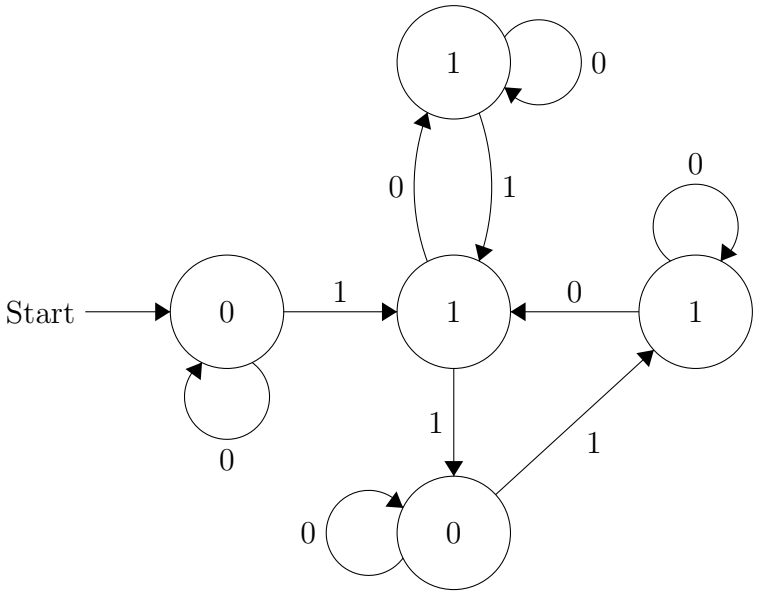
Automata and finite order elements in the Nottingham group



Djurre Tijsma
July 9, 2018

Master's thesis
Supervisor: prof. dr. Gunther Cornelissen
Second reader: prof. dr. Frits Beukers

Utrecht University

Utrecht University
Faculty of Science
Department of Mathematics

Djurre Tijsma, BSc: Automata and finite order elements in the Nottingham group
Master's thesis, Mathematical Sciences

Supervisor: prof. dr. Gunther Cornelissen
Second reader: prof. dr. Frits Beukers

Time frame: October 2017 - July 2018

The figure on the front page visualizes a 2-automaton generating
a sequence $(a_n)_{n\geq 0}$ for which the corresponding power series
$\sum_{n\geq 0} a_n t^n$ is an order 4 element in the Nottingham group $\mathcal{N}(\mathbf{F}_2)$.

Abstract

This thesis was written by Djurre Tijsma from October 2017 until July 2018 as part of the master's programme Mathematical Sciences at Utrecht University. The research was supervised by prof. dr. Gunther Cornelissen and the second reader is prof. dr. Frits Beukers.

We use automata theory to study the finite order elements of the Nottingham group $\mathcal{N}(\mathbf{F}_p)$ over the finite field $\mathbf{F}_p$ with p a prime number. From 2010 the only known elements of order not a prime number were three different elements of order 4. After introducing some preliminaries and the theory of p-automata, we present a method for constructing algebraic equations for finite order elements of $\mathcal{N}(\mathbf{F}_p)$ over the rational function field. In the specific case $p = 2$ we use a 2-automaton to construct for five different elements of order 4 an explicit power series. These five power series are different from the three known power series found in the literature.

Acknowledgments

This thesis would not have been possible without the help of a number of people. I extend my gratitude to all of them.

First of all, I would like to thank Gunther Cornelissen for being my supervisor and for giving me the opportunity to work on this topic. I greatly benefited from his guidance and his helpful suggestions during our meetings.

I would like to thank Frits Beukers for being the second reader of this thesis.

Lastly I thank Ragnar Groot Koerkamp, Harry Smit and Merlijn Staps who took the time to read parts of the manuscript and provided many valuable comments.

Contents

Introduction

The main object of study in this thesis are the finite order elements of the Nottingham group $\mathcal{N}(\mathbf{F}_p) = \{\sigma \in \mathbf{F}_p[\![t]\!] \mid \sigma(t) \equiv t \mod t^2\}$ with p a prime number and with group operation composition of power series. Group theoretically this an interesting group as it contains for example every finite p-group as a subgroup. Specifically of interest are the finite order elements of $\mathcal{N}(\mathbf{F}_p)$, which all have as order a power of p, and one of the questions one can ask is the following:

What do elements of order p^n in $\mathcal{N}(\mathbf{F}_p)$ look like and can we give explicit power series for them?

Klopsch considers in [12] the order p elements, he gave up to conjugation a standard form for every conjugation class of elements of order p. The next case to consider are the order p^2 elements. Since 2010 there are only three known explicit power series of non prime order and they all have order 4, see [9] and [6].

Using the theory of p-automata we study these elements of order p^n. A p-automaton can be considered as a machine that computes a sequence a_n (or equivalently a power series $\sum_{n\geq 0} a_n t^n$) when fed the base p expansion of n. In this way we have obtained five new explicit power series of order 4.

In Chapter 1 we introduce some concepts, tools and theory which we need in the remainder of the thesis. In Section 1.1 we start by recalling some basic notions of power series and we introduce the Cartier operators and some of their properties. These operators will be important for the chapter on p-automata. In Section 1.2 we give a small introduction to Witt vectors and the Artin-Schreier-theory describing the cyclic extension of a field of prime characteristic. In Section 1.3 we discuss valued fields and we a give a basic introduction to function fields.

In Chapter 2 we introduce the Nottingham group, the group of interest in this thesis. In Section 2.1 we define and treat some basic properties of the Nottingham group. The last two sections are about the finite order elements in the Nottingham group. Specifically, in Section 2.2 we look at the case of order p elements which was completely classified by Klopsch in [12]. In Section 2.3 we have a look at the order p^n elements for $n > 1$, which is less well understood.

In Chapter 3 we develop the theory of p-automata, which is essential to us for solving some algebraic equations in chapter 4. We start by defining in Section 3.1 concepts such as p-automaton and p-automatic sequences, and we finish with the theorem of Christol relating algebraic power series to automatic sequences. In Section 3.2 we give a direct algorithm for constructing the minimal p-automaton of the power series $(1 + at)^{-1/n}$, which has a nice description.

In Chapter 4 we apply the theory from the previous chapters to give in Section 4.1 a method for constructing algebraic equations of order p^n elements in $\mathcal{N}(\mathbf{F}_p)$ and in Section 4.2 we use this method to find five new explicit power series of order 4.

Chapter 1

Preliminaries

In this chapter we recall and introduce some basic properties of power series and Laurent series, we define the Cartier operators and treat a theorem of Ore. Then we discuss the existence and properties of certain n-th roots. We continue with introducing Witt vectors and a part of Artin-Schreier-Witt theory which we will use in Section 4.2 to create a cyclic Galois extension of degree 4 of a field of characteristic 2. After this, we give some results about Galois theory for complete fields and we finish by introducing the basics of function field theory. Throughout this whole chapter k will denote a field and p a prime number.

1.1 Formal power series and Cartier operators

In this section we start by recalling some basic properties of power series including n-th roots of power series. Then we introduce the Cartier operators on the field of Laurent series $\mathbf{F}_p(\!(t)\!)$. These operators are crucial for the development of the theory for p-automatic sequences as is done in Chapter 3.

Recall that the ring of formal power series in the variable t over k is given by

$$k[\![t]\!] = \{\sum_{n\geq 0} a_n t^n \mid a_n \in k\}$$

where the addition and multiplication laws are the usual one. It is well known that $k[\![t]\!]$ is a domain and that the power series $\sum_{n\geq 0} a_n t^n \in k[\![t]\!]$ is invertible (with respect to multiplication) if and only if $a_0 \neq 0$. The fraction field of $k[\![t]\!]$ is the field of formal Laurent

series $k(\!(t)\!)$, which is given by

$$k(\!(t)\!) = \{\sum_{n \geq m} a_n t^n \mid a_n \in k, m \in \mathbf{Z}\}\,.$$

So for any element of $k(\!(t)\!)$ only finitely many coefficients of the negative powers of t are non-zero. The field $k(\!(t)\!)$ comes equipped with a discrete valuation

$$v : k(\!(t)\!) \to \mathbf{Z} \cup \{\infty\}\,,$$

which is defined by $v(f) = \infty$ if $f = 0$ and

$$v(f) = \min_{n \in \mathbf{Z}} \{n \,|\, a_n \neq 0\}$$

if $f = \sum_{n \in \mathbf{Z}} a_n t^n \in k(\!(t)\!)$ is non-zero. That this is indeed a discrete valuation is easily verified. This turns $k[\![t]\!]$ into a complete local ring.

For $f \in k(\!(t)\!)$ and $g \in tk[\![t]\!]$, we define the composition $f \circ g \in k(\!(t)\!)$ by

$$(f \circ g)(t) := f(g(t))\,.$$

This definition makes sense, because the coefficient of t^0 in g is zero and hence we have for each $n \in \mathbf{Z}$ that the coefficient of t^n in $f(g(t))$ is a finite sum of non-zero elements of k. For an element $f \in tk[\![t]\!]$ denote the n-fold composition of f with itself by $f^{\circ n}$, so

$$f^{\circ n}(t) = (\underbrace{f \circ \ldots \circ f}_{n \text{ times}})(t)\,.$$

In Section 2.1 we show that if $f \in tk[\![t]\!]$ has a right or left compositional inverse $g \in tk[\![t]\!]$, then g is a two-sided inverse. We write $f^{\circ -1}$ for this element g, we set $f^{\circ 0} = t$ (the identity in $\mathcal{N}(k)$, see Section 2.1) and for $n \geq 1$ we write $f^{\circ -n} := (f^{\circ -1})^n$.

In our investigation of the Nottingham group, in Section 2.1, we need the existence and uniqueness of n-th roots of certain power series. For this we need Hensel's Lemma which is stated below, a proof can be found in F13 on page 58 in [13].

Theorem 1.1.1 (**Hensel's Lemma**). *Consider the complete local ring $R = k[\![t]\!]$ and a monic polynomial $f \in R[T]$. If $\alpha \in k$ is a simple root of f then there exists an element $a \in R$ with $a \equiv \alpha \mod t$ and $f(a) = 0$.*

Corollary 1.1.2. *Let $m, n \in \mathbf{Z}$ be two integers with $\gcd(p, n) = 1$ and $B \in 1 + tk[\![t]\!]$ a power series. Then there exists a unique power series $A \in 1 + tk[\![t]\!]$ satisfying $A^n = B^m$.*

Proof. Consider the polynomial $f(T) = T^n - B^m \in k[\![t]\!][T]$. We see that $f(1) \equiv 0 \mod t$ and $f'(1) = n \not\equiv 0 \mod t$ because $p \nmid n$. Applying Hensel's Lemma shows that there exists a unique power series $A \in 1 + tk[\![t]\!]$ such that $A^n = B^m$. □

For the polynomial $1+t \in \mathbf{F}_p[t]$ we can be more precise about its n-th roots. That is, we can give a formula for its coefficients by means of the generalized binomial theorem. We therefore first introduce the generalized binomial.

Definition 1.1.3 (**Generalized binomial**). *For each $n \geq 0$, define the polynomial $\binom{t}{n} \in \mathbf{Q}[t]$ by*

$$\binom{t}{n} := \frac{t(t-1)\cdots(t-n+1)}{n!}.$$

Note that $\binom{t}{0} = 1$ since we regard the empty product to be equal to 1.

Because of its use in the generalized binomial it is important to extend the binomial coefficient to $\mathbf{F}_p$. This lemma was stated in Exercise 11 in [2], we give our own proof.

Lemma 1.1.4. *Let $\frac{a}{b} \in \mathbf{Q}$ be written in lowest form and suppose that $p \nmid b$. Then p does not divide the denominator of $\binom{\frac{a}{b}}{n}$.*

For the proof of the above lemma we are going to work with the p-adic integers $\mathbf{Z}_p$ inside the field of p-adic numbers $\mathbf{Q}_p$.

Proof. It is clear that $f_n(t) := \binom{t}{n}$ is a polynomial in $\mathbf{Q}_p[t]$ and so a continuous map from $\mathbf{Q}_p$ to $\mathbf{Q}_p$. Since $\frac{a}{b} \in \mathbf{Z}_p$ we can write $\frac{a}{b} = \lim_{m\to\infty} \sum_{i=0}^{m} c_i p^i$ for some integers $0 \leq c_i < p$. Using the continuity of f_n, this gives

$$\binom{\frac{a}{b}}{n} = f_n(\tfrac{a}{b}) = \lim_{m\to\infty} f_n\left(\sum_{i=0}^{m} c_i p^i\right).$$

For each $m \geq 0$ we have $\sum_{i=0}^{m} c_i p^i \in \mathbf{Z} \subseteq \mathbf{Z}_p$, because f_n is continuous and $\mathbf{Z}_p$ is a closed subset of $\mathbf{Q}_p$. We see that the limit $f_n(\frac{a}{b})$ also lies in $\mathbf{Z}_p$. It follows that $f_n(\frac{a}{b})$ is an element of $\mathbf{Z}_p \cap \mathbf{Q}$ and hence p does not divide the denominator of $\binom{\frac{a}{b}}{n}$ when written in lowest form. □

Remark 1.1.5. We use the notation of the previous lemma. Since p doesn't divide the denominator of $\binom{\frac{a}{b}}{n}$ we can reduce this fraction modulo p to obtain an element of $\mathbf{F}_p$. We take this as the definition of $\binom{\frac{a}{b}}{n} \in \mathbf{F}_p$.

For a rational number a with p not dividing the denominator of a, we define the power series

$$(1+t)^a := \sum_{k\geq 0} \binom{a}{k} t^k \in \mathbf{F}_p[\![t]\!] \tag{1.1}$$

which is well-defined by Lemma 1.1.4. One can show that the power series in Equation (1.1) behaves exactly as one hopes: for $a, b \in \mathbf{Q}$ with p not dividing the denonimator of a and b we have $(1+t)^a(1+t)^b = (1+t)^{a+b}$ and $((1+t)^a)^b = (1+t)^{ab}$.

We move on to Cartier operators. The Frobenius map $x \mapsto x^p$ is an automorphism of $\mathbf{F}_p$, so for $A(t) = \sum_{n\in\mathbf{Z}} a_n t^n \in \mathbf{F}_p(\!(t)\!)$ we have

$$A(t)^p = \left(\sum_{n\in\mathbf{Z}} a_n t^n\right)^p = \sum_{n\in\mathbf{Z}} a_n t^{pn} = A(t^p)\,.$$

This is a useful property of Laurent series that we will encounter multiple times. The next definition introduces the Cartier operators.

Definition 1.1.6 (**Cartier Operator**). *Let $0 \le r < p$ be an integer. The Cartier operator Λ_r is defined on the monomials $t^n \in \mathbf{F}_p(\!(t)\!)$ with $n \in \mathbf{Z}$ by*

$$\Lambda_r(t^n) = \begin{cases} t^m & \text{if } n = pm + r \text{ for some } m \in \mathbf{Z}; \\ 0 & \text{otherwise.} \end{cases}$$

Extending this definition $\mathbf{F}_p$-linearly to $\mathbf{F}_p(\!(t)\!)$ gives the definition of the Cartier operator Λ_r on $\mathbf{F}_p(\!(t)\!)$. In particular we have for a power series $A = \sum_{n\ge 0} a_n t^n \in \mathbf{F}_p(\!(t)\!)$ that

$$\Lambda_r(A) = \Lambda_r\left(\sum_{n\in\mathbf{Z}} a_n t^n\right) = \sum_{n\in\mathbf{Z}} a_{pn+r} t^n\,.$$

We may apply the Cartier operators any number of times to a Laurent series. It turns out to be useful to extend the Cartier operators from a one-dimensional sequence over $\mathbf{F}_p$ to a k-dimensional sequence over $\mathbf{F}_p$.

Definition 1.1.7 (**Multi-dimensional Cartier operator**). *Let ℓ be some positive integer and consider an element $r = (r_0, r_1, \ldots, r_{\ell-1}) \in \mathbf{F}_p^\ell$. Define the Cartier operator Λ_r on the monomials $t^n \in \mathbf{F}_p(\!(t)\!)$ with $n \in \mathbf{Z}$ by*

$$\Lambda_r(t^n) = \begin{cases} t^m & \text{if } n = p^\ell m + r_0 + r_1 p + \ldots + r_{\ell-1}p^{\ell-1} \text{ for some } m \in \mathbf{Z} \\ 0 & \text{otherwise} \end{cases}.$$

Extending this definition $\mathbf{F}_p$-linearly to $\mathbf{F}_p(\!(t)\!)$ gives the definition of Λ_r on $\mathbf{F}_p(\!(t)\!)$.

For $\ell = 1$ the above definition reduces to the one given in Definition 1.1.6.

Remark 1.1.8. In a similar way as in Definition 1.1.6 we can define the Cartier operator Λ_r with $0 \le r < p$ of a sequence $a = (a_n)_{n\ge 0}$ by

$$\Lambda_r(a) := (a_{pn+r})_{n\ge 0}\,.$$

In an analogous way to what we did in Definition 1.1.7 we can define the Cartier operator Λ_r for $r \in \mathbf{F}_p^\ell$ on a sequence in $\mathbf{F}_p$.

The Cartier operator has some useful properties.

Lemma 1.1.9. *For two Laurent series $A, B \in \mathbf{F}_p(\!(t)\!)$ and an integer $0 \leq r < p$ we have*

(1) $A = \sum_{0 \leq r < p} t^r (\Lambda_r(A))^p$;

(2) $\Lambda_r(A^p B) = A \Lambda_r(B)$.

Proof. Write $A = \sum_{n \in \mathbf{Z}} a_n t^n$ then

$$\begin{aligned} A(t) &= \sum_{0 \leq r < p} \sum_{n \in \mathbf{Z}} a_{pn+r} t^{pn+r} = \sum_{0 \leq r < p} t^r \sum_{n \in \mathbf{Z}} a_{pn+r} (t^n)^p \\ &= \sum_{0 \leq r < p} t^r \left(\sum_{n \in \mathbf{Z}} a_{pn+r} t^n \right)^p = \sum_{0 \leq r < p} t^r (\Lambda_r(A))^p \,, \end{aligned}$$

which proves the first equality. If $B(t) = \sum_{n \in \mathbf{Z}} b_n t^n$ then

$$A^p B = \left(\sum_{n \in \mathbf{Z}} a_n t^{np} \right) \left(\sum_{n \in \mathbf{Z}} b_n t^n \right) = \sum_{m \in \mathbf{Z}} \sum_{pi + j = m} a_i b_j t^m$$

which gives

$$\Lambda_r(A^p B) = \sum_{m \in \mathbf{Z}} \sum_{pi + j = pm + r} a_i b_j t^m \,.$$

On the other hand we have

$$A \Lambda_r(B) = \left(\sum_{n \in \mathbf{Z}} a_n t^n \right) \left(\sum_{n \in \mathbf{Z}} b_{pn+r} t^n \right) = \sum_{m \in \mathbf{Z}} t^m \sum_{i+j=m} a_i b_{pj+r} \,.$$

Combining the last two equations shows that $\Lambda_r(A^p B) = A \Lambda_r(B)$. □

Remark 1.1.10. For a polynomial $A \in \mathbf{F}_p[t]$ and an integer $0 \leq r < p$ it follows directly from the definition of the Cartier operator that $\deg \Lambda_r(A) \leq \lfloor \frac{\deg A}{p} \rfloor \leq \frac{\deg A}{p}$.

