k-1}) \leq \frac{(k-1)(k)}{2} - 1$ and again $deg(f_{k-1}) \leq \frac{k(k+1)}{2} - 1 - \frac{(k-1)k}{2} = k - 1$ for each $1 \leq k \leq n-1$.
We therefore see that

$$r_n(q) = \sum_{i=0}^{n-1} f_i(q)Q_i(q) \tag{3.17}$$

with $deg(f_i) \leq i$ for $0 \leq i \leq j-1$, with the polynomials f_i uniquely determined by the Euclidean division algorithm. Since $r_n(q) \equiv f(q) \pmod{Q_n(q)}$, we have $f(q) - r_n(q) \equiv 0 \pmod{Q_n(q)}$, as required to prove the theorem. □

Following the theorem we could define some kind of independent basis of $\mathbb{Z}[q]/(Q_n(q))$, consisting of all products $q^j Q_i$ with $i \geq 0$ and $j = 0, 1, 2, ..., i$. Furthermore, as already said, we will call Equation 3.17 the finite Habiro expansion of r_n in $\mathbb{Z}[q]/(Q_n(q))$, in comparison with the (infinite) Habiro expansion we will use in the concept of the Habiro ring. Similarly to the fact that each polynomial with integer coefficients has a finite Φ_n-adic expansion, each polynomial $f \in \mathbb{Z}[q]$ has a finite Habiro expansion. This is because there is always an $n \in \mathbb{N}$ such that $deg(f) \leq \frac{n(n+1)}{2}$ and therefore is the unique polynomial of degree $< \frac{n(n+1)}{2}$ in a congruence class belonging to the ring $\mathbb{Z}[q]/(Q_n(q))$. Then we can take $f(q) = r_n(q)$ and obtain its Habiro expansion by the usual method of the Euclidean division algorithm.

Example 3.3. If we again take $n = 4$ and have a look at the Habiro expansion of the polynomial $f(q) = 8 - 5q + 6q^2 - 2q^4 - 2q^5 + q^6 + 2q^7 - q^8$ in $\mathbb{Z}[q]/(Q_4(q))$. We have $Q_3(q) = 1 - q - q^2 + q^4 + q^5 - q^6$ and therefore

$$f(q) = (q^2 - q - 1)Q_3(q) + 3q^2 - 5q + 9 \tag{3.18}$$

Therefore we have $f_3(q) = q^2 - q - 1$, and we see $deg(f_3) = 2$, as expected.
Since $Q_2(q) = q^3 - q^2 - q + 1$, we have $deg(Q_2) = 3$ and therefore $f_2(q) = 0$, by the fact that the remainder of the division of f by Q_3, has degree 2. Since $Q_1(q) = 1 - q$, we obtain

$$f(q) = (q^2 - q - 1)Q_3(q) + (-3q + 2)Q_1(q) + 7 \tag{3.19}$$

and therefore $f_1(q) = -3q + 2$ and $f_0 = 7$. Equation 3.19 gives us the Habiro expansion of f in $\mathbb{Z}[q]/(Q_4(q))$, with the condition that $deg(f_i) \leq i$ for each i.

4 Projective limits

4.1 Formal definitions

In the previous section we regarded the ring $\mathbb{Z}[q]/(Q_n(q))$ for finite n. In this section we will examine the so called projective (or inverse) limit of $\mathbb{Z}[q]/(Q_n(q))$ for $n \to \infty$, which gives the Habiro ring

$$\widehat{\mathbb{Z}[q]} = \lim_{\infty \leftarrow n} \mathbb{Z}[q]/(Q_n(q)) \tag{4.1}$$

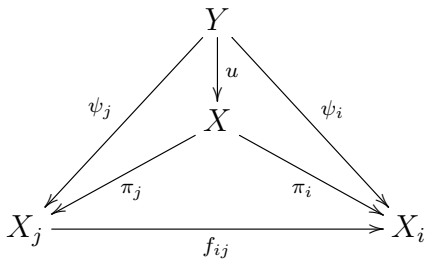
First we need to take a closer look at the concept of the projective limit. It is different from the (direct) limit used in mathematical analysis. It has, of course, something to do with projections. We will first pose a formal definition of the projective (or inverse) system of rings and the projective limit, which do not only hold for rings, but also for many other mathematical objects, such as groups.

Definition 4.1 (Projective system)**.** *Let I be an index set with the property that we can order the elements, for example $\mathbb{N}$, also called a poset. Let $(X_i)_{i\in I}$ be a family of rings. Furthermore, assume that we also have a family of homomorphism $f_{ij} : X_j \to X_i$ for $i \leq j$ such that*

1. *$f_{ii} = id_{X_i}$ for all $i \in I$*
2. *$f_{ik} = f_{ij} \circ f_{jk}$ for all $i \leq j \leq k$*

Then the pair of families $((X_i)_{i\in I}, (f_{ij})_{i\leq j\in I})$ is called a projective (or inverse) system of rings and homomorphisms over I and the functions f_{ij} are the so called transition homomorphisms.

Definition 4.2 (Projective limit)**.** *Let $((X_i)_{i\in I}, (f_{ij})_{i\leq j\in I})$ be again a projective system of rings and homomorphisms over I. A projective limit of the system is a ring X together with homomorphisms $\pi_i : X \to X_i$ defined for all $i \in I$, the so called projections. These projections must satisfy $\pi_i = f_{ij} \circ \pi_j$ for $i \leq j$. Additionally, for any other ring Y with homomorphisms $\psi_i : Y \to X_i$ for each $i \in I$ with $\psi_i = f_{ij} \circ \psi_j$, there must be a unique homomorphism $u : Y \to X$ such that the next diagram commutes for all $i \leq j$ [7]*



We will take $I = \mathbb{N}$, since we will encouter this case in the next sections.
The question may arise whether or not this definition makes sense, since we do not know if we defined something that exists. Therefore, define $X = \{\xi : \mathbb{N} \to \bigcup_{i=1}^{\infty} X_i \mid \xi_i \in X_i, f_{ij}(\xi_i) = \xi_j \text{ for all } i \leq j \in \mathbb{N}\}$. It will turn out that X is a projective limit of

the projective system, if we take $\pi_i(\xi) = \xi_i$ for each i. Then for $i \leq j$, we obviously have $\pi_i(\xi) = \xi_i = f_{ij}(\xi_j) = \xi_j = \pi_j(\xi)$, which results in $\pi_i = f_{ij} \circ \pi_j$. The fact that the projections π_i are homomorphims follows from the fact that $f_{ij}(\xi_j) = \xi_i$ with f_{ij} homomorphims. Let us assume that there is another ring Y together with homomorphims $\psi_i : Y \to X_i$ satisfying $\psi_i = f_{ij} \circ \psi_j$ for all $i \leq j \in \mathbb{N}$. Take an element $y \in Y$ and define $u(y) : \mathbb{N} \to \bigcup_{i=1}^{\infty} X_i$ given by $u_i(y) = \psi_i(y)$. Clearly, $u(y)$ satisfies the conditions in the definition of ξ and therefore $u(y) \in X$. Therefore by our above definition X is a projective limit of the system depicted in the diagram.
In the next sections we will often see that every $\xi \in X$ can be given as some infinite series, which we call an expansion, and ξ_i is a partial sum. Therefore $(\xi_i)_{i \in \mathbb{N}}$ forms a sequence. Furthermore, we see that if two rings X and Y both are a projective limit of a system, there exist homomorphisms $u : X \to Y$ and $v : Y \to X$. Therefore there exists a isomorphism between X and Y. Since all projective limits of a projective system are isomorphic, we often speak of 'the' projective limit of a system instead of 'a' projective limit.
We now start with two examples of projective limits, the ring of p-adic integers and the Φ_n-adic completion of the ring of polynomials with integer coefficients. We will not discuss the 'other' ring Y with homomorphisms ψ_i until Section 4.4.