The next theorem shows that there exists an algebraic relation over $\mathbf{F}_p(t)$ between the p-th powers of a power series in $\mathbf{F}_p(\!(t)\!)$ if it is algebraic over $\mathbf{F}_p(t)$. This special form will come in handy because it behaves well with respect to the Cartier operator. We sometimes call it the Ore form.

Theorem 1.1.11 (Ore). *Let $A \in \mathbf{F}_p(\!(t)\!)$, then A is algebraic over $\mathbf{F}_p(t)$ if and only if there exists an integer $n \geq 1$ and polynomials $B_0, B_1, \ldots, B_n \in \mathbf{F}_p[t]$, not all zero, such that*

$$B_0 A + B_1 A^p + B_2 A^{p^2} + \ldots + B_n A^{p^n} = 0 \,. \tag{1.2}$$

Moreover, one can even assume that $B_0 \neq 0$.

Proof. The direction ($\Leftarrow$) follows immediately from the definition of being algebraic over $\mathbf{F}_p(t)$. For ($\Rightarrow$) we know that there exists a polynomial $P(T) \in \mathbf{F}_p[t][T]$ of degree $\deg_T P = n$ such that $P(A) = 0$. Consider the powers $T, T^p, \ldots, T^{p^n}$, by Euclidean division there exists polynomials $S_i, R_i \in \mathbf{F}_p(t)[T]$ such that

$$T^{p^i} = S_i P + R_i$$

for $i = 0, 1, \ldots, n$ with $\deg_T R^i < n$. We now have $n+1$ polynomials R_i of degree between 0 and $n-1$ and so these polynomials are linearly dependent over $\mathbf{F}_p(t)$. Hence there exists $C_0, \ldots, C_n \in \mathbf{F}_p(t)$, not all zero, such that

$$0 = \sum_{i=0}^{n} C_i R_i \,.$$

This gives

$$\sum_{i=0}^{n} C_i T^{p^i} = P \sum_{i=0}^{n} C_i S_i + \sum_{i=0}^{n} C_i R_i = P \sum_{i=0}^{n} C_i S_i$$

and since A is a zero of the right hand side it follows that A is also a zero of the left hand side. By multiplying with a suitable polynomial we can take the coefficients of the T^{p^i} to be in $\mathbf{F}_p[t]$. This shows that A is a zero of an equation of the form in (1.2).

We will now show that we can take $B_0 \neq 0$. Assume that we have a relation

$$B_0 A + B_1 A^p + B_2 A^{p^2} + \ldots + B_n A^{p^n} = 0$$

with $B_i \in \mathbf{F}_p[t]$, not all zero, and n minimal. Since the B_i are not all zero we can find an integer $0 \leq r < p$ such that $\Lambda_r(B_j) \neq 0$ for some j. If $B_0 = 0$ then

$$0 = \Lambda_r \left(\sum_{i=0}^{n} B_i A^{p^i} \right) = \sum_{i=1}^{n} A^{p^{i-1}} \Lambda_r(B_i) \,,$$

using Lemma 1.1.9, which is an equation of a similar form with not all coefficients non-zero and smaller degree in A. This implies that n is not minimal, a contradiction. Hence we must have $B_0 \neq 0$. □

Remark 1.1.12. In the above proof we use Euclidean division to obtain the polynomials $R_i \in \mathbf{F}_p(t)[T]$ and then we use linear algebra to find a linear dependence between the R_i's. In practice, these polynomials can have big coefficients and the C_i's from the proof can get complicated. Putting an equation in Ore form can therefore be challenging. With the help of a computer for small equations it is feasible, but if the degrees of the equations get large then it becomes tedious and it can take a while.

1.2 The ring of Witt vectors and Artin-Schreier-Witt theory

In this section we introduce the ring of Witt vectors of an arbitrary ring. We use these Witt vectors to construct cyclic Galois extensions for a field k of prime characteristic. This section is written in an expository way and we have left out almost all of the proofs. For a careful treatment with proofs of the theory of Witt vectors we refer to Chapter 26 of [13]. Throughout this section, p denotes a prime number.

In order to define the ring of Witt vectors for an arbitrary ring it turns out to be useful to define it first for the ring $R = \mathbf{Q}[x_0, y_0, x_1, y_1, \ldots]$, the polynomial ring over $\mathbf{Q}$ in countably many variables. Consider the set $R^{\mathbf{N}}$, the set of all sequences $(a_0, a_1, \ldots)$ with $a_i \in R$. For an element $a = (a_0, a_1, \ldots) \in R^{\mathbf{N}}$ define its *ghost component* $a^* \in R^{\mathbf{N}}$ by $a^* = (a^{(0)}, a^{(1)}, \ldots)$ where

$$a^{(n)} = a_0^{p^n} + p a_1^{p^{n-1}} + \ldots + p^n a_n \text{ for every } n \geq 0\,.$$

Moreover we write $F(a)$ for the element $(a_0^p, a_1^p, \ldots) \in R^{\mathbf{N}}$. We work in the ring R so we may divide by powers of p. Using the identity

$$a^{(n)} = F(a)^{(n-1)} + p^n a_n$$

we can recover the element $a \in R^{\mathbf{N}}$ from its ghost component a^*. This fact enables us to define an addition and multiplication law on $R^{\mathbf{N}}$. This can be done as follows, for $a, b \in R^{\mathbf{N}}$ we define its sum $a + b \in R^{\mathbf{N}}$ as the unique element in $R^{\mathbf{N}}$ satisfying

$$(a + b)^{(n)} = a^{(n)} + b^{(n)} \text{ for all } n \geq 0\,.$$

Similarly we define the product $a \cdot b \in R^{\mathbf{N}}$ as the unique element in $R^{\mathbf{N}}$ satisfying

$$(a \cdot b)^{(n)} = a^{(n)} \cdot b^{(n)} \text{ for all } n \geq 0\,.$$

At the level of ghost components we just have coordinate-wise addition and multiplication. The next lemma shows that this defines a ring structure on $R^{\mathbf{N}}$.

Lemma 1.2.1. *Let R be as above. The set $R^{\mathbf{N}}$ becomes a commutative ring with zero element $0 = (0, 0, \ldots)$ and unit element $1 = (1, 0, \ldots)$ if we define addition and multiplication as above. We write $W(R)$ for this ring and call it the ring of Witt vectors over the ring R.*

The proof of Lemma 1.2.1 is not difficult. We therefore only illustrate it by giving a proof for the distributive law and leave the rest to the reader. Let $a, b, c \in W(R)$, using

the definitions of addition and multiplication in $W(R)$ we see that

$$\begin{aligned}(a \cdot (b+c))^{(n)} &= a^{(n)}(b+c)^{(n)} \\ &= a^{(n)}(b^{(n)} + c^{(n)}) \\ &= a^{(n)} \cdot b^{(n)} + a^{(n)} \cdot c^{(n)} \\ &= (a \cdot b)^{(n)} + (a \cdot c)^{(n)} \\ &= (a \cdot b + a \cdot c)^{(n)}\end{aligned}$$

holds for every $n \geq 0$. It follows that we have for all $a, b, c \in W(R)$ the identity

$$a \cdot (b+c) = a \cdot b + a \cdot c$$

and so the distributive law holds.

Let $x = (x_0, x_1, \ldots), y = (y_0, y_1, \ldots) \in W(R)$, we can recover the entries of $x + y$ from the entries of its ghost component $(x+y)^*$. In this recovering process we only divide by powers of p, this shows that $(x+y)_n$ is a polynomial in the entries of x and y, so

$$(x+y)_n \in \mathbf{Q}[x_0, y_0, \ldots, x_n, y_n]\,.$$

Consider the homomorphism $f : R \to R$ which sends x_i to a_i and y_i to b_i. Applying this to the polynomial $(x+y)_n$ shows that we have more generally that

$$(a+b)_n \in \mathbf{Q}[a_0, b_0, \ldots, a_n, b_n]$$

for all $a, b \in W(R)$. A similar result holds for $(a \cdot b)_n$. It turns out that even more is true, which is captured in the next theorem. See Lemma 1 on page 97 in [13] for a proof.

Theorem 1.2.2. *For two elements $a, b \in W(R)$ we have*

$$(a+b)_n - (a_n + b_n) \in \mathbf{Z}[a_0, b_0, \ldots, a_{n-1}, b_{n-1}]$$

and

$$(a \cdot b)_n \in \mathbf{Z}[a_0, b_0, \ldots, a_n, b_n]$$

for all $n \geq 0$.

So all the coefficients of these polynomials actually belong to $\mathbf{Z}$. This is of crucial importance for the construction of the ring of Witt vectors $W(S)$ for an arbitrary ring S. Using these "universal" identities and the fact that $W(R)$ is a ring we can transfer the ring structure from $W(R)$ to $W(S)$ (as a set $W(S)$ is just $S^{\mathbf{N}}$). A way to this is as follows. Let $a, b \in S^{\mathbf{N}}$ and consider the evaluation homomorphism $g : R \to S$ which maps x_i to a_i and y_i to b_i. Define the sum $a + b$ and product $a \cdot b$ by

$$(a+b)_n := g((x+y)_n) \text{ and } (a \cdot b)_n := g((x \cdot y)_n)$$

for every $n \geq 0$. One can show that this turns $W(S)$ into a ring with zero element $0 = (0, 0, \ldots)$ and unit element $1 = (1, 0, \ldots)$ but we won't do this here.

The formulas for addition and multiplication, i.e. $(a+b)_n$ and $(a \cdot b)_n$, in $W(R)$ (and hence in $W(S)$ for any ring S) become very complicated if the index n gets large. Knowing these formulas is important for the applications of the Witt vectors. We will give two ways for finding these formulas. One possibility is to start with the ghost components and try to solve successively for the addition formula and multiplication formulas. For $a, b \in W(R)$ we find that the first three components of a^* are

$$a^{(0)} = a_0, \quad a^{(1)} = a_0^p + pa_1, \quad a^{(2)} = a_0^{p^2} + pa_1^p + p^2 a_2$$

and we have similar formulas for $b^{(0)}, b^{(1)}$ and $b^{(2)}$. The ghost components of the sum $a+b$ are

$$\begin{aligned}
(a+b)_0 = (a+b)^{(0)} &= a_0 + b_0 \\
(a+b)_0^p + p(a+b)_1 = (a+b)^{(1)} &= a_0^p + b_0^p + p(a_1 + b_1) \\
(a+b)_0^{p^2} + p(a+b)_1^p + p^2(a+b)_2 = (a+b)^{(2)} &= a_0^{p^2} + b_0^{p^2} + p(a_1^p + b_1^p) + p^2(a_2 + b_2)
\end{aligned}$$

and for the product $a \cdot b$ we find

$$\begin{aligned}
(a \cdot b)_0 = (a \cdot b)^{(0)} &= a_0 b_0 \\
(a \cdot b)_0^p + (a \cdot b)_1 = (a \cdot b)^{(1)} &= (a_0^p + pa_1)(b_0^p + pb_1) \\
(a \cdot b)_0^{p^2} + p(a \cdot b)_1^p + p^2(a \cdot b)_2 = (a \cdot b)^{(2)} &= (a_0^{p^2} + pa_1^p + p^2 a_2)(b_0^{p^2} + pb_1^p + p^2 b_2)\,.
\end{aligned}$$

We see that $(a+b)_0$ and $(a \cdot b)_0$ are precisely the ordinary laws for addition and multiplication. Solving these equations for $(a+b)_1$ and $(a \cdot b)_1$ we find

$$(a+b)_1 = a_1 + b_1 + \frac{a_0^p + b_0^p - (a_0 + b_0)^p}{p} \text{ and } (a \cdot b)_1 = pa_1 b_1 + a_0^p b_1 + b_0^p a_1\,. \tag{1.3}$$

Because the formulas for $(a+b)_2$ and $(a \cdot b)_2$ become too big, we don't write them out explicitly. Note that $(a+b)_1$ is indeed a polynomial in $\mathbf{Z}[a_0, b_0, a_1, b_1]$ since p divides the binomial coefficient $\binom{p}{k}$ for every $1 \leq k \leq p-1$.
Another way to find these formulas is a bit mysterious and the relation with the Witt vectors is not so clear at first sight. It arises from a different way (as in Lemma 1 on page 97 of [13]) to prove Theorem 1.2.2, see for example [16]. For $a, b \in W(R)$ and $n \geq 0$ the polynomial $-(a+b)_n$ can be read of from the power series

$$\prod_{k \geq 0} \left(1 - b_k t^{p^k}\right) \cdot \prod_{m \geq 0} \left(1 - a_m t^{p^m}\right) \in R[\![t]\!]\,,$$

as the coefficient of t^{p^n} and the polynomial $-(a \cdot b)_n$ can be read of from the power series

$$\prod_{d,e \geq 1} \left(1 - a_d^{m/p^d} b_e^{m/p^e} t^m\right)^{p^{d+e}/m}\,,$$

where $m = p^{\max\{d,e\}}$, as the coefficient of t^{p^n}.

Another important property of the construction of the ring of Witt vectors is that it is functorial. This means that if $\varphi : S \to T$ is a ring homomorphism then we get an induced ring homomorphism

$$W(S) \to W(T) : (s_0, s_1, \ldots) \mapsto (\varphi(s_0), \varphi(s_1), \ldots) .$$

which we will also denote by φ.

We introduce three more important maps on the Witt ring $W(S)$ where S is an arbitrary ring. First we have the so-called *Verschiebung* map, German for *shift* map,

$$V : W(S) \to W(S) : (a_0, a_1, \ldots) \mapsto (0, a_0, a_1, \ldots)$$

This is an endomorphism on the additive group of $W(S)$ but not necessarily of the ring $W(S)$. For every $n \geq 0$ the subset $V^n(W(S))$ is an ideal of $W(S)$ consisting of all elements in $W(S)$ having a zero in the first n components, so

$$V^n(W(S)) = \{(a_0, a_1, \ldots) \mid \ a_0 = \ldots = a_{n-1} = 0\} .$$

This allows us to define the truncated Witt vectors of length n over S by

$$W_n(S) := W(S)/V^n(W(S)) .$$

Basically we forget about everything that happens outside the first n components. We will use these truncated Witt vectors in the next section.
Let k be a field of characteristic p, then the Frobenius map $F : z \mapsto z^p$ on k is a ring endomorphism and hence induces a ring endomorphism

$$F : W(k) \to W(k) : (a_0, a_1, \ldots) \mapsto (a_0^p, a_1^p, \ldots)$$

which restricts to a ring endomorphism on $W_n(k)$. Lastly, define the map $\wp$ on $W(k)$ by

$$\wp = F - \mathrm{id} ,$$

it is an endomorphism of the additive group of $W(k)$ but not necessarily of the ring $W(k)$. The map $\wp$ restricts to an endomorphism on the additive group of $W_n(k)$.

From now on let k be a field of characteristic p. We will show how one can use the truncated Witt ring $W_n(k)$ to construct cyclic Galois extensions of degree p^n of k.

Consider the map $\wp : W_n(k) \to W_n(k)$ defined in the previous section, the kernel of $\wp$ is precisely $W_n(\mathbf{F}_p)$ (where we have identified $\mathbf{F}_p$ with the prime field of k). Let $x \in W_n(k)$, one can show that there exists an $\alpha \in W_n(\overline{k})$ such that $\wp(\alpha) = x$ (here $\overline{k}$ denotes an algebraic closure of k). A way to do this is to use induction on n, for $n = 1$ this reduces

to finding an $\alpha_0 \in \overline{k}$ such that $\alpha_0^p - \alpha_0 = x_0$. Suppose $\alpha, \beta \in W_n(\overline{k})$ are two elements satisfying $\wp(\alpha) = \wp(\beta)$, then since $\wp$ is additive we get $\alpha - \beta \in \ker \wp = W_n(\mathbf{F}_p)$. This shows that solutions to the equation $\wp(\alpha) = x$ only differ up to an element of $W_n(\mathbf{F}_p)$. This allows us to write unambiguously

$$k(\wp^{-1}(x)) = k(\alpha) := k(\alpha_0, \ldots, \alpha_{n-1})\,.$$

It turns out that the extension $k(\wp^{-1}(x))/k$ is a Galois extension of degree at most p^n.

We are now ready to state the central theorem of Artin-Schreier-Witt theory (see also Theorem 5 on page 107 in [13]), which was first proven in [19].

Theorem 1.2.3 (**Artin-Schreier-Witt, 1936**). *A field extension k'/k is a finite cyclic Galois extension of degree p^n if and only if $k' = k(\wp^{-1}(x))$ for some $x \in W_n(k)$ satisfying $x_0 \notin \wp(k)$. Moreover, if $\alpha \in W_n(k')$ is an element such that $\wp(\alpha) = x$, then a generator σ for the Galois group $\mathrm{Gal}(k(\wp^{-1}(x))/k)$ is defined by $\sigma(\alpha_i) = (\alpha + 1)_i$ for all $0 \leq i \leq n-1$.*

We will look more closely at the above theorem by considering the cases $n = 1$ and $n = 2$. For $n = 1$ we will show that it reduces to the well known Artin-Schreier theory and for $n = 2$ we will demonstrate how to construct cyclic extensions of order p^2 using the truncated Witt ring $W_2(k)$.

Example 1.2.4. Suppose $n = 1$, then we know that $W_1(k)$ is just the field k. The requirement that $x_0 \notin \wp(k)$ ensures us that the polynomial $T^p - T - x_0$ is irreducible over k. Let $\alpha_0 \in \overline{k}$ be a zero of $T^p - T - x_0$ then $k(\alpha_0)/k$ is a degree p extension and since the other zeros of $T^p - T - x_0$ are given by $\alpha_0 + i$ with $1 \leq i \leq p-1$ we conclude that $k(\alpha_0)/k$ is a cyclic Galois extension of degree p.

Example 1.2.5. Suppose $n = 2$, let $x \in W_2(k)$ be a truncated Witt vector of length 2 with $x_0 \notin \wp(k)$ and $\alpha \in W_2(\overline{k})$ an element satisfying $\wp(\alpha) = x$. Writing out the equation $\wp(\alpha) = x$ in coordinates gives

$$(\alpha_0^p, \alpha_1^p) - (\alpha_0, \alpha_1) = (x_0, x_1)$$

which rewrites (using Equation (1.3)) to

$$(\alpha_0^p, \alpha_1^p) = (x_0, x_1) + (\alpha_0, \alpha_1) = \left(x_0 + \alpha_0, x_1 + \alpha_1 + \frac{x_0^p + \alpha_0^p - (x_0 + \alpha_0)^p}{p} \right)\,.$$

Note that we first have to expand $(x_0 + \alpha_0)^p$ and divide by p for this formula to make sense over a field of characteristic p. Theorem 1.2.3 ensures us that the extension $k(\alpha_0, \alpha_1)/k$ is a cyclic Galois extension of degree p^2 where α_0 and α_1 satisfy the equations

$$\alpha_0^p - \alpha_0 = x_0 \text{ and } \alpha_1^p - \alpha_1 = x_1 + \frac{x_0^p + \alpha_0^p - (x_0 + \alpha_0)^p}{p}\,.$$

That any cyclic Galois extension of degree p^2 can be obtained by such a system of equations is more difficult to prove. A generator σ of the Galois group is defined by

$$\sigma(\alpha_0) = \alpha_0 + 1 \text{ and } \sigma(\alpha_1) = \alpha_1 + \frac{\alpha_0^p + 1 - (\alpha_0 + 1)^p}{p}\,.$$

In Chapter 4 we are particular interested in the case $p = 2$. Therefore we have a closer look at the addition and multiplication formulas in the case $p = 2$ and we give the formulas for constructing a cyclic Galois extension of degree 4 and of degree 8 together with formulas for a generator of the Galois group.

Example 1.2.6. In the case $p = 2$ we give the formulas for addition and multiplication in the truncated Witt ring $W_3(k)$. For $a, b \in W_3(k)$ we have

$$\begin{aligned}(a+b)_0 &= a_0 + b_0\\ (a+b)_1 &= a_1 + b_1 + a_0b_0\\ (a+b)_2 &= a_2 + b_2 + a_1b_1 + a_0a_1b_0 + a_0b_0b_1 + a_0^3b_0 + a_0b_0^3\end{aligned}$$

and

$$\begin{aligned}(a\cdot b)_0 &= a_0b_0\\ (a\cdot b)_1 &= a_0^2b_1 + a_1b_0^2\\ (a\cdot b)_2 &= a_1^2b_1^2 + a_0^4b_2 + a_2b_0^4 + a_0^2a_1b_0^2b_1\,.\end{aligned}$$

The formulas given in Example 1.2.5 simplify a lot in the case $p = 2$ and even the formulas for a cyclic degree 8 extension are manageable. Let $x \in W_3(k)$ with $x_0 \notin \wp(k)$ and $\alpha \in W_3(\overline{k})$ an element such that $\wp(\alpha) = x$. The system of equations for a cyclic degree 8 extension then becomes

$$\alpha_0^2 - \alpha_0 = x_0 \tag{1.4}$$
$$\alpha_1^2 - \alpha_1 = x_1 + x_0\alpha_0 \tag{1.5}$$
$$\alpha_2^2 - \alpha_2 = x_2 + \alpha_1x_1 + \alpha_0\alpha_1x_1 + \alpha_0x_0x_1 + \alpha_0^3x_0 + \alpha_0x_0^3 \tag{1.6}$$

and a generator σ of the Galois group is defined by

$$\sigma(\alpha_0) = \alpha_0 + 1 \tag{1.7}$$
$$\sigma(\alpha_1) = \alpha_1 + \alpha_0 \tag{1.8}$$
$$\sigma(\alpha_2) = \alpha_2 + \alpha_0\alpha_1 + \alpha_0^3 + \alpha_0\,. \tag{1.9}$$

1.3 Completion of valued fields and function fields

In this section we start by introducing valued fields and their completions. Then we say something about the Galois theory for completions of valued fields. This is followed by an

introduction to function fields which is largely based upon Stichtenoth [18]. In Chapter 4 we apply this theory to give a method for constructing algebraic equations of finite order elements of the Nottingham group.

Let F be a field and $v : F \to \mathbf{Z} \cup \{\infty\}$ a discrete valuation of F. The pair (F, v) is called a valued field. We already encountered one example of a valued field, namely the field $k(\!(t)\!)$ with the valuation defined in the beginning of Section 1.1.

Let (F, v) be a valued field, then one can use v to turn the field F into a metric space. For example $|x| := 2^{-v(x)}$ for $x \in F$ and $|0| := 0$ defines a norm on F. It therefore makes sense to talk about convergence in a valued field. We say that a sequence $(x_n)_{n\geq 0}$ in F is convergent if there exists an element $x \in F$ which satisfies: for every $c \in \mathbf{R}$ there is an index $N \in \mathbf{N}$ such that $v(x - x_n) \geq c$ whenever $n \geq N$. Furthermore we call a sequence $(x_n)_{n\geq 0}$ a Cauchy sequence if it has the following property: for every $c \in \mathbf{R}$ there is an index $N \in \mathbf{N}$ such that $v(x_n - x_m) \geq c$ whenever $m, n \geq N$.

The following definition defines when a valued field is called complete and it lists some properties of a completion of a valued field.

Definition 1.3.1. *A valued field is said to be complete if every Cauchy sequence in it converges. Let (F, v) be a valued field, a completion of F is a valued field $(\hat{F}, \hat{v})$ with the following properties:*

(1) $F \subseteq \hat{F}$, and $\hat{v}|_F = v$;

(2) $\hat{F}$ is complete with respect to $\hat{v}$;

(3) F is dense in $\hat{F}$, that is, for each $z \in \hat{F}$ there is a sequence $(x_n)_{n\geq 0}$ in F with $z = \lim_{n\to\infty} x_n$. The valuation $v(z)$ is given by $v(z) = \lim_{n\to\infty} v(x_n)$.

It turns out that every valued field has a completion (see for instance Chapter 4 of [18]) and that it is unique in a certain way. More precisely, if (F, v) is a valued field for which $(\hat{F}, \hat{v})$ and $(\tilde{F}, \tilde{v})$ are both completions, then there is a unique isomorphism $f : \hat{F} \to \tilde{F}$ such that $\hat{v} = \tilde{v} \circ f$. We may therefore speak of the completion of a valued field and we write F_v for the completion of the valued field (F, v).

We continue with some results about Galois extensions of valued fields. We state two theorems and for their proofs we refer to Theorem 4.8 and Proposition 9.6 from Chapter 2 of [15].

Theorem 1.3.2. *Let K be a complete field with respect to some valuation v. The valuation v may be extended in a unique way to a valuation of any given algebraic extension L/K. When L/K is a finite extension the field L is complete with respect to the extended valuation.*

Theorem 1.3.3. *Let (K, v), (L, w) be two valued fields such that L/K is a finite Galois extension and $w|_K = v$. Consider the completion L_w of (L, w) and let K_v be the completion of K inside L_w. We then have that the extension L_w/K_v is Galois with*

$$\mathrm{Gal}(L_w/K_v) \cong \mathrm{Gal}_w(L/K) := \{\sigma \in \mathrm{Gal}(L/K) \mid w \circ \sigma = \sigma\}.$$

We are going to use Theorem 1.3.3 for constructing finite order elements of the Nottingham group. First we need some basics of function field theory in order to apply this to a specific extension of function fields in Section 4.2.

Definition 1.3.4. *An* algebraic function field *F/K is a field extension F/K such that F is a finite algebraic extension of $K(x)$ for some element $x \in F$ which is transcendental over K.*

Example 1.3.5. The simplest example of an algebraic function field is the rational function field. An algebraic function field F/K is called rational if $F = K(x)$ for some $x \in F$ which is transcendental over K.

We now introduce the notions of valuation rings, places and the residue class field.

Definition 1.3.6. *A* valuation ring *of the function field F/K is a ring $\mathcal{O} \subseteq F$ with the following properties:*

(1) $K \subsetneq \mathcal{O} \subsetneq F$, and

(2) for every $z \in F$ we have that $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

Example 1.3.7. Consider the rational function field $K(x)/K$. For an irreducible monic polynomial $p(x) \in K[x]$ consider the set

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], p(x) \nmid g(x) \right\}.$$

It is easily verified that $\mathcal{O}_{p(x)}$ is a valuation ring of $K(x)/K$.

We now state some properties of a valuation ring of a function field.

Proposition 1.3.8. *Let $\mathcal{O}$ be a valuation ring of the function field F/K. Then the following hold:*

(a) $\mathcal{O}$ is a local ring with $P = \mathcal{O} \backslash \mathcal{O}^\times$ as its unique maximal ideal, here $\mathcal{O}^\times$ is the group of units of $\mathcal{O}$.

(b) Let $0 \neq x \in F$, then $x \in P \Leftrightarrow x^{-1} \notin \mathcal{O}$.

(c) The maximal ideal P is a principal ideal.

(d) If $P = t\mathcal{O}$ for some $t \in \mathcal{O}$, then each $0 \neq z \in F$ has a unique representation of the form $z = t^n u$ for some $n \in \mathbf{Z}$ and $u \in \mathcal{O}^\times$.

Definition 1.3.9. *A place P of the function field F/K is the maximal ideal of some valuation ring $\mathcal{O}$ of F/K. Every element $t \in P$ such that $P = t\mathcal{O}$ is called a uniformizer for P. We write*

$$\mathbb{P}_F := \{P \mid P \text{ is a place of } F/K\}$$

for the set of all places of F/K.

Note that if $\mathcal{O}$ is a valuation ring of F/K and P is its maximal ideal, then $\mathcal{O}$ is uniquely determined by P. Hence $\mathcal{O}_P := \mathcal{O}$ is called the valuation ring of the place P. That the set of places is always non-empty is something that has to be proved, it is not immediate from the definitions. A proof can be found in Theorem 1.1.19 from Chapter 1 in [18]. To each place of a function field we can associate a discrete valuation as follows.

Definition 1.3.10. *Let F/K be an algebraic function field and $P \in \mathbb{P}_F$ a place. We associate to P a map $v_P : F \to \mathbf{Z} \cup \{\infty\}$ which is defined as follows. Choose a uniformizer t for P. Then every $0 \neq z \in F$ has a unique representation $z = t^n u$ with $u \in \mathcal{O}_P^\times$ and $n \in \mathbf{Z}$. Define $v_P(z) := n$ and $v_P(0) := \infty$.*

The above definition of v_P depends on a choice of uniformizer (which always exists), however one can show that the value of $v_P(z)$ is independent of this choice of uniformizer. So v_P is a well-defined map. We have the following theorem.

Theorem 1.3.11. *Let F/K be a function field.*

(a) For a place $P \in \mathbb{P}_F$, the function v_P defined above is a discrete valuation of F/K. Moreover we have

$$\begin{aligned} \mathcal{O}_P &= \{z \in F \mid v_P(z) \geq 0\}, \\ \mathcal{O}_P^\times &= \{z \in F \mid v_P(z) = 0\}, \\ P &= \{z \in F \mid v_P(z) > 0\}. \end{aligned}$$

(b) An element $x \in F$ is a prime element for P if and only if $v_P(x) = 1$.

(c) Conversely, suppose that v is a discrete valuation of F/K. Then the set $P := \{z \in F \mid v(z) > 0\}$ is a place of F/K, and $\mathcal{O}_P = \{z \in F \mid v(z) \geq 0\}$ is the corresponding valuation ring.

(d) Every valuation ring $\mathcal{O}$ of F/K is a maximal proper subring of F.

For a place P of a function field we saw above that $\mathcal{O}_P$ is a local ring, so we can look at its residue class field.

Definition 1.3.12. *Let $P \in \mathbb{P}_F$. Since P is a maximal ideal the* residue class ring $F_P := \mathcal{O}_P/P$ *is a field. For $x \in \mathcal{O}_P$ we define $x(P) \in F_P$ to be the* residue class *of x modulo P, for $x \in F \backslash \mathcal{O}_P$ we put $x(P) := \infty$. The map $x \mapsto x(P)$ from F to $F_P \cup \{\infty\}$ is called the residue class map with respect to P. We have $K \cap P = \{0\}$ so we can consider K as a subfield of F_P. We write* $\deg P := [F_P : K]$, *the* degree *of P.*

Example 1.3.13. Consider the case of the rational function field $K(x)/K$ and a monic irreducible polynomial $p(x) \in K[x]$. We write $P = P_{p(x)}$ for the maximal ideal of the valuation ring $\mathcal{O}_{p(x)}$. For $z \in F(x)$ we then have $v_P(z) = n$ if $z = p(x)^n \cdot \frac{f(x)}{g(x)}$ with $n \in \mathbf{Z}$, $f(x), g(x) \in K[x]$ and $p(x) \nmid f(x)g(x)$. For the residue class field of P we have $K(x)_P \cong K[x]/(p(x))$.

We now turn towards extensions of function fields.

Definition 1.3.14. *An algebraic function field F'/K' is called an* algebraic extension *of F/K if $F \subseteq F'$ is an algebraic field extension and $K \subseteq K'$. A place $P' \in \mathbb{P}_{F'}$ is said to lie over $P \in \mathbb{P}_F$ if $P \subseteq P'$, and we write $P' \mid P$.*

Proposition 1.3.15. *Let F'/K' be an algebraic extension of F/K. Suppose that P (resp. P') is a place of F/K (resp. F'/K'), and let $\mathcal{O}_P \subseteq F$ (resp. $\mathcal{O}_{P'} \subseteq F'$) denote the corresponding valuation ring, v_P (resp. $v_{P'}$) the corresponding discrete valuation. Then the following assertions are equivalent:*

(1) $P' \mid P$.

(2) $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$.

(3) There exists an integer $e \geq 1$ such that $v_{P'}(x) = e v_P(x)$ for all $x \in F$.

Moreover, if $P' \mid P$ then

$$P = P' \cap F \text{ and } \mathcal{O}_P = \mathcal{O}_{P'} \cap F$$

For this reason, P is also called the restriction of P' to F.

A consequence of the preceding proposition is that for $P' \mid P$ there is a canonical embedding of the residue class field $F_P = \mathcal{O}_P/P$ into the residue class field $F'_{P'} = \mathcal{O}_{P'}/P'$, given by

$$x(P) \mapsto x(P') \text{ for } x \in \mathcal{O}_P\,.$$

Therefore we can consider F_P as a subfield of $F'_{P'}$.

Definition 1.3.16. *Let F'/K' be an algebraic extension of F/K, and let $P' \in \mathbb{P}_{F'}$ be a place of F'/K' lying over $P \in \mathbb{P}_F$.*
(a) The integer $e(P'|P) := e$ with $v_{P'}(x) = e \cdot v_P(x)$ for all $x \in F$ is called the ramification index *of P' over P. We say that $P' \mid P$ is ramified if $e(P'|P) > 1$, and $P' \mid P$ is unramified if $e(P'|P) = 1$.*
(b) $f(P'|P) := [F'_{P'} : F_P]$ is called the relative degree *of P' over P.*

Proposition 1.3.17. *Let F'/K' be an algebraic extension of F/K and let P' be a place of F'/K' lying over $P \in \mathbb{P}_F$. Then*
(a) $f(P'|P) < \infty \Leftrightarrow [F' : F] < \infty$.
(b) If F''/K'' is an algebraic extension of F'/K' and $P'' \in \mathbb{P}_{F''}$ is an extension of P', then

$$e(P''|P) = e(P|P') \cdot e(P'|P)$$
$$f(P''|P) = f(P''|P') \cdot f(P'|P)\,.$$

Let F'/K' be an extension of F/K of degree $[F' : F] = n$ and let $P \in \mathbb{P}_F$. We then say that P is totally ramified in F'/F if there is a place $P' \in \mathbb{P}_{F'}$ with $P'|P$ and $e(P'|P) = n$. The next theorem shows how the ramification index and the relative degree of all places in $\mathbb{P}_{F'}$ above a place $P \in \mathbb{P}_F$ are related.

Theorem 1.3.18. *Let F'/K' be a finite extension of F/K and let $P_1, \ldots, P_m$ be all the places of F'/K' lying over P. We then have the equality*

$$\sum_{i=1}^{m} e(P_i|P) f(P_i|P) = [F' : F]\,.$$

An extension F'/K' of a function field F/K is said to be Galois if F'/F is a Galois extension of finite degree. Let P be a place of F/K. Then $\mathrm{Gal}(F'/F)$ acts on the set of all extensions $\{P' \in \mathbb{P}_{F'} \mid P \subseteq P'\}$ via $\sigma(P') = \{\sigma(x) \mid x \in P'\}$ and the corresponding valuation $v_{\sigma(P')}$ is given by

$$v_{\sigma(P')}(y) = v_{P'}(\sigma^{-1}(y)) \text{ for } y \in F'\,. \tag{1.10}$$

The following proposition is important for the applications of this section in chapter 4.

Proposition 1.3.19. *Let F/K be an algebraic function field of characteristic $p > 0$. Suppose that $u \in F$ is an element which satisfies the following condition:*

$$u \neq w^p - w \text{ for all } w \in F\,.$$

Let $F' = F(y)$ with $y^p - y = u$. For $P \in \mathbb{P}_F$ we define the integer m_P by

$$m_P := \begin{cases} m & \text{if there is an element } z \in F \text{ satisfying } v_P(u - (z^p - z)) = -m < 0 \\ & \text{and } m \not\equiv 0 \mod p \\ -1 & \text{if } v_P(u - (z^p - z)) \geq 0 \text{ for some } z \in F\,. \end{cases}$$

The integer m_P is well-defined. We then have that F'/F is a cyclic Galois extension. Moreover P is totally ramified in F'/F if and only if $m_P > 0$ and in that case P' is the unique place above P. If $z \in F$ is an element such that $v_P(u - (z^p - z)) = -m_P$, then $v_{P'}(y - z) = -m_P$.

For a place P of an algebraic function field F/K we get a discrete valuation v_P and hence we can consider the completion of F with respect to this valuation.

Theorem 1.3.20. *Let F/K be an algebraic function field and $P \in \mathbb{P}_F$ a place of degree 1. Consider the completion $\hat{F}_P$ of F with respect to the valuation v_P. Then every element $z \in \hat{F}_P$ has a unique representation of the form*

$$z = \sum_{i=n}^{\infty} a_i t^i \text{ with } n \in \mathbf{Z} \text{ and } a_i \in K\,,$$

where t is a uniformizer for P, and each element of this form is contained in $\hat{F}_P$. If we write v_P also for the extended valuation on $\hat{F}_P$ then we have for $z \neq 0$ that $v_P(z) = \min\{i \mid a_i \neq 0\}$.

Chapter 2

The Nottingham group

In this chapter we introduce the Nottingham group of a field. The finite order elements in this group are the central object of study in this thesis. We first define the group itself, prove some properties of it and then we look at its finite order elements. Throughout this whole chapter k is a field of characteristic p with p a prime number.

2.1 The Nottingham group

Definition 2.1.1. *The* Nottingham group *of a field k is the set*

$$\mathcal{N}(k) = \{\sigma \in k[\![t]\!] \mid \sigma(t) \equiv t \mod t^2\}$$

with as group operation composition of power series.

Note that the assumption that k has characteristic p is not necessary for the definition of the Nottingham group (and also for some other results in this chapter). Later on we will be looking at finite order elements of $\mathcal{N}(k)$ and if k has characteristic zero then t is the only element of finite order. In Theorem 2.1.2 we show that $\mathcal{N}(k)$ is a group under this operation. Sometimes the Nottingham group is also introduced as the subgroup of the automorphisms group $\mathrm{Aut}(k[\![t]\!])$ consisting of the normalized automorphisms, i.e. those automorphisms σ of $k[\![t]\!]$ satisfying $\sigma(t) \equiv t \mod t^2$. This point of view arises naturally in algebraic geometry.