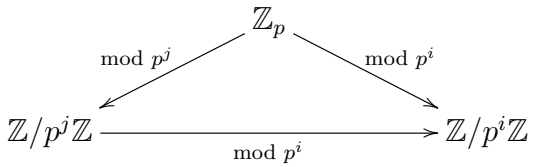
4.2 Two examples

The ring of p-adic integers

Probably the best known example of the projective limit is the ring of p-adic integers $\mathbb{Z}_p$ with p a prime. It contains all finite and infinite p-adic series. It is defined as $\lim_{\infty \leftarrow n} \mathbb{Z}/p^n\mathbb{Z}$ and it is called the p-adic completion of $\mathbb{Z}$, since it extends the 'normal' system of integers in the sense that the ring of p-adic integers also contains infinite series in the prime p.
First take a look at $\mathbb{Z}/p^n\mathbb{Z}$. We know that it consists of all congruence classes modulo p^n. Each contains a unique number between 0 and $p^n - 1$. In fact, we can write all these unique numbers in a finite p-adic expansion

$$m = m_0 + \sum_{i=1}^{n-1} m_i p^i \tag{4.2}$$

where m_i are called the p-adic digits and attain values between 0 and $p - 1$.
Define for $i \leq j$ the mapping $f_{ij} : \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ as $m \mapsto m \pmod{p^i}$, which is obviously a homomorphism. Every congruence class $m \in \mathbb{Z}/p^j\mathbb{Z}$ contains some unique element $\bar{m}$ between 0 and $p^j - 1$. The congruence class of $\bar{m}$ in $\mathbb{Z}/p^j\mathbb{Z}$ is mapped to the congruence class of $\bar{m} \pmod{p^i}$ in $\mathbb{Z}/p^i\mathbb{Z}$. Therefore this mapping is clearly well defined and surjective, since $i \leq j$ and every element $\bar{m}'$ between 0 and $p^i - 1$, also satisfies $0 \leq \bar{m}' \leq p^j - 1$. The mapping is not injective if $i \neq j$, by the fact that 1 and $p^i + 1$ are mapped to 1, but belong to a different congruence class modulo p^j. Obviously, f_{ii} is the identity mapping on $\mathbb{Z}/p^i\mathbb{Z}$ and we also have $f_{ik}(m) = (f_{ij} \circ f_{jk})(m)$ for all $m \in \mathbb{Z}/p^k\mathbb{Z}$ and $i \leq j \leq k$.
Observe that the mapping f_{ij} takes a congruence class in $\mathbb{Z}/p^j\mathbb{Z}$, looks at the finite p-adic expansion of an element and removes all powers of p greater than or equal to i. If this is not clear to you, there will be a longer explanation in the next section about the Habiro ring. The projective limit is depicted in the next diagram.



The ring of p-adic integers contains all finite and infinite p-adic series, as already mentioned in Section 4.1, and the series $\sum_{i=0}^{\infty} p^i$ converges in this ring. We will not discuss the exact reason for this, but we will get something similar in the Habiro ring with infinite Habiro expansions.
Surely, all integers ≥ 0 have a finite p-adic expansion, similar to the Φ_n-adic expansion introduced in Section 3.1, for example

$$78 = 1 + 4 \cdot 7 + 1 \cdot 7^2 \tag{4.3}$$

Here we also have a restriction on the coefficients of the p-adic expansion. These so called p-adic digits attain values between 0 and $p - 1$. But it turns out that in the ring of p-adic integers, some fractions also have a infinite p-adic expansion, and are therefore also p-adic integers.
We have for example if $p = 7$

$$\frac{1}{2} = 4 + 3 \cdot 7 + 3 \cdot 7^2 + 3 \cdot 7^3 + ... \tag{4.4}$$

by the fact that

$$\begin{aligned} 2(4 + 3 \cdot 7 + 3 \cdot 7^2 + 3 \cdot 7^3 + ...) &= 1 + 7 \cdot 7 + 6 \cdot 7^2 + 6 \cdot 7^3 + ... \\ &= 1 + 0 \cdot 7 + 7 \cdot 7^2 + 6 \cdot 7^3 + ... \\ &= 1 + 0 \cdot 7 + 0 \cdot 7^2 + 0 \cdot 7^3 + ... \\ &= 1 \end{aligned} \tag{4.5}$$

Furthermore a negative integer can also be given by an infinite p-adic expansion, for example

$$-2 = 5 + 6 \cdot 7 + 6 \cdot 7^2 + 6 \cdot 7^3 + ... \tag{4.6}$$

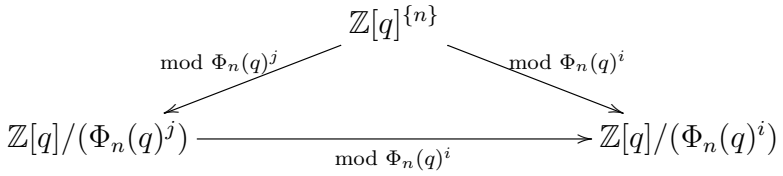
by the fact that

$$\begin{aligned} 2 + (5 + 6 \cdot 7 + 6 \cdot 7^2 + 6 \cdot 7^3 + ...) &= 7 + 6 \cdot 7 + 6 \cdot 7^2 + 6 \cdot 7^3 = 0 + 7 \cdot 7 + 7 \cdot 7^2 + 7 \cdot 7^3 + ... \\ &= 0 + 0 \cdot 7 + 0 \cdot 7^2 + ... = 0 \end{aligned} \tag{4.7}$$

We will not discuss these (infinite) p-adic expansions in the rest of this thesis, but we see that these infinite expansions only show up if we take the (projective) limit n to infinity.

The Φ_n-adic completion of $\mathbb{Z}[q]$

Since we have already looked at the quotient rings $\mathbb{Z}[q]/(\Phi_n(q)^j)$ for arbitrary $n, j \in \mathbb{N}$, it seems natural to investigate if the system has a projective limit for $j \to \infty$. We will keep in our minds that each congruence class in $\mathbb{Z}[q]/(\Phi_n(q)^j)$ can be identified with a unique polynomial of degree $< j\phi(n)$. Now, to construct the projective limit, we use the Φ_n-adic expansion of these polynomials. Define the mapping $f_{ij} : \mathbb{Z}[q]/(\Phi_n(q)^j) \to \mathbb{Z}[q]/(\Phi_n(q)^i)$ for $j \geq i$ by $m \mapsto m \pmod{\Phi_n(q)^i}$, which is in fact truncating the Φ_n-adic expansion of m at $\Phi_n(q)^i$, as it was with the ring of p-adic integers. These mappings are clearly homomorphisms satisfying the conditions in Definition 4.1.
Therefore $((\mathbb{Z}[q]/(\Phi_n(q)^j))_{j\in\mathbb{N}}, (f_{ij})_{i\leq j\in\mathbb{N}})$ is a projective system of rings and homomorphisms. If we now take the (projective) limit $j \to \infty$, we get a ring which we will denote by $\mathbb{Z}[q]^{\{n\}}$. Similarly to the ring of p-adic integers, this ring contains all finite and infinite Φ_n-adic expansions. Therefore it is also called the Φ_n-adic completion of $\mathbb{Z}[q]$, similarly to the ring of p-adic integers being caleed the p-adic completion of $\mathbb{Z}$. The projections $\pi_j : \mathbb{Z}[q]^{\{n\}} \to \mathbb{Z}[q]/(\Phi_n(q)^j)$ are again just truncating the Φ_n-adic expansion of an element at $\Phi_n(q)^j$, clearly satisfying the definition of a projective limit. This is depicted in the next diagram.