Lemma 2.1.2. *The set $\mathcal{N}(k)$ with group operation composition of power series is a group.*

Proof. For any two $f, g \in \mathcal{N}(k)$ it is easily verified that the compositions $f \circ g$ and $g \circ f$ exists and are elements of $\mathcal{N}(k)$. Composition of functions is always associative so the

group operation is automatically associative. The element $t \in \mathcal{N}(k)$ is clearly the identity with respect to the operation and so we are left to show that every element has an inverse. Let f be an element of $\mathcal{N}(k)$ and write

$$f(t) = \sum_{n \geq 1} a_n t^n$$

with $a_1 = 1$. Define the sequence $(b_n)_{n \geq 1}$ recursively by $b_1 = 1$ and for $n \geq 2$ (note that the coefficient for b_n equals $a_1^n = 1$):

$$\sum_{m=1}^{n} b_m \sum_{\substack{(i_1,\ldots,i_m) \in \mathbf{Z}^m_{>0} \\ i_1+\ldots+i_m=n}} a_{i_1} \cdots a_{i_m} = 0\,. \tag{2.1}$$

To the sequence $(b_n)_{n \geq 1}$ we associate the power series $g(t) = \sum_{n \geq 1} b_n t^n \in \mathcal{N}(k)$. Looking at the coefficient of t^n in $g(f(t))$ we see that it equals 1 if $n = 1$ and it equals the left hand side of Equation (2.1) if $n \geq 2$. It follows that $g(f(t)) = t$. In the same way we can show that there exists an $h \in \mathcal{N}(k)$ such that $h(g(t)) = t$ and then

$$h(t) = (h \circ (g \circ f))(t) = ((h \circ g) \circ f)(t) = f(t)\,. \tag{2.2}$$

So g is a two-sided inverse of f for the operation. Hence every element in $\mathcal{N}(k)$ has an inverse. This concludes the proof that $\mathcal{N}(k)$ is a group. □

The following definition introduces the depth of a power series and its initial coefficient. These are important invariants in our later study of the Nottingham group.

Definition 2.1.3. *For the element $f = t + a_{n+1}t^{n+1} + \ldots \in t + t^2 k[\![t]\!]$ define its* depth *and* initial coefficient *by respectively*

$$\delta(f) = n \quad \textit{and} \quad \operatorname{ico}(f) = a_{n+1}\,.$$

Under conjugation in $\mathcal{N}(k)$ the depth and the initial coefficient of an element remain unchanged.

Lemma 2.1.4. *For any two elements $f, g \in \mathcal{N}(k)$ we have*

$$\delta(g \circ f \circ g^{\circ -1}) = \delta(f) \quad \textit{and} \quad \operatorname{ico}(g \circ f \circ g^{\circ -1}) = \operatorname{ico}(f)\,.$$

Proof. Write h for the inverse $g^{\circ -1}$ of g. Suppose $f(t) \equiv t + at^n \mod t^{n+1}$ and $g(t) \equiv t + \sum_{i=m}^{n} b_i t^i \mod t^{n+1}$ where $a, b_m \neq 0$ and $m \geq 2$. We have

$$t = g(h(t)) \equiv h(t) + \sum_{i=m}^{n} b_i h(t)^i \mod t^{n+1}\,. \tag{2.3}$$

For each $i \geq m \geq 2$ we have

$$f(t)^i \mod t^{n+1} = t^i \mod t^{n+1},$$

this gives

$$(g \circ f)(t) \equiv f(t) + \sum_{i=m}^{n} b_i f(t)^i \mod t^{n+1} \equiv t + at^n + \sum_{i=m}^{n} b_i t^i \mod t^{n+1}$$

and so we find

$$(g \circ f \circ h)(t) \equiv h(t) + ah(t)^n + \sum_{i=m}^{n} b_i h(t)^i \mod t^{n+1}.$$

Using Equation (2.3) the above equation turns into

$$(g \circ f \circ h)(t) \equiv t + ah(t)^n \mod t^{n+1} \equiv t + at^n \mod t^{n+1}.$$

This proves the lemma. □

Definition 2.1.5. *For an element σ of $\mathcal{N}(\mathbf{F}_p)$ of order p^n we define its* depth sequence *by the n-tuple*

$$(\delta(\sigma), \delta(\sigma^{\circ p}), \ldots, \delta(\sigma^{\circ p^{n-1}})).$$

Clearly the depth sequence is an invariant of a finite order element. We can use the depth of an element of the Nottingham group to show that over a field of characteristic p any element of finite order has order a power of p. First we need an intermediate lemma.

Lemma 2.1.6. *For an element $f \in \mathcal{N}(k)$ we have $\delta(f^{\circ n}) = \delta(f)$ for every positive integer n with $\gcd(p, n) = 1$.*

Proof. The statement is clear if $f(t) = t$, so assume $f(t) \neq t$. Write $f(t) = t + at^m + \ldots$ with $a \neq 0$ and $m \geq 2$. We will prove by induction on n that

$$f^{\circ n}(t) \equiv t + nat^m \mod t^{m+1}. \tag{2.4}$$

The induction base $n = 1$ is clear, so suppose Equation (2.4) holds for some $n \geq 1$, then for $n + 1$ we have

$$\begin{aligned} f^{\circ(n+1)}(t) &= f^{\circ n}(f(t)) \\ &\equiv f(t) + naf(t)^m \mod t^{m+1} \\ &\equiv t + at^m + na(t + at^m)^m \mod t^{m+1} \\ &\equiv t + at^m + nat^m \mod t^{m+1} \\ &\equiv t + (n+1)at^m \mod t^{m+1}. \end{aligned}$$

This is precisely the statement for $n+1$, which proves the induction. Finally if $\gcd(p, n) = 1$ then $na \neq 0$ so it follows from Equation (2.4) that $\delta(f^{\circ n}) = \delta(f)$. □

It follows immediately from the identity in Equation (2.4), which is also valid in the case that the characteristic of k is zero, that t is the only element of finite order in $\mathcal{N}(k)$ if the characteristic of k is zero. We can use the previous lemma to prove the following important result.

Lemma 2.1.7. *Any element of finite order in $\mathcal{N}(k)$ has order a power of p.*

Proof. Suppose $f \in \mathcal{N}(k)$ with $f(t) \neq t$ has order $n \geq 2$. Write $n = mp^k$ with $p \nmid m$, $m \geq 1$ and $k \geq 0$. The element $f^{\circ p^k}$ clearly has order m. Using Lemma 2.1.6 this implies that

$$\delta(f^{\circ p^k}) = \delta(f^{\circ mp^k}) = \delta(t) = \infty$$

and so $f^{\circ p^k} = t$. The order of f is mp^k, so we must have $m = 1$. This proves the lemma. □

Having established that $\mathcal{N}(k)$ is indeed a group and that any finite order element has order a power of p we can ask ourselves what the structure of this group is. By an unpublished result by Leedham-Green and Weiss, which Camina proves in [5], we have the following theorem about subgroups of $\mathcal{N}(\mathbf{F}_p)$.

Theorem 2.1.8 (**Leedham-Green and Weiss, 1997**)**.** *Every finite p-group (order of the group is a power of p) embeds into $\mathcal{N}(\mathbf{F}_p)$.*

Even more is true. In [5] Camina shows that every countably based pro-p group can be embedded, as a closed subgroup, in the Nottingham group $\mathcal{N}(\mathbf{F}_p)$. A special case of Theorem 2.1.8 are the cyclic p-groups $\mathbf{Z}/p^n\mathbf{Z}$ for any $n \geq 1$. This gives the following corollary.

Corollary 2.1.9. *For any $n \geq 1$ there exists elements of order p^n in $\mathcal{N}(\mathbf{F}_p)$.*

The next question is central to this thesis.

Question. *What do finite order elements in the group $\mathcal{N}(\mathbf{F}_p)$ look like? Can we give explicit power series of order p, p^2, etc.?*

Using the theory of automata, developed in Chapter 3, we will study finite order elements and we will give a few elements of order 4 in $\mathcal{N}(\mathbf{F}_2)$ which were not previously known.

Example 2.1.10. The power series

$$f(t) = \frac{t}{1+t} = t + t^2 + t^3 + \dots$$

is a power series in $\mathcal{N}(\mathbf{F}_p)$ of order p, as one can easily check. More generally the power series

$$\frac{t}{\sqrt[n]{1+at^n}} \in \mathcal{N}(\mathbf{F}_p)$$

where $a \in \mathbf{F}_p^\times$ and n is a natural number with $\gcd(p,n) = 1$ has order p. In the next section we show that this power series is the only example of an order p element up to conjugation, a result due to Klopsch [12].

We will have a look at the Question by considering the two cases $n = 1$ and $n > 1$. In the order p case we will treat the complete classification up to conjugation and in the order p^n with $n > 1$ case we state some known results.

2.2 Order p elements in the Nottingham group

In this section we look at the first non-trivial case of the question raised in the previous section. Up to conjugacy in $\mathcal{N}(k)$ this question was completely answered by Klopsch [12]. He provides a standard form for an order p element up to conjugation.

Theorem 2.2.1 (**Klopsch, 2000**). *Let $f \in \mathcal{N}(k)$ be an element of order p, then f is conjugated to the power series*

$$F(n,a) := \frac{t}{\sqrt[n]{1+nat^n}} = \sum_{\ell \geq 0} \binom{-\frac{1}{n}}{\ell} (na)^\ell t^{n\ell+1} = t - at^{n+1} + \tfrac{n+1}{2} a^2 t^{2n+1} + \dots$$

for some integer $n > 0$ with $\gcd(p,n) = 1$ and $a \in k^\times$. Moreover both n and a depend uniquely on f.

A power series of the form $F(n,a)$ is said to be of Klopsch's form. We have the relation

$$F(n,a) \circ F(n,b) = F(n,a+b)$$

for all $a, b \in k$. This is easily verified, we have

$$F(n,a) \circ F(n,b) = \frac{\frac{t}{\sqrt[n]{1+nat^n}}}{\sqrt[n]{1+na\frac{t^n}{1+nbt^n}}} = \frac{t}{\sqrt[n]{1+nbt^n+nat^n}} = F(n,a+b)\,.$$

So for $a \in k^\times$ we have $F(n,a)^{\circ p} = F(n,pa) = F(n,0) = t$ and hence $F(n,a)$ has order p. Note that

$$\delta(F(n,a)) = n \quad \text{and} \quad \operatorname{ico}(F(n,a)) = a\,.$$

From Lemma 2.1.4 we know that the depth and the initial coefficient of a power series are invariant under conjugation. This shows that $a \in k^\times$ and n depend uniquely on f. Moreover the depth and the initial coefficient of a power series of order p are all that we have to know in order to determine to which Klopsch form it is conjugated.

In [2] a proof of Theorem 2.2.1 is sketched by breaking it up into a few exercises. The solutions we have come up with are pieced together to form a full proof of Theorem 2.2.1.

Proof of Theorem 2.2.1. Write K for the field of Laurent series $k(\!(t)\!)$. Since $f \in \mathcal{N}(k)$ the map

$$\sigma : K \to K : g \mapsto g \circ f \,,$$

is well-defined and it defines an automorphism of K as one can check (it doesn't necessarily fix K), its inverse is given by $g \mapsto g \circ f^{\circ -1}$. Let $G = \langle \sigma \rangle$ be the group of automorphisms generated by σ and write $F = K^G$ for the fix field of G. Because f has order p we have $G \cong \mathbf{Z}/p\mathbf{Z}$. By Artin's lemma the extension K/F is a Galois extension with Galois group G. The trace map of the extension K/F is defined by

$$\mathrm{Tr}_{K/F} : K \to K : x \mapsto \sum_{\tau \in G} \tau(x) \,.$$

Note that the image of $\mathrm{Tr}_{K/F}$ lies in F. We will first show that there exists an element $\alpha \in K \backslash F$ with $\mathrm{Tr}_{K/F}(\alpha) = 1$. Assume that $\alpha \in K \backslash F$ satisfies

$$\mathrm{Tr}_{K/F}(\alpha) = \mathrm{Tr}_{K/F}(\alpha^2) = \ldots = \mathrm{Tr}_{K/F}(\alpha^{p-1}) = 0 \,.$$

Using the Newton's identities between the elementary symmetric polynomials and power sums it follows that the coefficients of $T, T^2, \ldots, T^{p-1}$ of the minimal polynomial of α over F, $m_\alpha(T)$, are zero, that is

$$m_\alpha(T) := \prod_{\tau \in G}^{p} (T - \tau(\alpha)) = T^p - \beta$$

for some $\beta = (-1)^p \prod_{\tau \in G} \tau(\alpha) \in F$. Clearly $F \subsetneq F(\alpha) \subseteq K$ and since the degree $[K : F] = p$ is a prime number we conclude that $F(\alpha) = K$. This gives a contradiction with K/F being Galois because the minimal polynomial $m_\alpha(T)$ of α is inseparable over F (note $\mathrm{char}\, K = p$ and $m_\alpha(T) \in F[T^p]$). It follows that there exists an element $\alpha \in K \backslash F$ such that $\mathrm{Tr}_{K/F}(\alpha^i) \neq 0$ for some $1 \leq i \leq p-1$. The element $\frac{\alpha^i}{\mathrm{Tr}_{K/F}(\alpha^i)}$ has the desired property since $\alpha^i \notin F$, $\mathrm{Tr}_{K/F}(\alpha^i) \in F$ and its trace equals 1.

Before we continue, we need an intermediate result about the ramification index of the extension K/F (similarly to Definition 1.3.16. Let $e \in \mathbf{Z}_{>0}$ be the integer satisfying $v(F^\times) = e\mathbf{Z}$, this integer e is called the ramification index of K/F. Since K is complete

with respect to v and K/F is Galois we have that F is complete with respect to v as well. Theorem 1 on page 69 of [13] then shows that e divides $[K:F]=p$.

Let $\alpha \in K \backslash F$ be an element with trace 1, so $\mathrm{Tr}_{K/F}(\alpha)=1$. Define the element β by

$$\beta = \sum_{i=1}^{p-1} i \cdot \sigma^i(\alpha)\,.$$

Computing $\sigma(\beta)$ gives

$$\begin{aligned}\sigma(\beta) &= \sum_{i=1}^{p-1} i \cdot \sigma^{i+1}(\alpha) \\ &= \sum_{i=1}^{p-1} ((i+1)\cdot \sigma^{i+1}(\alpha) - \sigma^{i+1}(\alpha)) \\ &= (\beta - \sigma(\alpha)) - (\mathrm{Tr}_{K/F}(\alpha) - \sigma(\alpha)) \\ &= \beta - 1\,.\end{aligned}$$

Suppose $\gamma \in F$ is some element for which $v(\beta+\gamma) \geq 0$. We then have

$$-1 = \sigma(\beta) - \beta = \sigma(\beta+\gamma) - (\beta+\gamma) \equiv 0 \mod t$$

where we used that $\sigma \in \mathrm{Gal}(K/F)$ so $\sigma(\gamma)=\gamma$ and that $f \in \mathcal{N}(k)$. This gives a contradiction. For every $\gamma \in F$ we have therefore $v(\beta+\gamma) < 0$. This allows us to choose $\gamma \in F$ such that $v(\beta+\gamma)$ is maximal. If $p \mid v(\beta+\gamma)$ then since $e \in \{1,p\}$ we can find another element $\delta \in F$ which has the same valuation and leading coefficient as $\beta+\gamma$. This implies that $v(\beta+\gamma) < v(\beta+\gamma-\delta)$ contradicting the maximality of $v(\beta+\gamma)$. It follows that $p \nmid v(\beta+\gamma)$.

We finish the proof by giving an explicit element of $\mathcal{N}(k)$ to conjugate f to $F(n,a)$. Write $n=-v(\beta+\gamma)$, c for the coefficient of t^n in $\beta+\gamma$ and

$$b = t\left(\frac{(\beta+\gamma)t^n}{c}\right)^{-1/n} \in \mathcal{N}(k)$$

(note that $\frac{(\beta+\gamma)t^n}{c} \equiv 1 \mod t$ so we may extract the n-th root by Corollary 1.1.2). First we compute $\sigma(b) = b \circ f$, this gives

$$b \circ f = f\left(\frac{\sigma(\beta+\gamma)f^n}{c}\right)^{-1/n} = f\left(\frac{(\beta+\gamma-1)f^n}{c}\right)^{-1/n}\,. \tag{2.5}$$

Write $g = f(1-\frac{1}{\beta+\gamma})^{1/n}b^{-1}$ (note that $1-\frac{1}{\beta+\gamma} \equiv 1 \mod t$ so we may extract the n-th root). Since $(\beta+\gamma)b^n = c$ we have $g^n = \frac{(\beta+\gamma-1)f^n}{c}$. Both $\left(\frac{(\beta+\gamma-1)f^n}{c}\right)^{-1/n}$ and g are elements of

$1+tk[\![t]\!]$ so Corollary 1.1.2 assures us that g equals $\left(\frac{(\beta+\gamma-1)f^n}{c}\right)^{-1/n}$. Combining this with Equation (2.5) we get

$$b \circ f = fg^{-1} = b\left(1 - \frac{1}{\beta+\gamma}\right)^{-1/n} = \frac{b}{\sqrt[n]{1-\frac{b^n}{c}}} = F(n, -\tfrac{1}{nc}) \circ b\,.$$

This shows that f is conjugated (by b) to the Klopsch's form $F(n, -\frac{1}{nc})$. This concludes the proof. □

2.3 Order p^n elements in the Nottingham group

The order p case is very well understood, but this is different for the order p^n case if $n \geq 2$. There are some general results known about order p^n elements with $n \geq 2$, which we will discuss at the end of this section. What makes the p^n case so different is that there are almost no explicit power series expansions known of order p^n elements.

In Jean's PhD-thesis [9] from 2008 she uses formal groups together with Lubin-Tate theory to construct an element of order 4.

Theorem 2.3.1 (Jean, 2008). *The power series*

$$\begin{aligned}\sigma(t) &= \sum_{n\geq 0} \frac{t^{2^n}}{(1+t)^{3\cdot 2^n-1}} \\ &= t + t^2 + t^5 + t^7 + t^{10} + \dots\end{aligned} \tag{2.6}$$

in $\mathcal{N}(\mathbf{F}_2)$ has order 4.

It turns out that we can explicitly write down the power series expansion of **??** as follows:

$$\begin{aligned}\sigma(t) &= t + \sum_{k\geq 0}\left(t^{2+8k} + t^{7+8k} + \sum_{\ell\geq 0}\left(t^{4\cdot 2^k(4\ell+3)} + t^{4\cdot 2^k(4\ell+1)+1}\right)\right) \\ &= t + t^2\frac{1+t^5}{1+t^8} + \sum_{k\geq 2} t^{2^k}\frac{t^{2^{k+1}}+t}{t^{2^{k+2}}+1}\,.\end{aligned}$$

The series in this form was independently obtained by Byszewski and Cornelissen [4] in 2017 using a different method, namely by means of p-automata, to find new power series of order p^n.

In 2010 Chinburg and Symonds [6] gave a new example of an order 4 power series σ and in [3] they also give a formula for its inverse τ. They found this example by considering an elliptic curve in $\mathbb{P}^2_k$ which is stabilized by an order 4 automorphism σ of $\mathbb{P}^2_k$, considering the action on the completion of a local ring of a fix point of σ gave the power series in the next lemma. In [3] is shown that this specific method for constructing finite order power series is limited to the case $p^n = 4$.

Theorem 2.3.2 (**Chinburg and Symonds, 2010**). *The power series*

$$\begin{aligned}\sigma(t) &= t + t^2 + \sum_{k\geq 0}\sum_{\ell=0}^{2^k-1} t^{6\cdot 2^k+2\ell} \\ &= t + t^2 + t^6 + t^{12} + t^{14} + \dots\end{aligned}$$

and its inverse

$$\begin{aligned}\tau(t) &= \sum_{k\geq 0} t^{3\cdot 2^k-2} + \sum_{\ell\geq 2} t^{2^\ell-2} \\ &= t + t^2 + t^4 + t^6 + t^{10} + \dots\end{aligned}$$

both have order 4 in $\mathcal{N}(\mathbf{F}_2)$.

The above three examples of finite order power series in $\mathcal{N}(\mathbf{F}_p)$ were since 2010 the only examples of non-prime order elements. In Chapter 4 we construct, using 2-automata, five more explicit power series of order 4 in $\mathcal{N}(\mathbf{F}_2)$. The formulas are however not as simple as the previous three.

Each of the above three power series of order 4 satisfies an algebraic equation over $\mathbf{F}_2(t)$. In particular we have for the power series $\sigma(t)$ in Lemma 2.3.1 that

$$(1+t)\sigma(t)^2 + (1+t^2)\sigma(t) + t = 0\,.$$

The power series $\sigma(t)$ and $\tau(t)$ in Lemma 2.3.2 satisfy

$$(1+t^2)\sigma(t)^2 + \sigma(t) + t = 0$$

and

$$t^2\tau(t)^2 + \tau(t) + t + t^2 = 0\,.$$

The fact that each of these three equations has degree 2 makes it straightforward to find an expression for the power series expansion of σ. The first thing we have to do is putting the algebraic equation of σ into the form $A^2 + A = B$. Then a solution (given that it makes sense) is given by

$$A = B + B^2 + B^4 + B^{16} + \dots\,.$$

Working backwards to a formula for σ, we need to check that σ is the only solution to the algebraic equation satisfying $\sigma(t) \equiv t \mod t^2$. Doing so for σ and τ in [6] gives

$$\sigma(t) = \frac{\sum_{n\geq 0}(t+t^3)^{2^n}}{1+t^2}$$

and

$$\tau(t) = \frac{\sum_{n\geq 0}(t^3+t^4)^{2^n}}{t^2}\,.$$

From the point of view of solving algebraic equations these three power series are not difficult to construct if the algebraic equation is known. It turns out in general that generating algebraic equations for order p^n power series in $\mathcal{N}(\mathbf{F}_p)$ is not difficult (see Section 4.1). However, solving these algebraic equations becomes almost impossible if the degree exceeds 2. Moreover it is not known whether we can read off from an algebraic equation if it has a power series expansion which can explicitly be written down.
An algebraic equation can be used to compute the coefficients of one of its solutions up to an arbitrary order, but this gives no insight in the existence of a closed formula for it. We propose to solve this in certain cases by using p-automata. Our strategy is basically this: we construct a directed graph which "computes" the coefficients of an algebraic power series and then we hope that this graph contains some structure which we can use to give an explicit closed formula.

There are some more general things known about order p^n elements in $\mathcal{N}(\mathbf{F}_p)$. We will use some parts of it later.

In [10] Jean gives a description of the conjugacy classes of elements of order p^n in $\mathcal{N}(\overline{\mathbf{F}}_p)$ ($\overline{\mathbf{F}}_p$ denotes the algebraic closure of $\mathbf{F}_p$) in terms of the Witt vectors $W_n(\overline{\mathbf{F}}_p)$. Using Witt vectors she constructs a totally ramified cyclic Galois extension of $\mathbf{F}_p(\!(t)\!)$ of degree p^n for which a generator of the Galois group $\langle\sigma\rangle$ corresponds to an order p^n element in $\mathcal{N}(\overline{\mathbf{F}}_p)$. She shows that by choosing the Witt vector in an appropriate way one can also specify the depth sequence of an order p^n element (Jean actually does not use the terminology of a depth sequence but instead the lower breaks, these two notions are equivalent as Lubin remarks in Observation 8 in [14]).

Using local class field theory Lubin [14] gives an iterative method for calculating a power series of an order p^n element up to some order. Also he shows that there are up to conjugacy only finitely many elements with a given depth sequence. In particular he shows in the case $p = 2$ for the depth sequence $(1, 3)$ that there are at most 2 different conjugacy classes. It follows that from the three known order 4 elements in this section at least two are conjugated. The following Proposition makes precise which are and which are not conjugated.

Proposition 2.3.3. *The two power series in Lemma 2.3.2 are not conjugated and the power series in Lemma 2.3.1 is conjugated in $\mathcal{N}(\mathbf{F}_2)$ to the second power series in Lemma 2.3.2.*

Proof. Suppose the two power series in Lemma 2.3.2 are conjugated. Then there exists an element $f \in \mathcal{N}(\mathbf{F}_2)$ such that $f \circ \sigma = \tau \circ f$. Write $f(t) = t + a_2 t^2 + \ldots + a_5 t^5$, computing the coefficients of t^4 and t^5 in $f \circ \sigma = \tau \circ f$ gives

$$a_2 + a_3 + a_4 = 1 + a_2^2 + a_4 \quad \text{and} \quad a_3 + a_5 = a_5 \, .$$

We are working over $\mathbf{F}_2$ so the first equation gives $a_3 = 1$ and the second equation gives $a_3 = 0$, a contradiction. In a similar way we can prove the second assertion (again only the coefficients of t^4 and t^5). $\square$

Chapter 3

Automata

In this chapter we introduce the theory of p-automata and p-automatic sequences. The most important theorem of this chapter is a theorem by Christol which relates p-automatic sequences to algebraic power series. The first two sections are based upon the treatment of the theory of p-automata in [1], but are completely rewritten, including the proofs. In this way a quick introduction is possible. Throughout this chapter p denotes a prime number.

3.1 p-Automata

In this section we start by introducing a directed multigraph with a label for every vertex and edge. This a generalisation of the notion of a (directed) graph. This is followed up with the introduction of the p-automaton, p-automatic sequences and their corresponding p-kernel. Finally we give a proof of a theorem by Christol, that relates p-automatic sequences to the algebraicity of the corresponding power series.

Definition 3.1.1. *A* directed multigraph *is a pair (V, E) consisting of a subset V of $S \times I$ and a subset E of $V \times V \times I$ where S, I are two sets. The sets V and E have to satisfy the following two conditions:*

- *For every $s \in S$ there exists precisely one $i \in I$ such that $v = (s, i) \in V$. This $i \in I$ is called the label of v.*
- *If $e = (v, w, i) \in E$ then $v, w \in V$. The elements v and w are called respectively the initial and terminal vertex of e; the element i is called the label of e.*

Elements of S, V and E are called respectively vertices, labeled vertices *and* labeled directed edges*; the set I acts as the set of labels. An element of E of the form (x, x, i) is called a loop. We call a directed multigraph (V, E)* finite *if the sets S and I are both finite.*

Remark 3.1.2. We will only work with labeled vertices and labeled directed edges and not with ordinary (unlabeled) graphs. Therefore we call elements of V and E respectively vertices and edges. Note that we allow multiple edges between two vertices; these edges then necessarily need to have different labels.

Definition 3.1.3. *Let (V, E) be a directed multigraph and $v \in V$ a vertex. Write $N^+(v)$ for the set of edges in E with v as initial vertex, so*

$$N^+(v) = \{w \in V \mid (v, w, i) \in E \text{ for some } i\}$$

and define $N^-(v)$ as the set of edges having v as terminal vertex, so

$$N^-(v) = \{w \in V \mid (w, v, i) \in E \text{ for some } i\}\,.$$

Write $\deg^+(v)$ and $\deg^-(v)$ for the cardinalities of the sets $N^+(v)$ and $N^-(v)$ respectively.

Loops centered at some vertex v are counted in both $N^+(v)$ and $N^-(v)$.

Example 3.1.4. One can visualise a directed multigraph by using the usual visualisation of a graph, but we have instead of points large circles with a label inside, arrows instead of lines and each arrow has a label. An example of a directed multigraph is given in **??**, circles are vertices, arrows are edges and numbers are labels (the word "Start" will be explained later).

Recall the base p expansion of a natural number. Let $n \in \mathbf{Z}_{>0}$ be a natural number. Then there exists a unique integer $m \geq 0$ and unique integers $0 \leq x_0, \ldots, x_m \leq p-1$ with $x_m \neq 0$ such that

$$n = x_0 + x_1 p + x_2 p^2 + \ldots + x_m p^m = \sum_{i=0}^{m} x_i p^i\,.$$

The next definition introduces the set S_p of all finite sequences in $\mathbf{F}_p$ which we equip with the operation of concatenation.

Definition 3.1.5. *Write S_p for the set of all finite sequences in $\mathbf{F}_p$, so*

$$S_p = \bigcup_{n=1}^{\infty} \mathbf{F}_p^n\,.$$

Let $a, b \in S_p$ be elements with $a = (a_0, \ldots, a_{m-1})$ and $b = (b_0, \ldots, b_{n-1})$. Define the concatenation of a and b, denoted by ab, by

$$ab := (a_0, \ldots, a_{m-1}, b_0, \ldots, b_{n-1}) \in \mathbf{F}_p^{m+n} \subseteq S_p\,.$$

For an element $a \in \mathbf{F}_p^n$ we write $|a| = n$ for the number of entries of a. Let $n \geq 0$, we write 0^n for the sequence $(0, \ldots, 0) \in \mathbf{F}_p^n$ (if $n = 0$ then we regard 0^0 as non-existent).

Note that S_p is just short of an identity element to being an associative monoid. In order to go back and forward from S_p to $\mathbf{Z}_{>0}$ we need the following two maps.

Definition 3.1.6. *Define the map $(.)_p : \mathbf{Z}_{>0} \to S_p$ by*

$$(n)_p = (x_0, x_1, \ldots, x_m)$$

where $n = \sum_{i=0}^{m} x_i p^i$ with $x_m \neq 0$ is the base p expansion.
Conversely define the map $[.]_p : S_p \to \mathbf{Z}_{>0}$ by

$$[a]_p = \sum_{i=0}^{n} a_i p^i$$

for $a = (a_0, \ldots, a_n) \in S_p$.

The map $(.)_p$ associates the p-adic digits to a natural number and $[.]_p$ associates a natural number to a sequence of p-adic digits. For a natural number n we see that $|(n)_p|$ equals the number of digits of n in the base p expansion and moreover we have the identity $[(n)_p]_p = n$ which is easily verified. Note however that $([a]_p)_p = a$ does not hold for all $a \in S_p$. Take for example $a = (1, 0)$. Then $[(1, 0)]_p = 1$ and $(1)_p = (1)$ but $(1) \neq (1, 0)$. The definition of $[.]_p$ allows us to rewrite the definition of $\Lambda_r(t^n)$ in Definition 1.1.7 by

$$\Lambda_r(t^n) = \begin{cases} t^m & \text{if } n = p^\ell m + [r]_p \text{ for some } m \in \mathbf{Z}; \\ 0 & \text{otherwise.} \end{cases}$$

The next definition introduces the concept of a p-automaton.

Definition 3.1.7 (**p-Automaton**). *A* p-automaton *is a triplet (V, E, s) consisting of a finite directed multigraph (V, E) and an element $s \in V$, called the start vertex, which satisfy the following two properties:*

- *The set of labels I as in the definition of a directed multigraph (Definition 3.1.1) equals $\mathbf{F}_p$.*
- *For every vertex $v \in V$ and label $i \in \mathbf{F}_p$ there exists a unique $w \in V$ such that $(v, w, i) \in E$.*

Moreover, a p-automaton is called leading zeros invariant *if it has the property that the labels of the initial and terminal vertex of any edge with label 0 are equal.*

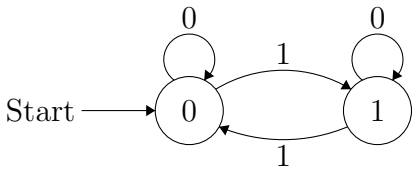


Figure 3.1: A 2-automaton generating the Thue-Morse sequence.

See Figure 3.1 for an example of a leading zeros invariant 2-automaton, the arrow with "Start" next to it points towards the start vertex. An example of automaton which is not leading zeros invariant can be found in (3.2). The second condition says that every vertex has precisely p outgoing edges and each of those edges has a unique label from $\mathbf{F}_p$. The next definition introduces a way to walk through a p-automaton using an element of S_p. We will use this to turn a p-automaton into a machine which generates a sequence.

Definition 3.1.8. *Let $G = (V, E, s)$ be a p-automaton and $x = (x_0, \ldots, x_{n-1}) \in S_p$ some element. We say that the vertex $v \in V$ is* defined *by x if there exists a sequence $v_0, v_1, \ldots, v_n$ of vertices in V satisfying $v_0 = s$, $v_n = v$ and $(v_i, v_{i+1}, x_i) \in E$ for all $0 \leq i \leq n-1$. Although we have not defined $(0)_p$, we make the convention that $(0)_p$ defines the start vertex s.*

Note that every element of S_p defines a unique vertex in a p-automaton. We are ready to define the notion of a p-automatic sequence in $\mathbf{F}_p$.

Definition 3.1.9 (**p-Automatic sequence**)**.** *Let $a = (a_n)_{n\geq 0}$ be a sequence in $\mathbf{F}_p$. The sequence a is called* p-automatic *if there exists a p-automaton G such that a_n equals the label of the vertex defined by $(n)_p$ in G. In this case we sometimes also say that G* generates *a or that G* generates *the power series $\sum_{n\geq 0} a_n t^n \in \mathbf{F}_p[\![t]\!]$.*

Example 3.1.10. Define the sequence $a = (a_n)_{n\geq 0}$ as follows: if $(n)_2$ contains an even number of ones then $a_n = 0$ and if $(n)_2$ contains an odd number of ones then $a_n = 1$. This sequence is known as the Thue-Morse sequence. A 2-automaton generating a is given in Figure 3.1.

To every sequence in $\mathbf{F}_p$ we can associate the so-called p-kernel $K_p(a)$ defined below. It turns out that this is a crucial object in the theory of p-automata because it allows us to distinguish between p-automatic sequences and ordinary sequences in $\mathbf{F}_p$, see also Theorem 3.1.12.

Definition 3.1.11 (**p-Kernel**)**.** *Let $a = (a_n)_{n\geq 0}$ be a sequence in $\mathbf{F}_p$. Define the* p-kernel *of a as the set*

$$K_p(a) = \{(a_{p^m n+r})_{n\geq 0} \mid m \geq 0, 0 \leq r < p^m\}$$

consisting of all subsequences of a for which the indices form an arithmetic progression with difference p^m and initial number r.

For a sequence a in $\mathbf{F}_p$ the elements of the p-kernel $K_p(a)$ are generated by a p-automaton which is closely related to the p-automaton that generates a. The first part of the proof of Theorem 3.1.12 shows this.

Theorem 3.1.12 (Eilenberg). *Let $a = (a_n)_{n\geq 0}$ be a sequence in $\mathbf{F}_p$, then a is p-automatic if and only if the p-kernel $K_p(a)$ of a is finite.*

Proof. For ($\Rightarrow$), we first consider some general construction. Let $G = (V, E, s)$ be a p-automaton, $v \in V$ a vertex and let $w \in V$ be a vertex defined in (V, E, v) by an element $(0, \ldots, 0) \in S_p$ of some finite length or just v itself. Construct a new p-automaton, $G_{v,w}$, out of G as follows:

- Add a new vertex t with the same label as the vertex v.
- For each $(w, w', i_{ww'}) \in N^+(w)$ add the directed edge $(t, w', i_{ww'})$.
- Change the start vertex from s to t.

One can verify that all conditions of a p-automaton are fulfilled, so $G_{v,w}$ is a p-automaton. What we have basically done here is that we have added a new vertex t which is in every aspect, except possibly for its label, the same as the vertex w.

Suppose the p-automaton $G = (V, E, s)$ generates the p-automatic sequence a. Fix a sequence $b \in K_p(a)$ with $b_n = a_{p^m n+r}$ for all $n \geq 0$ for some fixed $m \geq 0$ and $0 \leq r < p^m$. Let v and w be the end vertices of the walks defined by $(r)_p$ and $(r)_p 0^{m-|(r)_p|}$ in G respectively. We claim that the p-automaton $G_{v,w}$ generates the sequence $(b_n)_{n\geq 0}$.
For $n = 0$, note that the label of t is the same as the label of v by definition which equals $a_r = b_0$. By construction of $G_{v,w}$ we have for each $n \geq 1$ that the vertex defined by $(r)_p 0^{m-|(r)_p|}(n)_p = (p^m n + r)_p$ in G is the same as the vertex defined by $(n)_p$ in $G_{v,w}$. This proves the claim. It follows that every sequence $b \in K_p(a)$ is generated by a p-automaton of the form $G_{v,w}$ for some $v, w \in V$. Since V is finite this shows that there can only be finitely many elements in $K_p(a)$.

For ($\Leftarrow$), suppose that the p-kernel $K_p(a)$ is finite. We will construct a p-automaton which generates a. Take for the set of vertices V the pairs (b, b_0) where $b = (b_0, \ldots) \in K_p(a)$ and let the set of edges E be defined by $((b, b_0), (c, c_0), i) \in E$ if and only $\Lambda_i(b) = c$ where $b = (b_0, \ldots), c = (c_0, \ldots) \in K_p(a)$. Consider the p-automaton $(V, E, (a, a_0))$, we are left to show that this p-automaton indeed generates a. If $n = 0$, then $(0)_p$ defines by definition a_0 and if $n > 0$ consider the walk defined by $(n)_p$, it has as its final vertex $(\Lambda_{(n)_p}(a), a_n)$ since $\Lambda_{(n)_p}(a) = (a_{n+mp^{|(n)_p|}})_{m\geq 0}$. It follows that a is a p-automatic sequence. □

Remark 3.1.13. Using the notation of the first part of the proof of Theorem 3.1.12, note that if G is leading zeros invariant then any element of $K_p(a)$ is generated by (V, E, v) for

some $v \in V$. Indeed, then we have in the construction $v = w$, hence $\#K_p(a) \leq \#V$. In particular the whole construction of $G_{v,w}$ is unnecessary. On the other hand, if G is not leading zeros invariant then something similar still holds. Namely, for any $b = (b_n)_{n\geq 0} \in K_p(a)$ there exists a vertex $v \in V$ such that the sequence $(c_n)_{n\geq 0}$ generated by the p-automaton (V, E, v) satisfies $b_n = c_n$ for all $n \geq 1$ (but possibly $b_0 \neq c_0$). This shows that we always have the bound $\#K_p(a) \leq p \cdot \#V$. Theorem 3.1.15 shows that we can indeed have $K_p(a) > \#V$.

It is straightforward to construct two different p-automata generating the same sequence. This brings us to a notion of equivalent automata: two p-automata are called equivalent if they generate the same sequence. This notion of equivalent automata gives a partition of the set of all leading zeros invariant p-automata. Consider a class of p-automata in this partition. In this class there is a p-automaton with a minimal number of vertices. The following lemma relates this number to the p-kernel.

Lemma 3.1.14. *Let a be a p-automatic sequence. There exists a leading zeros invariant p-automaton generating the sequence a with a minimal number of vertices, more specifically this minimal number of vertices equals $\#K_p(a)$.*

Proof. The second part of the proof of Theorem 3.1.12 shows the existence of a leading zeros invariant p-automaton (V, E, s) generating a with precisely $\#K_p(a)$ vertices. Indeed, if $((b, b_0), (c, c_0), 0) \in E$ then $\Lambda_0(b) = c$ which implies that $b_{pn} = c_n$ for all $n \geq 0$ and specifically $b_0 = c_0$. On the other hand, the first part of Theorem 3.1.12 shows that if a p-automaton is leading zeros invariant then the number of vertices is at least $\#K_p(a)$. This proves the lemma. □

Example 3.1.15. Consider the 2-automaton in Figure 3.2, generating the sequence a. It is clear that this is an example of an automaton which is not leading zeros invariant. This is illustrated by the fact that $\#K_2(a) = 9$ but the number of vertices equals 6.