4.3 Constructing the Habiro ring

Finally we are ready to take a closer look at the Habiro ring. As already mentioned the Habiro ring is defined as the projective limit of $n \to \infty$ for the quotient rings $\mathbb{Z}[q]/(Q_n(q))$. Define the mapping $f_{ij} : \mathbb{Z}[q]/(Q_j(q)) \to \mathbb{Z}[q]/(Q_i(q))$ for $j \geq i$ by $m \mapsto m \pmod{Q_i(q)}$. Let us have a look at the features of this mapping.

Example 4.1. Consider the mapping $f_{23} : \mathbb{Z}[q]/(Q_3(q)) \to \mathbb{Z}[q]/(Q_2(q))$. Let us take an element in $\mathbb{Z}[q]/(Q_3(q))$ and denote its unique polynomial of degree smaller than 6 by m. Denote the Habiro expansion of m in $\mathbb{Z}[q]/(Q_3(q))$ by

$$m(q) = m_0 + m_1(q)Q_1(q) + m_2(q)Q_2(q) \tag{4.8}$$

Since $deg(m_1) \leq 1$ we have $deg(m_0 + m_1Q_1) \leq 2 < deg(Q_2)$. Therefore $m_0 + m_1Q_1 \notin (Q_2)$. We thus see $m(q) \equiv m_0 + m_1(q)Q_1(q) \pmod{Q_2(q)}$, and $m_0 + m_1Q_1$ is clearly the unique polynomial of degree < 3 of an element (congruence class) of $\mathbb{Z}[q]/(Q_2(q))$. We now understand what the mapping f_{23} is about. It takes a congruence class in $\mathbb{Z}[q]/(Q_3(q))$ and considers its unique polynomial of degree smaller than 6. It only takes the first two terms of the Habiro expansion of this polynomial and maps the congruence class in $\mathbb{Z}[q]/(Q_3(q))$ to the congruence class of the polynomial, given by these first two terms, in $\mathbb{Z}[q]/(Q_2(q))$.

For example, let us consider the congruence class of the polynomial $m(q) = 3 + 2q - 4q^2 + q^3 + q^5 - q^6$. By the fact that $Q_3(q) = 1 - q - q^2 + q^4 + q^5 - q^6$, we see $m(q) \equiv 2 + 3q - 3q^2 + q^3 - q^4 \pmod{Q_3(q)}$, and therefore $2 + 3q - 3q^2 + q^3 - q^4$ is the unique polynomial of degree smaller than 6 in this congruence class. The Habiro expansion of this polynomial is given by

$$2 + 3q - 3q^2 + q^3 - q^4 = 2 + 4qQ_1(q) - qQ_2(q) \tag{4.9}$$

The mapping f_{23} maps the congruence class of $m(q)$ to the congruence class of $2 + 4qQ_1(q)$ in $\mathbb{Z}[q]/(Q_2(q))$.

In general we can therefore describe the mapping f_{ij} as follows

1. Take a congruence class $m \in \mathbb{Z}[q]/(Q_j(q))$.
2. Determine the polynomial of smallest degree in this congruence class, which is unique and has degree $< \frac{j(j+1)}{2}$ as often mentioned before.
3. Consider the Habiro expansion of this polynomial and take the first i terms.
4. The congruence class of these first i terms in $\mathbb{Z}[q]/(Q_i(q))$ will be the image of m by f_{ij}.

We now should have a clear idea of what the mapping f_{ij} actually does. By our definition of this mapping we clearly see that it satisfies $f_{ij}(1) = 1$, $f_{ij}(x+y) = f_{ij}(x) + f_{ij}(y)$ and $f_{ij}(xy) = f_{ij}(x)f_{ij}(y)$. Therefore the mapping f_{ij} is a homomorphism. By the fact that f_{ii} is clearly the identity mapping and $f_{ik} = f_{ij} \circ f_{jk}$ for all $i \leq j \leq k$ by our definition of the mappings f_{ab}, we have that $((\mathbb{Z}[q]/(Q_n(q)))_{n\in\mathbb{N}}, (f_{ij})_{i\leq j\in\mathbb{N}})$ is a inverse system of rings and homomorphisms, as defined in Definition 4.1.
We now would like to actually take the inverse limit of $n \to \infty$, obtaining the Habiro ring. But if we look again at Definition 4.2 we see that, apart from the ring $X = \widehat{\mathbb{Z}[q]}$, we should also have projections $\pi_n : \widehat{\mathbb{Z}[q]} \to \mathbb{Z}[q]/(Q_n(q))$ for each $n \in \mathbb{N}$. Also by definition, these projections are given by $m \mapsto m \pmod{Q_n(q)}$, strikingly similar to the homomorphism f_{ij} used in the projective limit. By the above reasoning we also easily see that these projections are homomorphisms, and satisfy $\pi_i = f_{ij} \circ \pi_j$ for $i \leq j$. But the question arises what the elements of the Habiro ring look like. Similarly to the p-adic completion of integers and the Φ_n-adic completion of $\mathbb{Z}[q]$, we suggest that the elements of Habiro ring are finite or infinite Habiro expansions, that is, every element $m \in \widehat{\mathbb{Z}[q]}$ can be uniquely written as

$$m(q) = \sum_{n=0}^{\infty} m_n(q)Q_n(q) \tag{4.10}$$

with $m_n \in \mathbb{Z}[q]$ and $deg(m_n) \leq n$ for all $n \in \mathbb{N}_0$. In this way we can describe the projections π_n $(n \geq 1)$ as follows

1. Take an element $m \in \widehat{\mathbb{Z}[q]}$, which is in fact some kind of congruence class, but it can be represented as an infinite Habiro expansion given in Equation 4.10.
2. Consider this Habiro expansion and take the first n terms.
3. The congruence class of the first n terms in $\mathbb{Z}[q]/(Q_n(q))$ is the image of f under the projection π_i.

Therefore we see that the restrictions on the degree of the coefficients in the infinite Habiro expansion are quite obvious, since the restrictions also hold for all finite Habiro expansions and the projections map the infinite Habiro expansions to finite expansion. Let us now prove the next lemma.

Lemma 4.3. *Every element m of the Habiro ring can be written as $\sum_{n=0}^{\infty} m_n(q)Q_n(q)$ and this expansion is unique.*

Proof. Assume to the contrary that there is an element $m \in \widehat{\mathbb{Z}[q]}$ that cannot be written as a Habiro expansion. Obviously $\pi_n(m)$ is defined for each $n \in \mathbb{N}$. Now define $\bar{m} \in \widehat{\mathbb{Z}[q]}$ as

$$\bar{m}(q) = \lim_{n\to\infty} \pi_n(m) = \sum_{n=0}^{\infty} m_n(q)Q_n(q) \tag{4.11}$$

where $m_0(q) = \pi_1(m)$, $m_1(q) = \frac{\pi_2(m)-m_0(q)}{Q_1(q)}$, etcetera. Clearly $\bar{m}$ is a Habiro expansion. Since m cannot be written as a Habiro expansion, we certainly have $m \neq \bar{m}$, therefore there must be a smallest $n \geq 0$ such that $\pi_n(m) \neq \pi_n(\bar{m})$. This is clearly a contradiction with the definition of $\bar{m}$ in Equation 4.11.
Now we will prove that there is only one way to write m as a Habiro expansion. We already observed this fact while discussing the finite Habiro expansions defined in Section 3.3. Suppose that there is an element $m \in \widehat{\mathbb{Z}[q]}$, that can be written as a Habiro expansion in two different ways $\bar{m}$ and $\hat{m}$. Then there has to be a smallest $n \in \mathbb{N}_0$ such that $\bar{m}_n(q) \neq \hat{m}_n(q)$. Then $\pi_n(\bar{m}) \neq \pi_n(\hat{m})$, which is a contradiction, since $0 = \pi_n(0) = \pi_n(\bar{m} - \hat{m}) \neq 0$, by the fact that π_n is a homomorphism for each $n \in \mathbb{N}$. □

If we take a closer look at Equation 4.10 we see that there are in fact many elements in $\widehat{\mathbb{Z}[q]}$, that are not defined in $\mathbb{Z}[q]$, since this infinite sum does not converge. But we can observe that all elements of $\widehat{\mathbb{Z}[q]}$ have a clear, well defined value at all roots of unity. Choose ζ to be a root of unity with order $ord(\zeta)$. Then $Q_{ord(\zeta)}(\zeta) = (1-\zeta)(1-\zeta^2)\cdots(1-\zeta^{ord(\zeta)}) = 0$. By Equation 3.8 we see that $Q_n \mid Q_k$ for all $k \geq n$. Therefore we have $Q_k(\zeta) = 0$ for all $k \geq ord(\zeta)$. This results in

$$m(\zeta) = \left[\sum_{n=0}^{ord(\zeta)-1} m_n(\zeta)Q_n(\zeta) \right] \tag{4.12}$$

Since all coefficients of the Habiro expansion of m are polynomials with integer coefficients, we therefore have $m_n(\zeta), Q_n(\zeta) \in \mathbb{Z}[\zeta]$ for all $0 \leq n < ord(\zeta)$. Thus the next corollary follows.

Corollary 4.4. *Let m be an element of $\widehat{\mathbb{Z}[q]}$ and ζ be a root of unity. Then we have $m(\zeta) \in \mathbb{Z}[\zeta]$.*

In the Φ_n-adic completion of $\mathbb{Z}[q]$ we see that all elements have a well defined value at only certain roots of unity, namely the primitive nth roots of unity. Then the values of the elements just equal the constant term in their Φ_n-adic expansion. Since we do not deal with polynomial in the ring of p-adic integers, we do not see something similar in that projective limit.

Now let us turn back to the projections π_n. If all elements of the Habiro ring can be represented as a Habiro expansion, such as in Equation 4.10, we certainly see that for each $m \in \mathbb{Z}[q]/(Q_n(q))$, the unique polynomial of degree $< \frac{n(n+1}{2}$ in m is an element of $\widehat{\mathbb{Z}[q]}$. This is because the Habiro ring also contains all finite Habiro expansions, by taking all coefficients m_i equal to 0 for $i \geq n$. Therefore the mappings π_n are clearly surjective, as are the mappings f_{nj} ($n \leq j$ by the same reasoning.
Both families of mappings are clearly not injective (for $n \neq j$, by the fact that the elements $m, m + Q_n \in \mathbb{Z}[q]/(Q_j(q)), \widehat{\mathbb{Z}[q]}$ are both mapped to $m \in \mathbb{Z}[q]/(Q_n(q))$ by our definition of the mapping. By the fact that these mappings are surjective, we also see that we can easily construct an element $m \in \widehat{\mathbb{Z}[q]}$. We can choose m_0 as a constant in $\mathbb{Z}$, $m_1(q)$ as a polynomial in $\mathbb{Z}[q]$ with $deg(m_1) \leq 1$ and so on.
We will summarize all these observations in the next theorem.

Theorem 4.5. *Let m be an element of the Habiro ring. Then it can be uniquely written as a Habiro expansion, that is*

$$m = \sum_{n=0}^{\infty} m_n(q) Q_n(q) \tag{4.13}$$

with $m_n \in \mathbb{Z}[q]$ and $deg(m_n) \leq n$. The value $m(\zeta)$ is well defined for ζ a root of unity. Furthermore all elements of the form $\sum_{n=0}^{\infty} m_n(q)Q_n(q)$ with m_n as above, are in fact elements of the Habiro ring.

The Habiro ring is often called the cyclotomic completion of $\mathbb{Z}[q]$, similarly to the ring $\mathbb{Z}[q]^{\{n\}}$ being the Φ_n-adic completion of $\mathbb{Z}[q]$. Similar in the ring $\mathbb{Z}[q]^{\{n\}}$ the elements are only all defined at the roots of Φ_n; therefore it has the name Φ_n-adic completion of $\mathbb{Z}[q]$.
One remarkable property of the Habiro ring is that q has an inverse in $\widehat{\mathbb{Z}[q]}$, in contrast with $\mathbb{Z}[q]$, where only ± 1 are units. We have indeed

$$\begin{aligned} q \sum_{n=0}^{\infty} q^n Q_n(q) &= \sum_{n=0}^{\infty} q^{n+1} Q_n(q) = \sum_{n=0}^{\infty} (1 - (1 - q^{n+1})) Q_n(q) \\ &= \sum_{n=0}^{\infty} (Q_n(q) - Q_{n+1}(q)) = Q_0(q) = 1 \end{aligned} \tag{4.14}$$

and therefore $q^{-1} = \sum_{n=0}^{\infty} q^n Q_n(q)$. Therefore all positive powers of q have an inverse element in $\widehat{\mathbb{Z}[q]}$, that is $\pm q^{-k} = \pm(\sum_{n=0}^{\infty} q^n Q_n(q))^k$ for all $k \in \mathbb{N}_0$ by the fact that the inverse of ± 1 is ± 1 respectively. It is thought, but not yet proven, that plus or minus the powers of q are the only elements in $\widehat{\mathbb{Z}[q]}$ with an inverse element.

4.4 A mapping from $\mathbb{Z}[q]$ to $\widehat{\mathbb{Z}[q]}$

So far, in the two examples and the Habiro ring, we did not consider the last condition; that is, the existence of a homomorphism $u : Y \to X$ for a projective limit X and some specified rings Y, as seen in Definition 4.2.
In the case of the Habiro ring, it turns out that $\mathbb{Z}[q]$ satisfies the properties of Y, with the homomorphisms $\psi_n : \mathbb{Z}[q] \to \mathbb{Z}[q]/(Q_n(q))$ given by $m \mapsto m \pmod{Q_n(q)}$. Really interesting is the mapping u between $\mathbb{Z}[q]$ and $\widehat{\mathbb{Z}[q]}$, which has to be a homomorphism by the definition. It seems quite natural to take the mapping which maps $m \in \mathbb{Z}[q]$ to its (finite) Habiro expansion. Since this mapping is in fact some kind of identity mapping (it maps m to m, written in another way), it is obviously a homomorphism, thus satisfying Definition 4.2. But the question arises how to construct this mapping. As in Section 3.3, we could try and use the Euclidean division algorithm to find all the polynomials m_i, starting with the highest i with non-zero term, but this forces us to calculate Q_n for each $n \in \mathbb{N}$, which is not required. There is another algorithm to find the (finite) Habiro expansion of a polynomial m. It uses the following other notation of the Habiro expansion.

$$\begin{aligned} m(q) &= m_0 + m_1(q)Q_1(q) + m_2(q)Q_2(q) + m_3(q)Q_3(q) + ... \\ &= m_0 + (1-q)[m_1(q) + m_2(q)(1-q^2) + m_3(q)(1-q^2)(1-q^3) + ...] \\ &= m_0 + (1-q)[m_1(q) + (1-q^2)[m_2(q) + (1-q^3)[m_3(q) + ...]]] \end{aligned} \tag{4.15}$$

The algorithm is as follows

1. Write $m(q) = h_1(q)(1-q) + r_0$ with $deg(r_0) < 1$, as in the Euclidean division algorithm.
2. From the above discussion we see $r_0 = m_0$.
3. If $h_1(q) \neq 0$, we write $h_1(q) = h_2(q)(1-q^2) + r_1(q)$ with $deg(r_1) < 2$.
4. We again see $r_1(q) = m_1(q)$.
5. Repeat the previous two steps, always increasing all non-zero numbers with 1, that is, first test if $h_k(q) \neq 0$. Then write $h_k(q) = h_{k+1}(q)(1-q^{k+1}) + r_k(q)$ with $deg(r_k) < k+1$, and state $r_k(q) = m_k(q)$. Then take $k = k+1$ and repeat the cycle.