Example 3.1.16. Consider the 2-automaton in Figure 3.3. This 2-automaton is leading zeros invariant as one can see from the graph. By the proof of Theorem 3.1.12 we see that the 2-kernel $K_2(a)$ is contained in the set

$$\{(a_n)_{n\geq 0}, (a_{2n})_{n\geq 0}, (a_{1+2n})_{n\geq 0}, (a_{2+4n})_{n\geq 0}, (a_{1+4n})_{n\geq 0}, (a_{5+8n})_{n\geq 0}\}$$

where a is the sequence generated by the 2-automaton. By computing the first 7 terms of each sequence one finds that all these sequences are different, hence $\#K_2(a) = 6$.

The next lemma gives an equivalent criterion for a sequence to be p-automatic.

Lemma 3.1.17. *Let $a = (a_n)_{n\geq 0}$ be a sequence in $\mathbf{F}_p$. Then a is p-automatic if and only if there exists a finite set S satisfying the following two conditions:*

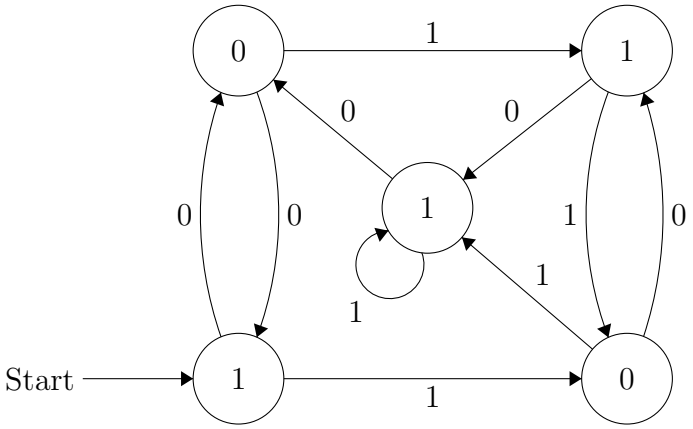


Figure 3.2: A 2-automaton which is not leading zeros invariant.

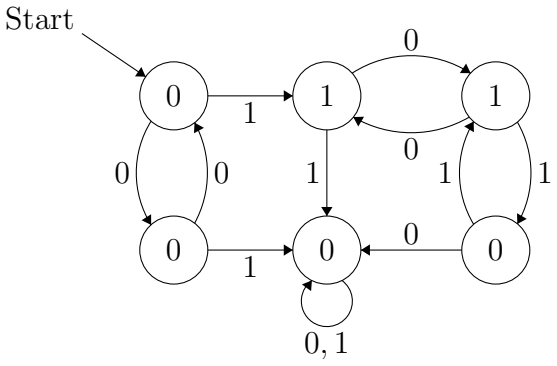


Figure 3.3: A 2-automaton generating the power series $A(t) = \frac{t}{\sqrt[3]{1+t^3}} \in \mathbf{F}_2[\![t]\!]$.

(1) $A = \sum_{n\geq 0} a_n t^n \in S$;

(2) for all $B \in S$ *and for all integers* $0 \leq r < p$ *we have* $\Lambda_r(B) \in S$.

The last condition says that the set S is "stable" under the Cartier operator.

Proof. Write $K_p(a) = \{a^{(1)}, \ldots, a^{(k)}\}$ for the elements of the p-kernel. Take for S the set

$$S = \{\sum_{n\geq 0} a_n^{(i)} t^n \mid 1 \leq i \leq k\}\,.$$

We clearly have $A \in S$. For $A' = \sum_{n\geq 0} a_n^{(i)} t^n$ we have

$$\Lambda_r(A') = \sum_{n\geq 0} a_{pn+r}^{(i)} t^n$$

and since $K_p(a)$ is finite there exists some $1 \leq j \leq k$ such that $(a_{pn+r}^{(i)})_{n\geq 0} = (a_n^{(j)})_{n\geq 0}$. It follows that $\Lambda_r(B) \in S$ and so both conditions do indeed hold.

Conversely, suppose that both conditions are met for some finite set S. Let $m \geq 0$ and $0 \leq r < p^m$. By definition of the Cartier operator we have

$$\Lambda_{(r)_p 0^{m-|(r)_p|}}(A) = \sum_{n\geq 0} a_{p^m n+r} t^n\,.$$

Using the second condition we get $\sum_{n\geq 0} a_{p^m n+r} t^n \in S$. This shows that the corresponding power series of any element from $K_p(a)$ is in S. Since S is finite so is $K_p(a)$. □

The next theorem (see also [7]) is by far the most important result of this chapter. It gives a surprising and beautiful criterion for a sequence to be p-automatic. It relates p-automatic sequences to algebraic power series.

Theorem 3.1.18 (Christol, 1979). *The power series* $A = \sum_{n\geq 0} a_n t^n \in \mathbf{F}_p[\![t]\!]$ *is algebraic over* $\mathbf{F}_p(t)$ *if and only if the sequence* $a = (a_n)_{n\geq 0}$ *is* p*-automatic.*

Proof. Assume that the sequence a is p-automatic. By Theorem 3.1.12 the p-kernel $K_p(a)$ is finite. Write $K_p(a) = \{a^{(1)}, \ldots, a^{(m)}\}$ and set $a^{(1)} = a$. Using linear algebra we will show that A satisfies an algebraic equation over $\mathbf{F}_p(t)$.

Define for each $1 \leq i \leq m$ the power series $A_i(t) = \sum_{n\geq 0} a_n^{(i)} t^n$ and for each $k \geq 0$ let V_k be the vector space over $\mathbf{F}_p(t)$ spanned by $A_1(t^{p^k}), \ldots, A_m(t^{p^k})$, so

$$V_k = \mathrm{Span}_{\mathbf{F}_p(t)}(A_1(t^{p^k}), \ldots, A_m(t^{p^k}))\,.$$

In particular we have $\dim V_k \leq m$ for every $k \geq 0$. By substituting t^{p^k} for t in the first property of Lemma 1.1.9 we find that

$$A_i(t^{p^k}) = \sum_{0 \leq r < p} t^r \sum_{n \geq 0} a^{(i)}_{pn+r} \left(t^{p^{k+1}}\right)^n \tag{3.1}$$

for every $1 \leq i \leq m$. By definition of the p-kernel we have $(a^{(i)}_{pn+r})_{n \geq 0} \in K_p(a)$ and therefore the power series $\sum_{n \geq 0} a^{(i)}_{pn+r}(t^{p^{k+1}})^n$ equals $A_j(t^{p^{k+1}})$ for some $1 \leq j \leq m$. We have $A_i(t^{p^k}) \in V_{k+1}$ for every $1 \leq i \leq m$, combining this with the definition of V_k we get an increasing sequence of vector spaces $V_0 \subseteq V_1 \subseteq V_2 \subseteq \ldots$. For the vector space V_m this implies that the power series

$$A(t), A(t)^p, \ldots, A(t)^{p^m}$$

are all contained in V_m (note that $A(t)^p = A(t^p)$). The vector space V_m has dimension at most m, so there must be a linear dependence among these $m+1$ power series. This shows the existence of $B_0, \ldots, B_m \in \mathbf{F}_p(t)$ such that

$$B_0 A(t) + \ldots + B_m A(t)^{p^m} = 0\,.$$

Which is an algebraic relation for A.

Conversely, assume that the power series A is algebraic over $\mathbf{F}_p(t)$. The idea for proving that a is p-automatic is to construct an explicit finite set of Laurent series which is mapped into itself under the Cartier operators. By Theorem 1.1.11 there exists polynomials $B_0, \ldots, B_m \in \mathbf{F}_p[t]$ with $B_0 \neq 0$ such that

$$B_0 A + B_1 A^p + \ldots + B_m A^{p^m} = 0\,.$$

The polynomial B_0 is invertible in $\mathbf{F}_p(\!(t)\!)$ because $B_0 \neq 0$. Define the element $T \in \mathbf{F}_p(\!(t)\!)$ by $T = AB_0^{-1}$ and for each $1 \leq i \leq m$ let C_i be the polynomial $C_i = -B_i B_0^{p^i - 2} \in \mathbf{F}_p[t]$. We compute

$$\begin{aligned}\sum_{k=1}^{m} C_k T^{p^k} &= -\sum_{k=1}^{m} B_k B_0^{p^k-2} A^{p^k} B_0^{-p^k} = -\sum_{k=1}^{m} B_k B_0^{-2} A^{p^k} \\ &= B_0^{-2}\left(B_0 A - \sum_{k=0}^{m} B_k A^{p^k}\right) = AB_0^{-1} = T\,.\end{aligned}$$

So far we have only rewritten our algebraic equation to another equation in the variable T for which the coefficient of T equals 1. Write

$$N = \max\{\deg B_0, \max_{1 \leq i \leq m}\{\deg C_i\}\}$$

and define the set S by

$$S = \{\sum_{k=0}^{m} D_k T^{p^k} \in \mathbf{F}_p(\!(t)\!) \mid D_k \in \mathbf{F}_p[t] \text{ and } \deg D_k \leq N \text{ for all } 0 \leq k \leq m\}\,.$$

From the definition of S it is clear that S is a finite set. We will show that S is mapped into itself under the Cartier operators. Let $\sum_{k=0}^{m} D_k T^{p^k} \in S$ be a Laurent series and let $0 \leq r < p$ be some integer. Applying Λ_r to this Laurent series gives

$$\begin{aligned}
\Lambda_r\left(\sum_{k=0}^{m} D_k T^{p^k}\right) &= \Lambda_r\left(D_0 T + \sum_{k=1}^{m} D_k T^{p^k}\right) \\
&= \Lambda_r(D_0 T) + \sum_{k=1}^{m} \Lambda_r\left(D_k T^{p^k}\right) \\
&= \sum_{k=1}^{m} \Lambda_r\left(D_0 C_k T^{p^k}\right) + \sum_{k=1}^{m} T^{p^{k-1}} \Lambda_r(D_k) \\
&= \sum_{k=1}^{m} T^{p^{k-1}} \Lambda_r(D_k + D_0 C_k)\,.
\end{aligned}$$

For each $1 \leq k \leq m$ we can bound the degree of the polynomial $D_k + D_0 C_k$ from above by using Remark 1.1.10

$$\deg \Lambda_r(D_k + D_0 C_k) \leq \frac{\deg(D_k + D_0 C_k)}{p}\,. \tag{3.2}$$

Since $\deg D_k, \deg C_k \leq N$ we have $\deg(D_k + D_0 C_k) \leq 2N$ and therefore we find

$$\deg \Lambda_r(D_k + D_0 C_k) \leq \frac{2N}{p} \leq N\,.$$

This shows that $\Lambda_r\left(\sum_{k=0}^{m} D_k T^{p^k}\right) \in S$ and so S is indeed mapped into itself by the Cartier operators. Finally, note that $A = B_0 T \in S$ and so it follows from Lemma 3.1.17 that the sequence $a = (a_n)_{n \geq 0}$ is p-automatic. □

Remark 3.1.19. If we only know that a sequence is p-automatic then the above theorem does not give us any way to compute the algebraic equation for the corresponding power series. However, if the p-automaton is given then we can follow the steps of the proof to find an algebraic equation. This comprises expressing each of the elements $A(t), \ldots, A(t^{p^m})$ as linear combinations of the power series $A_1(t^{p^m}), \ldots, A_m(t^{p^m})$ and then finding a linear dependence between these linear combinations. It turns out that in practice this can be quite a challenging task because the computations involve complicated rational functions in $\mathbf{F}_p(t)$. Moreover the degree of the minimal polynomial of A is often much smaller than the degree of the algebraic equation obtained by doing this linear algebra. So it is often necessary to factor the obtained polynomial into irreducible factors.

3.2 The p-automata of the power series $(1+at)^{-1/n}$

As an illustration of p-automata we give an algorithm for constructing a leading zeros invariant p-automaton that generates the coefficients of the power series $(1+at)^{-1/n}$, where $a \in \mathbf{F}_p^\times$ and n is a positive integer with $\gcd(p,n) = 1$. Later we will show that with a slight modification we even have found the minimal p-automaton. We start with a lemma which relates the power series starting at a vertex v in a p-automaton to the power series generated by the terminal vertices of the outgoing edges of v.

Lemma 3.2.1. *Let (V,E,s) be a leading zeros invariant p-automaton. Consider a vertex $v \in V$ and let $v_i \in V$ be the vertices such that $(v,v_i,i) \in E$. Write $A = \sum_{n\geq 0} a_n t^n$ for the power series generated by (V,E,v) and A_i for the power series generated by (V,E,v_i). We then have the relation*

$$A = \sum_{0\leq r<p} t^r A_r(t)^p \,.$$

Proof. Using the first property of Theorem 1.1.9 we can write

$$A = \sum_{0\leq r<p} t^r \sum_{n\geq 0} a_{pn+r}(t^p)^n \,.$$

Since (V,E,s) is leading zeros invariant we have $\sum_{n\geq 0} a_{pn+r}t^n = A_r(t)$ for each $0 \leq r < p$. The result follows. □

The next theorem gives an algorithm for constructing a p-automaton of a class of power series.

Theorem 3.2.2. *Suppose $n \in \mathbf{Z}_{>0}$ with $\gcd(p,n) = 1$ and an element $a \in \mathbf{F}_p^*$ are given. Write $m = \mathrm{ord}_n(p)$ (so m is the least positive integer such that $p^m \equiv 1 \mod n$) and let $0 \leq x_i < p$ for $0 \leq i \leq m-1$ be integers such that*

$$\frac{p^m - 1}{n} = \sum_{i=0}^{m-1} x_i p^i \,.$$

Define the set T by

$$T = \{a^r \tbinom{s}{r} \mod p \mid s \in \{x_0, \ldots, x_{m-1}\}, 0 \leq r < p\}$$

and write $\langle T \rangle$ for the set of all finite products of elements of T. Let V be the set

$$\{(v_{i,j}, i) \mid i \in \langle T \rangle, j \in \mathbf{Z}/m\mathbf{Z}\}$$

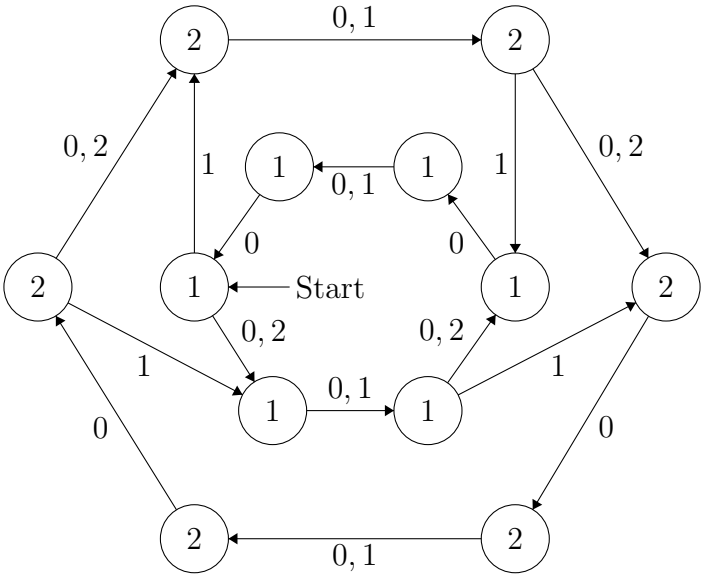


Figure 3.4: A 3-automaton generating the power series $(1+t)^{-1/7} \in \mathbf{F}_3[\![t]\!]$, the vertex with label zero and all edges towards it are left out.

and write E for the set

$$E = \{((v_{i,j}, i), (v_{\ell,j+1}, \ell), r) \mid \ell = a^r \binom{x_j}{r} i\}\,.$$

Then $G := (V, E, (v_{1,0}, 1))$ is a leading zeros invariant p-automaton which generates the power series $(1+at)^{-1/n}$.

Remark 3.2.3. The general structure of the p-automaton defined in Theorem 3.2.2 is as follows. We have $\#\langle T\rangle$ directed cycles of length m, the vertices in each such cycle all have the same label and these cycles are linked together in a certain way. For two examples see Figure 3.4 and Figure 3.5.

The graph defined in Theorem 3.2.2 has some very useful symmetry which is made precise in the next lemma. We will make use of this symmetry in the proof of Theorem 3.2.2.

Lemma 3.2.4. *For $0 \neq s \in \langle T\rangle$ define the map*

$$\varphi_s : G \to G \tag{3.3}$$

by sending the vertex $(v_{i,j}, i)$ to $(v_{si,j}, si)$. Then φ_s is a graph automorphism (of the underlying directed graph) of $G_{p,n,a}$ which preserves the labeling of the edges, that is for every edge $e \in E$ the edges e and $\varphi_s(e)$ have the same label.

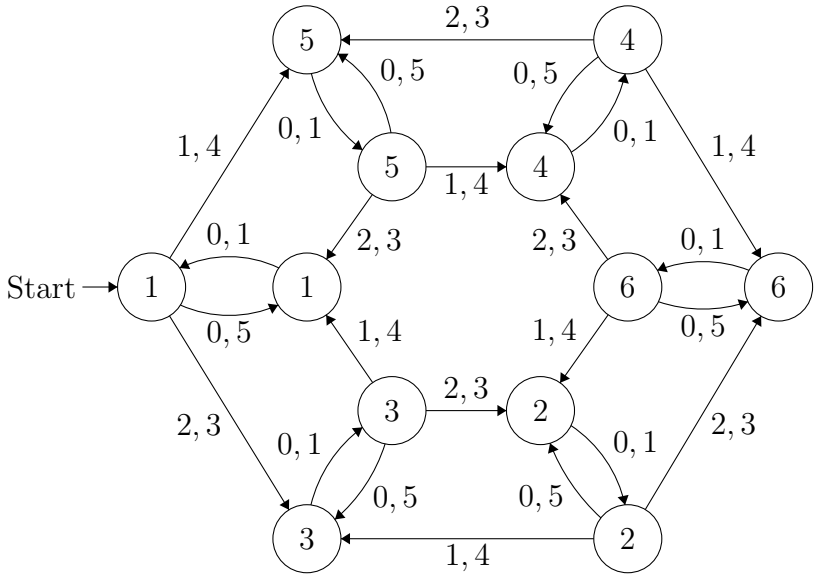


Figure 3.5: A 7-automaton generating the coefficients of the power series $(1+t)^{-1/4} \in \mathbf{F}_7[\![t]\!]$, the vertex with label zero and all edges towards it are left out.

Proof. Since $s \neq 0$ the map φ_s is bijective on the vertices V, we have $\ell = a^r \binom{x_j}{r} i$ if and only if $s\ell = a^r \binom{x_j}{r} si$ and so by definition of the set of edges E we have

$$((v_{i,j}, i), (v_{\ell,j+1}, \ell), r) \in E \Leftrightarrow ((v_{si,j}, i), (v_{s\ell,j+1}, \ell), r) \in E \tag{3.4}$$

It follows that φ_s is indeed a graph automorphism of G. □

We now give the proof of Theorem 3.2.2.

Proof. From the definition of G it follows that G has finitely many vertices, that each vertex has precisely p outgoing edges with each a different label form $\mathbf{F}_p$ and that

$$((v_{i,j}, i), (v_{\ell,j+1}, \ell), 0) \in E$$

if and only if $\ell = i$. This shows that G is a leading zeros invariant p-automaton.