We can also use this algorithm to calculate the finite terms of an infinite Habiro expansion, which clearly cannot be done using the Euclidean division algorithm, where we had to find the highest i with non-zero term m_i. We also do not have to calculate all Q_n explicitly. We use this algorithm in the next example.

Example 4.2. As in Example 3.3 we want to examine the Habiro expansion of the polynomial $m(q) = 8 - 5q + 6q^2 - 2q^4 - 2q^5 + q^6 + 2q^7 - q^8$. Using a computer or using old-school long divison on paper we obtain

$$m(q) = (q^7 - q^6 - 2q^5 + 2q^3 + 2q^2 - 4q + 1)(1-q) + 7 \tag{4.16}$$

Therefore we obtain $m_0 = 7$ and $h_1(q) = q^7 - q^6 - 2q^5 + 2q^3 + 2q^2 - 4q + 1$. We again use the Euclidean division algorithm, but this time we divide $h_1(q)$ by $1 - q^2$, giving

$$h_1(q) = (-q^5 + q^4 + q^3 + q^2 - q - 1)(1 - q^2) - 3q + 2 \tag{4.17}$$

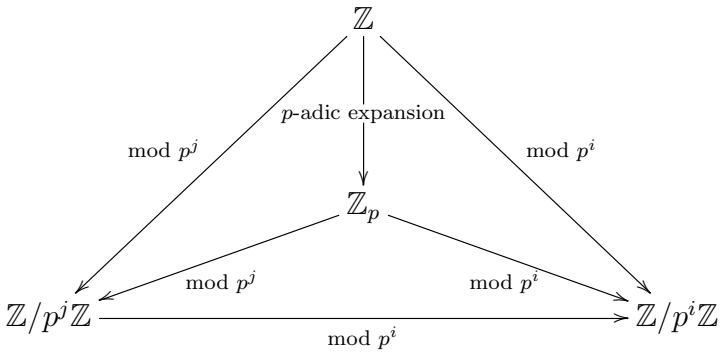
Therefore we obtain $m_1(q) = -3q + 2$ and $h_2(q) = -q^5 + q^4 + q^3 + q^2 - q - 1$. We use the division algorithm twice more to see

$$h_2(q) = (q^2 - q - 1)(1 - q^3) + 0 = h_3(q)(1 - q^3) \tag{4.18}$$

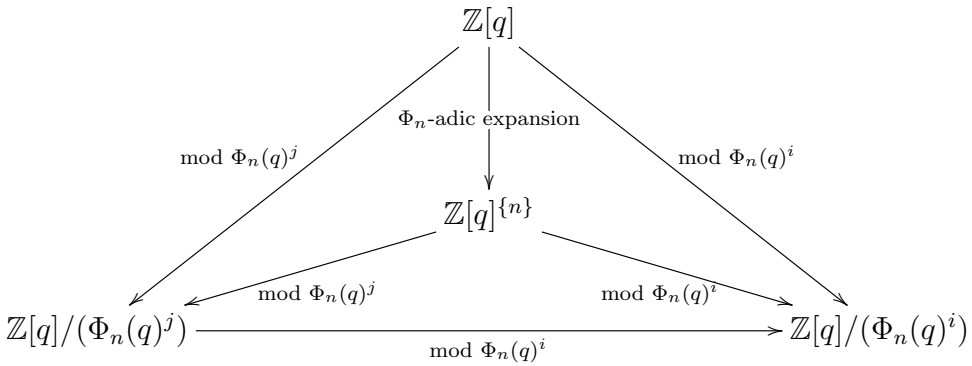
$$h_3(q) = 0(1 - q^4) + q^2 - q - 1 \tag{4.19}$$

This results in $m_2(q) = 0$ and $m_3(q) = q^2 - q - 1$, and thus we get the same Habiro expansion as in Equation 3.19 of Example 3.3.

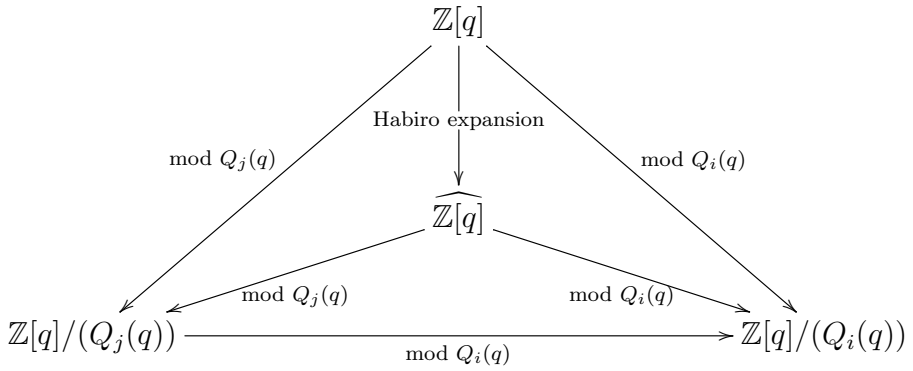
In our examples of the p-adic integers and the Φ_n-adic completion of $\mathbb{Z}[q]$, we also did not discuss the specific rings Y. In fact, there is a homomorphism between $\mathbb{Z}$ and the ring of p-adic integers, sending an integer to its finite p-adic expansion.
Similarly, there is a homomorphism between $\mathbb{Z}[q]$ and $\mathbb{Z}[q]^{\{n\}}$, which maps a polynomial in $\mathbb{Z}[q]$ to its Φ_n-adic expansion. We therefore conclude that the rings $\widehat{\mathbb{Z}[q]}$, $\mathbb{Z}[q]^{\{n\}}$ and $\mathbb{Z}_p$ are in some ways very similar.
We can now extend the diagrams of the projective limits of these systems. For the ring of p-adic integers we have



For the Φ_n-adic completion of $\mathbb{Z}[q]$ we have



Finally, for the Habiro ring $\widehat{\mathbb{Z}[q]}$ we have



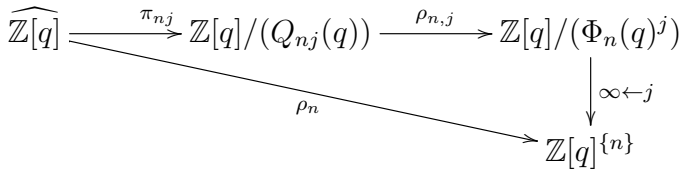
4.5 A mapping from $\widehat{\mathbb{Z}[q]}$ to $\mathbb{Z}[q]^{\{n\}}$

Since there is are homomorphisms from $\mathbb{Z}[q]$ to both $\widehat{\mathbb{Z}[q]}$ and $\mathbb{Z}[q]^{\{n\}}$, we could try and find a mapping $\rho_n : \widehat{\mathbb{Z}[q]} \to \mathbb{Z}[q]^{\{n\}}$, to make the triangle some kind of 'complete'. Since an element m of the Habiro ring has a well defined value at all primitive nth roots of unity, it seems logical to expect this element m to have a Φ_n-adic expansion. By Corollary 2.8 we have $Q_k(q) = (-1)^k \prod_{j=1}^{k} \Phi_j(q)^{\lfloor \frac{k}{j} \rfloor}$ and therefore $\Phi_n(q)^{\lfloor \frac{k}{n} \rfloor}$ is the highest power of Φ_n which divides Q_k. Therefore we have

$$m(q) = \sum_{i=0}^{n-1} m_i(q)Q_i(q) + \Phi_n(q) \sum_{i=n}^{2n-1} \left(m_i(q) \frac{Q_i(q)}{\Phi_n(q)} \right) + \Phi_n(q)^2 \sum_{i=2n}^{3n-1} \left(m_i(q) \frac{Q_i(q)}{\Phi_n(q)^2} \right) + ... \tag{4.20}$$

This may seem like a proper Φ_n-adic expansion for m, but it is certainly not. Since $deg(m_{n-1}(q)Q_{n-1}(q)) \leq (n-1) + \frac{(n-1)n}{2}$, it is possible to have $deg(m_{n-1}(q)Q_{n-1}(q)) \geq \phi(n)$ for $n \geq 2$. Therefore we can write $m_{n-1}(q)Q_{n-1}(q) = a(q)\Phi_n(q) + b(q)$ with $a, b \in \mathbb{Z}[q]$ and a non-zero, by the Euclidean division algorithm. This means that the first sum in Equation 4.20 can also contain a non-zero term with Φ_n. We will come back to this problem in a moment.

Introduce the mapping $\rho_{n,j}$ for all $n, j \in \mathbb{N}$ which takes an element m of the Habiro ring and maps it to $\mathbb{Z}[q]/(\Phi_n(q)^j)$, by computing the remainder of m after division by $\Phi_n(q)^j$. This mapping is again a homomorphism. The question arises how to do this. We see that all terms $m_i(q)Q_i(q)$ in the Habiro expansion of m with $i \geq jn$ are divisible by $\Phi_n(q)^j$, so only the first jn terms of the Habiro expansion are interesting for this mapping $\rho_{n,j}$. Therefore we can see $\rho_{n,j}$ as mapping m to the first jn terms of its Habiro expansion (in $\mathbb{Z}[q]/(Q_{nj}(q))$ and then compute the remainder modulo $\Phi_n(q)^j$. Thus we can see $\rho_{n,j}$ as a mapping from $\mathbb{Z}[q]/(Q_{nj}(q))$ to $\mathbb{Z}[q]/(\Phi_n(q)^j)$. If we increase j and eventually take the projective limit $j \to \infty$ we obtain a mapping ρ_n from $\widehat{\mathbb{Z}[q]}$ to $\mathbb{Z}[q]^{\{n\}}$, which is again clearly a homomorphism. All these observations are summarized in the next diagram.



We see that, if the Φ_n-adic expansion of m exists, $\rho_{n,j} \circ \pi_{nj}$ maps m to the first j terms of this Φ_n-adic expansion. We will now prove the next theorem.

Theorem 4.6. *Let $n \in \mathbb{N}$. Then there exists an injective homomorphism $\rho_n : \widehat{\mathbb{Z}[q]} \to \mathbb{Z}[q]^{\{n\}}$ which maps each element $m \in \widehat{\mathbb{Z}[q]}$ to its unique Φ_n-adic expansion, that is $m(q) \mapsto \sum_{j=0}^{\infty} a_j(q)\Phi_n(q)^j = m(q)$ with $a_j \in \mathbb{Z}[q]$ and $deg(a_j) < \phi(n)$.*

Proof. By the fact that the ρ_n should be an injective homomorphism, the kernel of ρ_n should only contain 0. Assume to the contrary that there is an element $m \in \widehat{\mathbb{Z}[q]}$ which is mapped to $0 \in \mathbb{Z}[q]^{\{n\}}$. Then, using the diagram, we obviously have $\rho_{n,j} \circ \pi_{nj}(m) = 0$ for all $j \in \mathbb{N}$. Now take a look back at our 'false' Φ_n-adic expansion in Equation 4.20. If we take $j = 1$ we see $\Phi_n \mid m$ and therefore $\Phi_n(q) \mid \sum_{i=0}^{n-1} m_i(q)Q_i(q)$. Using this we can rewrite

$$m(q) = \Phi_n(q)\left(\frac{\sum_{i=0}^{n-1} m_i(q)Q_i(q)}{\Phi_n(q)} + \frac{\sum_{i=n}^{2n-1} m_i(q)Q_i(q)}{\Phi_n(q)}\right) + \Phi_n(q)^2 \sum_{i=2n}^{3n-1}\left(m_i(q)\frac{Q_i(q)}{\Phi_n(q)^2}\right) + ... \tag{4.21}$$

Now increase j to 2, to obtain $\Phi_n^2 \mid m$ from the fact that $\rho_{n,2} \circ \pi_{2n}(m) = 0$. Therefore we have again $\Phi_n(q)^2 \mid \left(\Phi_n(q)\left(\frac{\sum_{i=0}^{n-1} m_i(q)Q_i(q)}{\Phi_n(q)} + \frac{\sum_{i=n}^{2n-1} m_i(q)Q_i(q)}{\Phi_n(q)}\right)\right)$, which results in

$$m(q) = \Phi_n(q)^2\left(\frac{\sum_{i=0}^{2n-1} m_i(q)Q_i(q)}{\Phi_n(q)^2} + \frac{\sum_{i=2n}^{3n-1} m_i(q)Q_i(q)}{\Phi_n(q)^2}\right) + ... \tag{4.22}$$

We can continue this process to see that m is divisible by $\Phi_n(q)^j$ for arbitrary high $j \in \mathbb{N}$. Therefore m must be equal to 0.
Since this homomorphism is injective we see that each element of $\widehat{\mathbb{Z}[q]}$ is mapped to a unique element in $\mathbb{Z}[q]^{\{n\}}$, which clearly has a Φ_n-adic expansion. The finite terms of the Φ_n-adic expansion of m are given by $\rho_{n,j} \circ \pi_{nj}(m)$ for each $j \in \mathbb{N}$. □

Example 4.3. For example, let us consider the infinite sum $m(q) = \sum_{n=0}^{\infty} Q_n(q)$, which is clearly an element of the Habiro ring. Since the cyclotomic polynomial $\Phi_n(q)$ divides $Q_k(q)$ exactly $\lfloor \frac{k}{n} \rfloor$ times, the Φ_n-adic expansion of m is given by

$$m(q) = (1 + Q_1(q) + ... + Q_{n-1}(q)) + \Phi_n(q)\frac{Q_n(q) + Q_{n+1}(q) + ... + Q_{2n-1}(q)}{\Phi_n(q)} + \Phi_n(q)^2\frac{Q_{2n}(q) + Q_{2n+1}(q) + ... + Q_{3n-1}(q)}{\Phi_n(q)^2} + ...$$

5 Unique identification with values at the roots of unity

In the previous section we already mentioned that all elements of the Habiro ring have well defined values in $\mathbb{C}$ at all roots of unity. We will denote the set of all roots of unity by $Z^{\bar{\mathbb{Q}}}$. As mentioned in the introduction, it even turns out that the elements are uniquely determined by their values at a certain subset of the roots of unity. This whole section will be devoted to prove this statement.