Write $A_{i,j}$ for the power series generated by the p-automaton $(V, E, (v_{i,j}, i))$. Note that $A_{0,j} = 0$ for all $j \in \mathbf{Z}/m\mathbf{Z}$. We will use the symmetry described in Theorem 3.2.4 to show that for any non-zero $s \in \langle T \rangle$ we have $sA_{i,j} = A_{si,j}$ for every pair of indices i, j.
Let $s \in \langle T \rangle$ be non-zero and consider some integer $\ell \geq 0$. If $(\ell)_p$ defines the vertex $(v_{\alpha,\beta}, \alpha)$ in $(V, E, (v_{i,j}, i))$ then by Theorem 3.2.4 the sequence $(\ell)_p$ defines the vertex $(v_{s\alpha,\beta}, s\alpha)$ in $(V, E, (v_{si,j}, si))$. It follows immediately that $sA_{i,j} = A_{si,j}$.

Because $(v_{i,j}, i)$ has outgoing edges to the vertices $(v_{a^r\binom{x_j}{r}_{i,j+1}}, a^r\binom{x_j}{r}i)$ we get from Theorem 3.2.1 the relation

$$A_{i,j} = \sum_{0\le r<p} t^r A^p_{a^r\binom{x_j}{r}_{i,j+1}}. \tag{3.5}$$

Since $a^r\binom{x_j}{r} \in T$ we may apply the above remark to Equation (3.5), this gives

$$\begin{aligned} A_{i,j} &= \sum_{0\le r<p} t^r A^p_{a^r\binom{x_j}{r}_{i,j+1}} \\ &= \sum_{0\le r<p} \binom{x_j}{r} (at)^r A^p_{i,j+1} \\ &= (1+at)^{x_j} A^p_{i,j+1} \end{aligned}$$

for all i, j (since $\binom{x_j}{r} = 0$ for $r > x_j$). Iterating the above equality for $i = 1$ gives

$$\begin{aligned} A_{1,0} &= (1+at)^{x_0} A^p_{1,1} \\ &= (1+at)^{x_0+px_1} A^{p^2}_{1,2} \\ &\vdots \\ &= A^{p^{m-1}}_{1,m-1}(1+at)^{x_0+px_1+\ldots+p^{m-2}x_{m-2}} \\ &= A^{p^m}_{1,0}(1+at)^{\frac{p^m-1}{n}}. \end{aligned}$$

Since $A = A_{1,0} \neq 0$ we see that A satisfies the algebraic equation

$$1 = (1+at)^{\frac{p^m-1}{n}} A^{p^m-1}.$$

Because $A \equiv 1 \mod t$ we find by Corollary 1.1.2 that A equals the power series $(1+at)^{-1/n}$. This is exactly what we wanted to show. □

Remark 3.2.5. In the above description of the p-automaton $G_{p,n,a}$ we see that the label of a terminal vertex of an outgoing edge from a vertex with label zero also has label zero. Therefore we can replace all vertices with label 0 in (V, E) with one vertex with label 0, so this vertex has p loops attached to it. This reduces the number of vertices but the new p-automaton still generates the same power series. In Theorem 3.2.6) we proof that this is also a minimal p-automaton for $(1+at)^{-1/n}$.

Lemma 3.2.6. *Consider the p-automaton constructed in Theorem 3.2.2. This is a minimal p-automaton for the power series $(1+at)^{-1/n}$ if we merge all vertices with label zero.*

Proof. The end points of the outgoing edges of each vertex with label zero has label zero. This shows that we can merge all the vertices with label zero into one vertex with label zero and this new p-automaton still generates $(1+at)^{-1/n}$. We will use the same notation as in Theorem 3.2.2 but the vertices with label zero all coincide.

If we disregard the vertex with label zero, then we get a union of some m-cycles, each m-cycle having only vertices with identical labels, which are connected in some way. If we can show that each vertex of an arbitrary m-cycle generates a different sequence, then we are done. By the graph automorphism φ_s defined in Definition 3.2.4 it suffices to do this for one such cycle. Let v, w be two different vertices with label 1 in G and suppose that (V, E, v) and (V, E, w) generate the same sequence. Let $k > 0$ be an integer such that $(v_{1,0}, 1)$ is defined by 0^k in (V, E, v) and let $(v_{1,i}, 1)$ be the vertex defined by 0^k in (V, E, w). Since (V, E, v) and (V, E, w) generate the same sequence so do $(V, E, (v_{1,0}, 1))$ and $(V, E, (v_{1,i}, 1))$, the same holds for $(V, E, (v_{1,i}, 1))$ and $(V, E, (v_{1,2i}, 1))$, etc.. It follows that the p-automata $(V, E, v_{1,j})$ for $j \in \langle i \rangle \subseteq \mathbf{Z}/m\mathbf{Z}$ all generate the same power series.[1] Let $\ell \in \langle i \rangle$ be the smallest element then $\langle i \rangle = \langle \ell \rangle$ and $\ell \mid m$.
The p-automata $(V, E, v_{1,0})$ and $(V, E, v_{1,\ell})$ generate the same power series and therefore so do $(V, E, v_{1,s})$ and $(V, E, v_{1,\ell+s})$ for every $s \in \mathbf{Z}/m\mathbf{Z}$. The labels of the terminal vertices of the edges labeled 1 with begin vertices $v_{1,s}$ and $v_{1,\ell} + s$ respectively are ax_s and $ax_{\ell+s}$. Since $a \neq 0$ we find that $x_s = x_{\ell+s}$ holds for all $s \in \mathbf{Z}/m\mathbf{Z}$. This means that if we define $c = x_0 + x_1 p + \ldots + x_{\ell-1} p^{\ell-1}$ then we can write

$$\begin{aligned} \frac{p^m - 1}{n} &= x_0 + x_1 p + \ldots + x_{m-1} p^{m-1} \\ &= c + c p^{\ell} + \ldots + c p^{m-\ell} \\ &= c(1 + p^{\ell} + p^{2\ell} + \ldots + p^{m-\ell}) \\ &= c \frac{p^m - 1}{p^{\ell} - 1}\,. \end{aligned}$$

This implies that $n \mid p^{\ell} - 1$ and so $\mathrm{ord}_n(p) \mid \ell \mid m = \mathrm{ord}_n(p)$ hence $\ell = m$. The equality $\ell = m$ implies that $i = 0$ and this in turn implies that $v = w$. Which gives a contradiction. □

It turns out that changing the start vertex in G from Theorem 3.2.2 gives a p-automaton that generates a power series which is similar to $(1 + at)^{-1/n}$.

Lemma 3.2.7. *Using the notation of Theorem 3.2.2 we have that the power series $A_{s,j}$ generated by $(V, E, (v_{s,j}, s))$ equals the power series $A_{1,j}$ generated by $(V, E, (v_{1,j}, 1))$ multiplied with s.*

Proof. This is clear if $s = 0$, if $0 \neq s \in \langle T \rangle$ then this follows by the first part of the proof of Theorem 3.2.2. □

Lemma 3.2.8. *Using the notation of Theorem 3.2.2 we have that*

$$A_{1,j} = (1 + at)^{-(p^{m-j} \mod n)/n}$$

if $n \geq 2$ and $A_{1,j} = (1 + at)^{-1}$ if $n = 1$ for $j \in \mathbf{Z}/m\mathbf{Z}$.

[1] We write $\langle j \rangle$ for the subgroup of $\mathbf{Z}/m\mathbf{Z}$ generated by j.

Proof. If $n = 1$ then $m = 1$ and if $m = 1$ we can use Theorem 3.2.7 with $j = 0$ to prove the statement easily. Suppose that $m, n \geq 2$ and consider some $1 \leq j \leq m-1$. We can write

$$\begin{aligned}\frac{p^m - 1}{n} &= \sum_{k=0}^{m-1} x_k p^k \\ &= (x_0 + \ldots + x_{j-1}p^{j-1}) + p^j(x_j + \ldots + x_{m-1}p^{m-j-1}) \\ &= S_j + p^j T_j\end{aligned}$$

where $S_j = x_0 + \ldots + x_{j-1}p^{j-1}$ and $T_j = x_j + \ldots + x_{m-1}p^{m-j-1}$. By successively using the identity $A_{1,k} = (1+at)^{x_k} A_{1,k+1}^p$ we get

$$A_{1,j} = (1+at)^{x_j + x_{j+1}p + \ldots + x_{m-1}p^{m-j-1}} A_{1,0}^{p^{m-j}} = (1+at)^{-(p^{m-j} - nT_j)/n}.$$

We have $p \nmid \frac{p^m-1}{n}$ so $x_0 \neq 0$ and hence for $1 \leq j \leq m-1$ we have $1 \leq S_j \leq p^j - 1$ since $x_0 \neq 0$. This gives

$$1 \leq \frac{p^m - 1}{n} - p^j T_j \leq p^j - 1$$

implying

$$\frac{n}{p^j} \leq p^{m-j} - \frac{1}{p^j} - nT_j \leq n\left(1 - \frac{1}{p^j}\right)$$

which is equivalent to

$$\frac{n+1}{p^j} \leq p^{m-j} - nT_j \leq n - \frac{n-1}{p^j}.$$

If $n \geq 2$ then $1 \leq p^{m-j} - nT_j < n$ so the result follows. □

By looking at the construction of the p-automaton in Theorem 3.2.2 we can say something about the size of the vertex set.

Lemma 3.2.9. *The minimal p-automaton generating the power series $(1+at)^{-1/n}$ has at most $m(\#\langle T\rangle - 1) < mp$ vertices.*

Proof. That the number of vertices is at most $m(\#\langle T\rangle - 1) + 1$ reflects the merging of all vertices with label zero (if there are any vertices with label zero). The inequality follows from the fact that $\langle T\rangle \subseteq \mathbf{F}_p$. □

Chapter 4

New order 4 elements in $\mathcal{N}(\mathbf{F}_2)$

In this chapter we give a method, outlined in [4], for obtaining algebraic equations of finite order elements in $\mathcal{N}(\mathbf{F}_p)$. This uses the theory of automata developed in Chapter 3. We use this in the special case $p = 2$, which results in five new explicit power series in $\mathcal{N}(\mathbf{F}_2)$ of order 4.

4.1 Algebraic equations of order p^n elements in $\mathcal{N}(\mathbf{F}_p)$

Using the theory we have introduced in the previous chapters we give a method for constructing algebraic equations of finite order p^n elements in $\mathcal{N}(\mathbf{F}_p)$.

Consider the rational function field $\mathbf{F}_p(z)/\mathbf{F}_p$ and a truncated Witt vector $\beta \in W_n(\mathbf{F}_p(z))$ with $\beta_0 \notin \wp(\mathbf{F}_p(z))$. Let $\alpha \in W_n(\overline{\mathbf{F}_p(z)})$ be an element satisfying $\wp(\alpha) = \beta$. By Theorem 1.2.3 we have a Galois extension $F/\mathbf{F}_p(z) = \mathbf{F}_p(z, \alpha)/\mathbf{F}_p(z)$ of function fields with Galois group cyclic of degree p^n. Assume that $P \in \mathbb{P}_{\mathbf{F}_p(z)}$ is a place which is totally ramified in the function field extension $F/\mathbf{F}_p(z)$. Write $Q \in \mathbb{P}_F$ for the unique place above P; then $e(Q|P) = p^n$ and $f(Q|P) = 1$. In particular Q is a place of degree 1. Let $\widehat{F}_Q$ be the completion of F with respect to the valuation v_Q. By Theorem 1.3.20 we have

$$\widehat{F}_Q \cong \mathbf{F}_p(\!(t)\!)$$

where $t \in F$ is a uniformizer of Q (so $v_Q(t) = 1$). Let $u \in \mathbf{F}_p(z)$ be a uniformizer of P. The completion $\mathbf{F}_p(\!(u)\!)$ of $F_p(z)$ at P sits inside the field $\mathbf{F}_p(\!(t)\!)$. In this way we get the commuting diagram:

$$\begin{array}{ccc} F & \hookrightarrow & \mathbf{F}_p(\!(t)\!) \\ | & & | \\ \mathbf{F}_p(z) & \hookrightarrow & \mathbf{F}_p(\!(u)\!) \end{array}$$

By Theorem 1.3.3 we have an isomorphism

$$\mathrm{Gal}(\mathbf{F}_p(\!(t)\!)/\mathbf{F}_p(\!(u)\!)) \cong \mathrm{Gal}_{v_Q}(F/\mathbf{F}_p(z)) \tag{4.1}$$

relating the Galois group of $\mathbf{F}_p(\!(t)\!)/\mathbf{F}_p(\!(u)\!)$ to a subgroup of $\mathrm{Gal}(F/\mathbf{F}_p(z))$. Let σ be some element of $\mathrm{Gal}(F/\mathbf{F}_p(z))$. Because P is totally ramified we have $\sigma(Q) = Q$, so by (1.10) we see that $v_Q \circ \sigma = v_Q$ holds and hence it follows from (4.1) that we have an isomorphism of Galois groups

$$\mathrm{Gal}(\mathbf{F}_p(\!(t)\!)/\mathbf{F}_p(\!(u)\!)) \cong \mathrm{Gal}(F/\mathbf{F}_p(z))\,. \tag{4.2}$$

Through this isomorphism any $\sigma \in \mathrm{Gal}(F/\mathbf{F}_p(z))$ lifts uniquely to a continuous automorphism of $\mathbf{F}_p(\!(t)\!)$ fixing $\mathbf{F}_p(\!(u)\!)$ (the topology on $\mathbf{F}_p(\!(t)\!)$ is induced by the valuation v_Q). We denote this lift also by σ. Note that $v_Q(\sigma(t)) = v_Q(t) = 1$, so $\sigma(t)$ takes the form

$$\sigma(t) = a_1 t + a_2 t^2 + a_3 t^3 + \dots$$

for some $a_i \in \mathbf{F}_p$. Since σ is a continuous map on $\mathbf{F}_p(\!(t)\!)$, σ acts on an element $f(t) \in \mathbf{F}_p(\!(t)\!)$ by replacing every occurrence of t in Laurent series expansion of $f(t)$ with $\sigma(t)$. For instance we have

$$\sigma^{\circ 2}(t) = a_1\sigma(t) + a_2\sigma(t)^2 + a_3\sigma(t)^3 + \dots\,.$$

By (4.2) the Galois group $\mathrm{Gal}(\mathbf{F}_p(\!(t)\!)/\mathbf{F}_p(\!(u)\!))$ has order p^n, so σ has order p^k for some $k \geq 0$. This gives $\sigma^{\circ p^k}(t) = t$ and comparing the coefficients of t on both sides shows $a_1^{p^k} = 1$ and hence $a_1 = 1$ since we work over a field of characteristic p. This shows that $\sigma(t)$ is an element of order p^k in the Nottingham group $\mathcal{N}(\mathbf{F}_p)$.
We have the system of equations $\wp(\alpha) = \beta$ available as well as equations for t and $\sigma(t)$. We can try to use these equations to find an algebraic equation for $\sigma(t)$ over $\mathbf{F}_p(t)$. If we have such an equation then by passing to $\mathbf{F}_p(\!(t)\!)$ the element $\sigma(t) \in \mathbf{F}_p(\!(t)\!)$ satisfies the same equation. In this setting we can apply the theorem of Christol from Chapter 3 to find a p-automaton generating $\sigma(t)$. We used the Mathematica package [17] to compute the p-automata, among other things it contains an algorithmic implementation of the theorem of Christol.

There are a couple of remarks we need to place concerning the above method for constructing algebraic equations.

Remark 4.1.1.
- Varying some of the parameters like the truncated Witt vector β, the place P, the uniformizer t and the Galois automorphism σ can gives a lot of different algebraic equations. In the examples we considered, there was always only one choice for the place P, so we cannot say something about varying the place.

- For a fixed Witt vector β and a place P, we can consider the order p^n elements in the Galois group since we are interested in those. Varying the uniformizer t gives in practice many different algebraic equations, but there can be also a large overlap (different uniformizer give the same algebraic equation).

- For a fixed $\beta \in W_n(\mathbf{F}_p(z))$ and a place P it turns out that for any choice of uniformizer t and an automorphism σ of order p^n the depth sequence of σ is the same. As the depth sequence is an invariant of finite order elements of $\mathcal{N}(\mathbf{F}_p)$ this is an easy way to get non-conjugated elements of $\mathcal{N}(\mathbf{F}_p)$. From Observation 5 from [14] and Theorem 6 in [11] one can deduce what the possible depth sequences are. In [10] Jean generalizes the work of Kanesaka and Sekiguchi [11], this includes giving a construction of certain Witt vectors which allows you to specify in advance the depth sequences of all elements which can be studied using the above method.

- The method has the disadvantage that it contains two black boxes: a variant of the Groebner basis and the algorithm deduced from the proof of Theorem 3.1.18. With a variant of the Groebner basis algorithm we mean an algorithm that is able to eliminate some variables. It has the disadvantage that we don't how long we need to wait for obtaining an output, of what this output consists of and how complicated it is. The algorithm of Christol also has the problem that one does not know when it will finish and also not how many vertices the output has. We were able to use the above method to find algebraic equations for order 9 elements in $\mathcal{N}(\mathbf{F}_3)$, however every computation of a corresponding 3-automaton took more memory then our computer had available.

- To make everything run as smoothly as possible it is important to factor the output of the Groebner basis over $\mathbf{F}_p[t, \sigma(t)]$ in order to find the minimal equation of $\sigma(t)$. As a consequence the degree of the algebraic relation for $\sigma(t)$ is as small as possible. Another reason why this is useful is because can output different automata for different algebraic equations even if one of the equations is just a multiple of the other.

4.2 New order 4 elements in $\mathcal{N}(\mathbf{F}_2)$

We apply the method from the previous section to construct five new explicit power series of order 4 of $\mathcal{N}(\mathbf{F}_2)$.

Let β be the truncated Witt vector $\beta = (z^{-1}, 0) \in W_2(\mathbf{F}_2(z))$ and $(z) = P$ a place of $\mathbf{F}_2(z)$ (note that $z^{-1} \notin \wp(\mathbf{F}_2(z))$, since $v_Q(\wp(\mathbf{F}_2(z))) \subseteq \mathbf{Z}\backslash\{-1, -3, \ldots\}$) and suppose that $\alpha = (x, y) \in W_2(\overline{\mathbf{F}_2(z)})$ is a solution to $\wp(\alpha) = \beta$. This gives us the system of equations

(see (1.6))

$$\begin{cases} x^2 - x &= z^{-1} \\ y^2 - y &= xz^{-1} \end{cases}$$

and $F/\mathbf{F}_2(z) = \mathbf{F}_2(z,x,y)/\mathbf{F}_2(z)$ is a cyclic Galois extension of degree 4. Using Equation (1.9) a generator σ of $\mathrm{Gal}(F/\mathbf{F}_2(z))$ is defined by

$$\sigma(x) = x + 1 \quad \text{and} \quad \sigma(y) = y + x\,,$$

the inverse τ of σ is define by

$$\tau(x) = x + 1 \quad \text{and} \quad \tau(y) = y + x + 1\,,$$

Consider the place $P = (z)$ of $\mathbf{F}_2(z)$, we will show that it totally ramifies in the extension $F/\mathbf{F}_2(z)$. We have $v_P(z^{-1}) = -1$ so by Theorem 1.3.19 the place P totally ramifies in the extension $\mathbf{F}_2(z,x)/\mathbf{F}_2(z)$. If P' denotes the unique place in $\mathbb{P}_{\mathbf{F}_2(z,x)}$ above P then we have $e(P'|P) = 2$ and $f(P'|P) = 1$, the same proposition also shows that $v_{P'}(x) = -1$. Since $v_{P'}(z) = e(P'|P)v_P(z) = 2$ we get $v_{P'}(xz^{-1}) = -3$ using Theorem 1.3.19 again shows that P' totally ramifies in the extension $F/\mathbf{F}_2(z,x)$. Write Q for the unique place in $\mathbb{P}_F$ above P' then $e(Q|P') = 2$ and $f(Q|P') = 1$, the same proposition also shows that $v_Q(y) = -3$. Because

$$e(Q|P) = e(Q|P')e(P'|P) = 4 \quad \text{and} \quad f(Q|P) = f(Q|P')f(P'|P) = 1 \tag{4.3}$$

the place P ramifies completely in $F/\mathbf{F}_2(z)$ and Q is the unique place above P. The Q-valuations of the elements z, x and y are $v_Q(z) = 4, v_Q(x) = -2$ and $v_Q(y) = -3$. This will enable us to compute the valuations of many elements of F.