Example 5.1. In $\mathbb{R}[q]$ and $\mathbb{Z}[q]$, we know that a polynomial f of degree n is uniquely determined by its values $f(x)$ at $n+1$ different points x. For example, if we have $f(0)=1$, $f(1)=2$ and $f(2)=5$ for a polynomial of degree 2, $f(q)=q^2+1$.
This maybe seems quite irrelevant, since it is familiar to use that polynomials are uniquely detemermined by its (function) values. But this is not the case in each ring. If we take for example the polynomial q^p-q over the finite field with p elements $\mathbb{F}_p$. Since $x^p=x$ for all elements in this finite field, we have $q^p-q=0$ on $\mathbb{F}_p$, but it is not identically to the 0-polynomial. Therefore we see that values do not uniquely determine the coefficients in some cases.

We will make our previous statement more formal.

Theorem 5.1. *Let Z be a subset of the set all roots of unity $Z^{\bar{\mathbb{Q}}}$ containing infinitely many elements of prime power order, that is, of order $p_i^{k_i}$ for some prime p_i and $k_i \in \mathbb{N}$. Denote $P_Z = \prod_{\zeta\in Z}\mathbb{Z}[\zeta]$. Then the mapping $\epsilon_Z : \widehat{\mathbb{Z}[q]} \to P_Z$ given by $m(q) \mapsto (m(\zeta))_{\zeta\in Z}$ is an injective homomorphism.*

We will first prove that this mapping is a homomorphism. The value of the function 1 is 1 at all roots of unity. Since all elements of the Habiro ring have well defined values at all roots of unity ζ, we have $m(\zeta)=\sum_{i=0}^{ord(\zeta)-1} m_i(\zeta)Q_i(\zeta)$ for all elements m. Thus we see easily $m(\zeta)+n(\zeta)=(m+n)(\zeta)$ and $m(\zeta)n(\zeta)=(mn)(\zeta)$. Therefore all conditions for a ring homomorphism are satisfied.
Proving the fact that this mapping is injective is a lot harder. We therefore decompose the mapping ϵ_Z into two separate mappings as displayed in the diagram.

$$\begin{array}{ccccc} \widehat{\mathbb{Z}[q]} & \xrightarrow{\sigma_{N_Z}} & P_{N_Z} & \xrightarrow{\gamma_Z} & P_Z \\ {\scriptstyle \rho_n}\downarrow & & & & \\ \mathbb{Z}[q]^{\{n\}} & & & & \end{array}$$

The mappings are in fact given by

- $\sigma_T : \widehat{\mathbb{Z}[q]} \to P_T$ for all $T \subset \mathbb{N}$ where $P_T = \prod_{t\in T}\mathbb{Z}[q]/(\Phi_t(q))$ given by $m(q) \mapsto (m(q) \pmod{\Phi_t(q)})_{t\in T}$.
- $\gamma_Z : P_{N_Z} \to P_Z$ for all $Z \subset Z^{\bar{\mathbb{Q}}}$ and $N_Z = \{ord(\zeta) | \zeta \in Z\}$. The mapping is defined as $\gamma((m_n(q))_{n\in N_Z}) = (m_n(\zeta))_{\zeta\in Z}$.

5.1 Injectivity of σ_T

We first pose the theorem to be proven in this section. We do not take $T \subset \mathbb{N}$ to be N_Z in this case, but prove a more general statement.

Theorem 5.2. *For any $T \subset \mathbb{N}$ containing infinitely many prime powers, the mapping $\sigma_T : \widehat{\mathbb{Z}[q]} \to P_T$ given by $m(q) \mapsto (m(q) \pmod{\Phi_t(q)})_{t\in T}$ is injective.*

Proof. Suppose to the contrary that this mapping is not injective. Then we know that the kernel does not consist only of the zero element of the Habiro ring. In other words, there is an non-zero element $m \in \widehat{\mathbb{Z}[q]}$ such that $\sigma_T(m) = 0$.
We now recall the mapping $\rho_n : \widehat{\mathbb{Z}[q]} \to \mathbb{Z}[q]^{\{n\}}$ from Section 4.5 given by $m(q) \mapsto \sum_{j=0}^{\infty} a_j(q)\Phi_n(q)^j$ with $a_j \in \mathbb{Z}[q]$ and $deg(a_j) < \phi(n)$. This mapping is just a Φ_n-adic expansion of m. By Theorem 4.6 we know that this mapping is injective and therefore $\rho_n(m) \neq 0$ and we can write $\rho_n(m) = \sum_{j=0}^{\infty} a_j(q)\Phi_n(q)^j$, where $a_l(q) \neq 0$ for at least one $l \in \mathbb{N}_0$.
Since $\sigma_T(m) = 0$ we have by definition of σ_T that $m(q) \equiv 0 \pmod{\Phi_t(q)}$ for all $t \in T$ and therefore $\Phi_t \mid m$. If we denote the (infinitely many) prime powers in T by $r_1, r_2, ...$, where $r_i < r_{i+1}$ for all i, we claim to have $\Phi_{r_1}\Phi_{r_2}\cdots\Phi_{r_k} \mid m$ for every $k \geq 1$. Since we have already proven the case $k = 1$ above, we suppose $k \geq 2$. Assume that $\Phi_{r_1}\Phi_{r_2}\cdots\Phi_{r_{k-1}} \mid m$. Then we can write

$$m(q) = \Phi_{r_1}(q)\Phi_{r_2}(q)\cdots\Phi_{r_{k-1}}(q)d(q) \tag{5.1}$$
$$= \Phi_{r_1}(q)\Phi_{r_2}(q)\cdots\Phi_{r_{k-1}}(q)(b(q) + \Phi_{r_k}(q)c(q)) \tag{5.2}$$

with $b, c, d \in \widehat{\mathbb{Z}[q]}$.
We obtain the last equation by taking $b(q) \equiv d(q) \pmod{\Phi_{r_k}(q)}$. Following the last equation and the fact that $\Phi_{r_k} \mid m$, we see: $\Phi_{r_k} \mid \Phi_{r_1}\Phi_{r_2}\cdots\Phi_{r_{k-1}}b$. We also have $\Phi_{r_k}(\zeta_{r_k}) = 0$ for ζ_{r_k} a primitive r_kth root of unity. Thus we obtain the equation:

$$\Phi_{r_1}(\zeta_{r_k})\Phi_{r_2}(\zeta_{r_k})\cdots\Phi_{r_{k-1}}(\zeta_{r_k})b(\zeta_{r_k}) = 0 \tag{5.3}$$

Using the fact that $r_i < r_k$ for all $i < k$, we have that ζ_{r_k} is not a r_i-th root of unity and therefore $\Phi_{r_i}(\zeta_{r_k}) \neq 0$ for $i = 1, 2, ..., k-1$. Thus we obtain by Equation 5.3 that $b(\zeta_{r_k}) = 0$. Since ζ_{r_k} is a zero of b, we know that the minimal polynomial of ζ_{r_k} must be a divisor of b. Since the minimal polynomial of a root of unity is its cyclotomic polynomial Φ_{r_k}, we have $\Phi_{r_k} \mid b$ and therefore we obtain from Equation 5.2 $\Phi_{r_1}\Phi_{r_2}\cdots\Phi_{r_k} \mid m$, as requested.
We already observed that $\rho_n(m)$ is just the Φ_n-adic expansion of m, that is, we are writing m in a base consisting of powers of Φ_n instead of product of powers of q and the polynomial Q_j. Therefore, $\rho_n(m)$ is still divisible by the same polynomials, and therefore also by $\Phi_{r_1}\Phi_{r_2}\cdots\Phi_{r_k}$.
Furthermore we have $\Phi_1(q)^l \mid m$ by definition of l in the beginning of this proof. We observe that 1 is the only zero of $\Phi_1(q)^l$ and is not a zero of $\Phi_{r_1}\Phi_{r_2}\cdots\Phi_{r_k}$ by the fact that 1 is a first root of unity and $\Phi_{r_1}\Phi_{r_2}\cdots\Phi_{r_k}$ has precisely the r_1st, r_2nd, ..., r_kth roots of unity as its zeroes with $r_1, r_2, ..., r_k$ prime powers, which are therefore greater than or equal to 2. Since $\Phi_1(q)^l = (q-1)^l$ is monic and $\Phi_{r_1}\Phi_{r_2}\cdots\Phi_{r_k}$ is a product of monic polynomials, we have $gcd(\Phi_1(q)^l, \Phi_{r_1}\Phi_{r_2}\cdots\Phi_{r_k}) = 1$. Since both divide $\rho_n(m)$, we must also have $\Phi_{r_1}\Phi_{r_2}\cdots\Phi_{r_k} \mid \frac{m(q)}{\Phi_1(q)^l}$.

For simplicity we will define $\bar{m}(q) = \frac{m(q)}{\Phi_1(q)^l}$. By Corollary 2.11 we obtained $\Phi_{r_i} \in (p_i, \Phi_1)$ for each i. Therefore we can write $\Phi_{r_i}(q) = v_i(q)p_i + w_i(q)\Phi_1$ for some $v_i, w_i \in \mathbb{Z}[q]$. Thus we have for each $k \geq 1$ the following equation

$$\Phi_{r_1}(q) \cdots \Phi_{r_k}(q) = v_1(q) \cdots v_k(q)p_1 \cdots p_k + \Phi_1 s(q) \tag{5.4}$$

Here s is a unique polynomial in $\mathbb{Z}[q]$. We now see $\Phi_{r_1}\Phi_{r_2} \cdots \Phi_{r_k} \in (p_1 p_2 \cdots p_k, \Phi_1)$ and by the fact that $\Phi_{r_1}\Phi_{r_2} \cdots \Phi_{r_k} \mid \bar{m}$, we have $\bar{m} \in (p_1 p_2 \cdots p_k, \Phi_1)$.
Now take a look back at the Φ_n-adic expansion of m and take $n = 1$, which gives $\Phi_1(q) = q - 1$. Then we see $\bar{m}(q) = \frac{\rho_1(m)}{\Phi_1(q)^l} = \sum_{j=0}^{\infty} a_{j+l}\Phi_1(q)^j$. Since $a_{j+l}\Phi_1(q)^j \in (\Phi_1(q)) \subset (p_1 p_2 \cdots p_k, \Phi_1)$ for all $j \geq 1$ and $\bar{m} \in (p_1 p_2 \cdots p_k, \Phi_1)$ we also have $a_l = \bar{m}(q) - \sum_{j=1}^{\infty} a_{j+l}\Phi_1(q)^j \in (p_1 p_2 \cdots p_k, \Phi_1)$.
By the fact that a_l is a number, we cannot have $\Phi_1 \mid a_l$ unless $a_l = 0$ and we must have $p_1 p_2 \cdots p_k \mid a_l$. Now we claim that $a_l = 0$. Suppose to the contrary that $a_l \neq 0$. Then there is a $t \in \mathbb{N}_0$ such that $2^t \leq |a_l| < 2^{t+1}$. From the above result we have $p_1 p_2 \cdots p_{t+1} \mid a_l$. But, since 2 is the smallest prime, we obtain $p_1 p_2 \cdots p_{t+1} \geq 2^{t+1} > |a_l|$. Therefore, it is impossible to have $p_1 p_2 \cdots p_{t+1} \mid a_l$ unless $a_l = 0$.
This is a contradiction and thus we have proven the theorem. □

5.2 Injectivity of γ_Z

In Theorem 5.1 was stated that Z should be a subset of the set all roots of unity containing infinitely many elements of prime power order. A bit further we defined $N_Z = \{ord(\zeta) \mid \zeta \in Z\}$. Consequently we see that $N_Z \subset \mathbb{N}$ is containing infinitely many prime powers, and thus N_Z is satisfying the conditions of T in Theorem 5.2. Now will we prove the injectivity of γ_Z

Theorem 5.3. *Let Z be a subset of the set all roots of unity $Z^{\bar{\mathbb{Q}}}$ containing infinitely many elements of prime power order and N_Z be defined as above, then the mapping: $\gamma_Z : P_{N_Z} \to P_Z$ defined as $\gamma((m_n(q))_{n \in N_Z}) = (m_n(\zeta))_{\zeta \in Z}$ is injective.*

Proof. An element of P_{N_Z} contains an element of $\mathbb{Z}[q]/(\Phi_n(q))$ for each unique number n, which is an order of a root of unity $\zeta \in Z$. The mapping γ_Z evaluates the element of $\mathbb{Z}[q]/(\Phi_n(q))$ in all $\zeta \in Z$ with order n, and does this for all $n \in N_Z$. Therefore we observe that γ_Z is the direct product of the mapping $\mathbb{Z}[q]/(\Phi_n(q)) \to \prod_{\zeta \in Z, ord(\zeta)=n} \mathbb{Z}[\zeta]$, given by $m(q) \mapsto (m(\zeta))_{\zeta \in Z, ord(\zeta)=n}$. We claim that this mapping is a injective homomorphism. The homomorphism property can be obtained very quickly, since 1 is mapped to 1 (the order of 1 as root of unity is 1), and the product and addition structure is preserved. If there is one ζ of order n such that $m(\zeta) = 0$, then by definition ζ is a zero of f and thus the minimal polynomial of ζ, the cyclotomic polynomial $\Phi_n(q)$, divides f. Since $m(q) \in \mathbb{Z}[q]/(\Phi_n(q))$, we have $m(q) = 0$. Therefore, if $(f(\zeta)) = 0$ for any ζ we have $m(q) = 0$. Thus the kernel consist of only the 0-function, and the homomorphism is injective.
Since γ_Z is the direct product of these injective homomorphisms, it is also injective and the theorem is proven. □

We now conclude with the proof of Theorem 5.1

Proof. We already stated that the mapping ϵ_Z is a homomorphism. Furthermore we see that: $\epsilon_Z = \gamma_Z \circ \sigma_{N_Z}$ and both are injective mappings for Z satisfying the conditions of the theorem. Thus is ϵ_Z an injective homomorphism. □

The consequences of this theorem might not be clear directly. But, by the fact that functions are determined by their function values, it means that we can regard the elements of the Habiro ring as functions. We see, in contrary to the polynomial $q^p - q$ over $\mathbb{F}_p$, that a element of the Habiro ring is equal to 0 if it is 0 at a certain set of points. This is one of the most important properties of the Habiro ring, and therefore Habiro used it in his description of the ring, quoted in the introduction. To actually do (function) analysis on these elements, we need to introduce differentiation on elements of the Habiro ring, but we will not further discuss that.

References

[1] K. Habiro, Cyclotomic Completions of Polynomial Rings, *Publ. IRMS, Kyoto University*, **40** (2004), 1127-1146.

[2] C.W.K. Lo, M. Marcolli. $\mathbb{F}_\zeta$-geometry, take motives and the Habiro ring, arXiv:1310.2261.

[3] G.J.O. Jameson, The cyclotomic polynomials, *Departement of Mathematics and Statistics, Lancaster University*, http://www.maths.lancs.ac.uk/∼jameson/cyp.pdf.

[4] F. Beukers, Dictaat Rings and Galois Theory, *Departement of Mathematics, Utrecht University*.

[5] P. Morandi, *Field and Galois Theory*, Springer-Verlag, New York, 1996.

[6] J. Shurman, Cyclotomic polynomials. *Departement of Mathematics, Reed College*, http://people.reed.edu/∼jerry/332/21cyclo.pdf.

[7] http://en.wikipedia.org/wiki/Inverse limit, diagram.