For four specific choices of uniformizers t we will derive an algebraic equation for $\sigma(t)$ and $\tau(t)$. The results are show in Table 4.1. We illustrate this for a specific choice of uniformizer. Consider the uniformizer $t = \frac{x}{y}$ (note that $v_Q(t) = -2 - (-3) = 1$), we have the following system of equations

$$\begin{cases} x^2 - x &= z^{-1} \\ y^2 - y &= xz^{-1} \\ yt &= x \\ (y+x)\sigma(t) &= x + 1 \end{cases}.$$

We want to use this system to eliminate the variables x, y and z. We can do this by hand but in practice using a variant of the Groebner basis algorithm is much more efficient. Doing the calculations gives us the following minimal equation for $\sigma(t)$ over $\mathbf{F}_2(t)$:

$$(1+t)\sigma(t)^2 + (1+t^2)\sigma(t) + t = 0\,. \tag{4.4}$$

We have already seen this equation in Lemma 2.3.1. The Viète formulas show that the sum of the two solutions of (4.4) equals $1 + t$. We know that one of the solutions equals t modulo t^2, so this also determines it. Plugging in

$$\sigma(t) = t + a_2t^2 + a_3t^3 + \ldots$$

$x^2t = y$	
(1)	$t^2\sigma^2 + \sigma + t + t^2 = 0$
(2)	$(1 + t^2)\tau^2 + \tau + t = 0$
$yt = x$	
(3)	$(1 + t)\sigma^2 + (1 + t^2)\sigma + t = 0$
(4)	$t\tau^2 + (1 + t^2)\tau + t^2 + t = 0$
$t(x^2 + xy) = 1 + x^2 + y$	
(5)	$t^2\sigma^4 + (1 + t + t^2 + t^4)\sigma^2 + (t + t^2 + t^3)\sigma + t^3 = 0$
(6)	$t^2\tau^4 + (1 + t)\tau^3 + (t + t^2 + t^4)\tau^2 + (t + t^2)\tau + t^2 = 0$
$t(x^3 + y) = xy$	
(7)	$t^4\sigma^4 + (1 + t^2)\sigma^3 + (t + t^3)\sigma^2 + t^3 = 0$
(8)	Same as for (7).

Table 4.1: Table of the minimal polynomials of σ and τ over $\mathbf{F}_2(t)$ for 4 different uniformizers t.

and solving some equations gives us the first few coefficients of $\sigma(t)$ which we need for the algorithm of Christol, implemented by Rowland in [17], to work.

We have drawn the 2-automaton corresponding to (4.4) in Table 4.2. It is the automaton labeled (3). It has the useful property that the only directed cycles are the loops. For every vertex v with label 1 this enables us to write down all the sequences in S_2 ending in a 1 (so for example $(0, 0, 1)$ ends in a 1 but $(1, 0, 0)$ doesn't) which define the vertex v. In our case these are

$$(1), (0, 1), (1, 0,)0^k(1), (1, 0)0^k(1, 0)(\ell)_2, (0, 1, 0)(\ell)_2, (1, 1, 1)(m)_2 \quad \text{and} \quad (0, 0)0^k(1, 1)(m)_2$$

where $k, m \geq 0$ and $\ell > 0$ (we regard the expression $(0)_2$ as non-existing, so $(1, 1, 1)(0)_2$ just means $(1, 1, 1)$). These elements correspond respectively to the following parts of the power series expansion of $\sigma(t)$:

$$t, t^2, t^{1+4\cdot 2^k}, t^{1+4\cdot 2^k(1+4\ell)}, t^{2+8\ell}, t^{7+8n} \text{ and } t^{4\cdot 2^k(3+4n)}.$$

Adding all these monomials gives the following power series expansion of $\sigma(t)$ (which is already somewhat simplified):

$$\sigma(t) = t + t^2 + \sum_{k\geq 0} \left(t^{2+8k} + t^{7+8k}\right) + \sum_{k,\ell\geq 0} \left(t^{4\cdot 2^k(4\ell+3)} + t^{1+4\cdot 2^k(4\ell+1)}\right).$$

Remark 4.2.1. We used the Mathematica package [17] written by Rowland for computing the 2-automaton for each of the 8 algebraic equations in Table 4.1. The results are shown in Table 4.2 and Table 4.3. For this algorithm to work we need the first few coefficients of the power series expansion of $\sigma(t)$ (if we haven't provided enough the algorithm wil say to which order the coefficients are need). The method we use to find these coefficients needs some computation, but in practice it is always fast.

Let $m \geq 2$ be some integer. We know that the power series we are looking for has the form

$$f(t) = t + a_2 t^2 + a_3 t^3 + \ldots + a_m t^m \mod t^{m+1}\,. \tag{4.5}$$

So we replace $\sigma(t)$ in the algebraic equation by (4.5) and then start by successively solving for the coefficients a_i. It happens that there are sometimes multiple possibilities for some a_i and so we can get in the end a few different candidates (often there is just one). In the situation of multiple candidates we can compute $f^{\circ 4}$. If this yields something different than t then we know f is not the one we are looking for. When we know the depth sequence corresponding to σ, there is another thing we can do. Namely, from this depth sequence we can compute the the depths of σ and $\sigma^{\circ 2}$ which we can compare with the depths of f and $f^{\circ 2}$. If they do not coincide then f is not the right one.

As an example consider the equations labeled (7) and (8) in Table 4.1: they are the same. In this case we have an algebraic equation of which two zeroes are the different elements σ and τ from $\mathcal{N}(\mathbf{F}_2)$. It turns out that $\sigma^{\circ 2} = \tau^{\circ 2}$ is another zero of the same equation (by looking at the coefficient of σ^3 the fourth zero is not an element of $\mathbf{F}_2[\![t]\!]$).

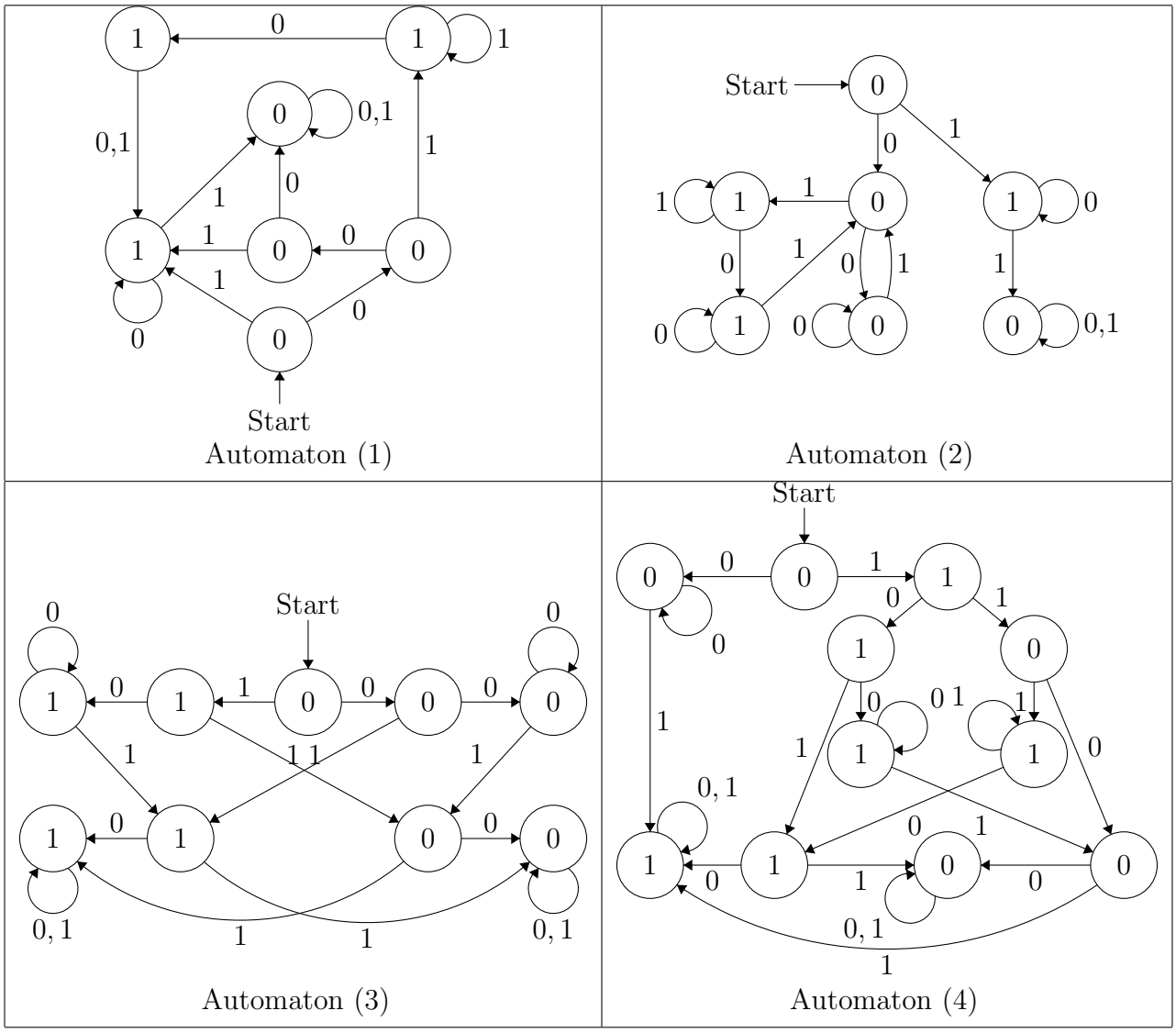


Table 4.2: 2-Automata of order 4 corresponding to the algebraic equations in Table 4.1.

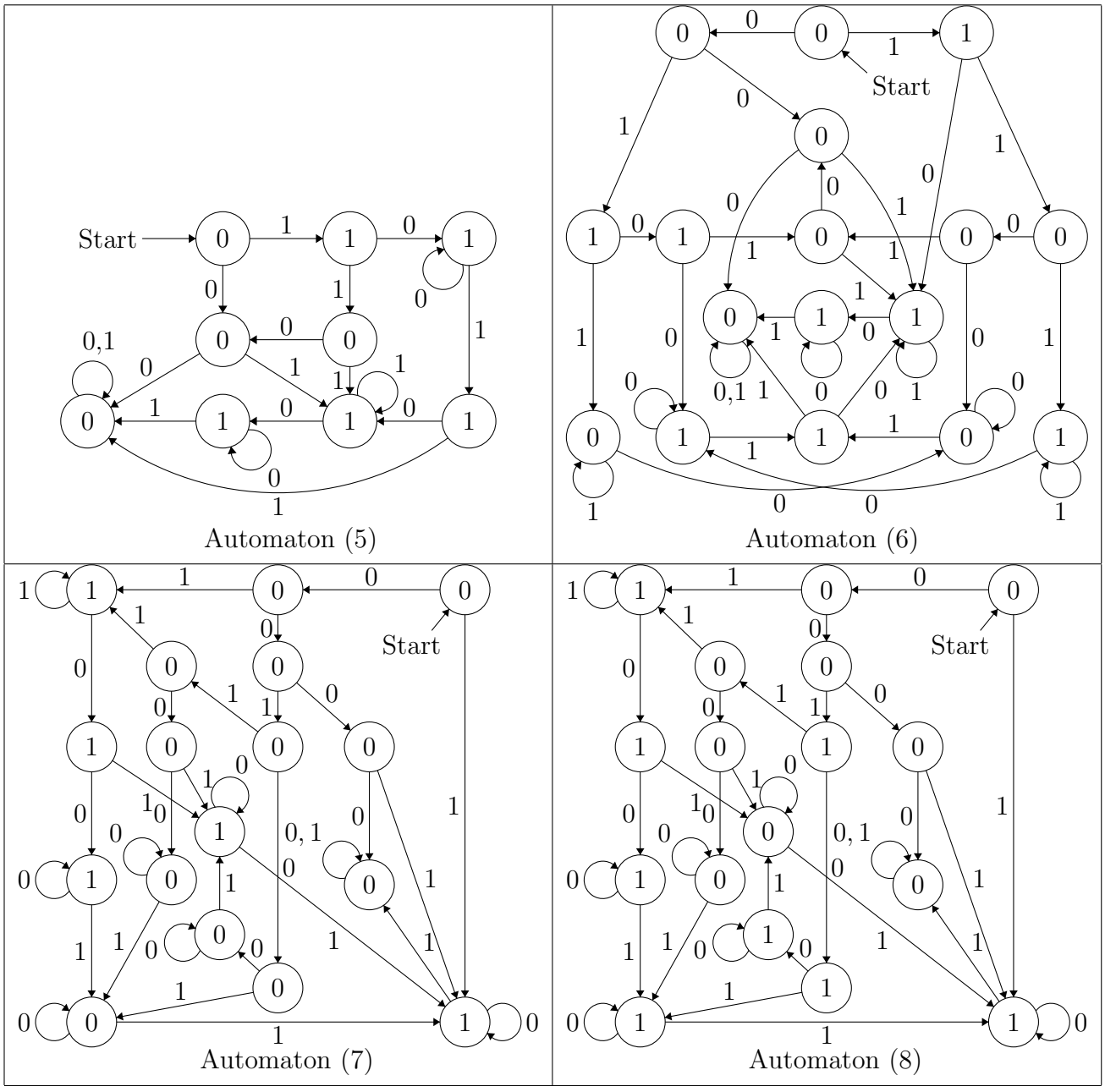


Table 4.3: 2-Automata of order 4 corresponding to the algebraic equations in Table 4.1.

The 2-automata labeled (1), (2) and (3) in Table 4.2 correspond to known order 4 series. Specifically (1) and (2) corresponds respectively to the power series τ and σ in Lemma 2.3.2 and (3) corresponds to Lemma 2.3.1. Therefore we focus our attention on

the 2-automata in Table 4.2 and Table 4.3 labeled (4), (5), (6), (7) and (8). Each of these directed graphs has also the same properties that the automaton labeled (3) has: the only directed cycles are loops. We can therefore use the same method to find the explicit power series of the remaining five 2-automata. The calculations are long and tedious but doable by hand. Doing so gives us the next theorem.

Theorem 4.2.2. *The power series generated by the 2-automata numbered (4), (5), (6), (7) and (8) in Table 4.2 and Table 4.3 are new examples of order 4 elements in $\mathcal{N}(\mathbf{F}_2)$ with depth sequence $(1,3)$. Their explicit power series are given in the table below.*

Label	Power series of order 4
(4)	$t+\sum_{k\geq 0}\left(t^{5+8k}+t^{11+16k}\right)+\sum_{k,\ell\geq 0}\left(t^{2\cdot 2^k(2\ell+1)}+t^{1+8\cdot 2^k(4\ell+3)}+t^{-1+8\cdot 2^k+32\cdot 2^k\ell}\right)$
(5)	$t+\sum_{k\geq 0}\left(t^{4\cdot 2^k-2}+t^{4\cdot 2^k+1}+t^{16\cdot 2^k-5}+t^{8\cdot 2^k-1}\right)+\sum_{k,\ell\geq 0}t^{1-12\cdot 2^k+32\cdot 2^{k+\ell}}$
(6)	$t^2+\sum_{k\geq 0}\left(t^{8\cdot 2^k-1}+t^{8\cdot 2^k-4}+t^{64\cdot 2^k-24}+t^{64\cdot 2^k-21}+t^{16\cdot 2^k-6}+t^{32\cdot 2^k-5}+t^{4\cdot 2^k-3}\right)$ $+\sum_{k,\ell\geq 0}\left(t^{2-48\cdot 2^k+64\cdot 2^{k+\ell}}+t^{3-16\cdot 2^k+32\cdot 2^{k+\ell}}\right)$ $+(1+t)\sum_{k,\ell,m\geq 0}t^{-2+8\cdot 2^k-48\cdot 2^{k+\ell}+64\cdot 2^{k+\ell+m}}$
(7)	$t+t^8+t^{44}+\sum_{k\geq 0}\left(t^{4\cdot 2^k-2}+t^{32\cdot 2^k-4}+t^{12\cdot 2^k-2}+t^{96\cdot 2^k-4}+t^{32\cdot 2^k+4}\right.$ $\left.+t^{32\cdot 2^k+20}+t^{64\cdot 2^k+44}\right)$ $+\sum_{k,\ell\geq 0}\left(t^{12+64\cdot 2^k+128\cdot 2^{k+\ell}}+t^{-2+12\cdot 2^k+16\cdot 2^{k+\ell}}+t^{-4+96\cdot 2^k+128\cdot 2^{k+\ell}}\right)$ $+\sum_{k,\ell,m\geq 0}\left(t^{-2+4\cdot 2^k+16\cdot 2^{k+\ell}+32\cdot 2^{k+\ell+m}}+t^{-4+32\cdot 2^k+128\cdot 2^{k+\ell}+256\cdot 2^{k+\ell+m}}\right)$
(8)	$t+t^4+t^8+t^{20}+\sum_{k\geq 0}\left(t^{4\cdot 2^k-2}+t^{32\cdot 2^k-4}+t^{64\cdot 2^k+44}+t^{64\cdot 2^k+12}+t^{32\cdot 2^k+20}\right)$ $+\sum_{k,\ell\geq 0}\left(t^{-2+24\cdot 2^k+32\cdot 2^{k+\ell}}+t^{-4+96\cdot 2^k+128\cdot 2^{k+\ell}}+t^{4+32\cdot 2^k+64\cdot 2^{k+\ell}}+t^{-2+4\cdot 2^k+16\cdot 2^{k+\ell}}\right.$ $\left.+t^{-4+32\cdot 2^k+128\cdot 2^{k+\ell}}+t^{12+64\cdot 2^k+128\cdot 2^{k+\ell}}\right)$ $+\sum_{k,\ell,m\geq 0}\left(t^{-4+32\cdot 2^k+128\cdot 2^{k+\ell}+256\cdot 2^{k+\ell+m}}+t^{-2+4\cdot 2^k+16\cdot 2^{k+\ell}+32\cdot 2^{k+\ell+m}}\right)$

Note that since the automaton labeled (4) satisfies a degree 2 equation we can also solve it using the method proposed in Section 2.3. This then gives the more compact formula for $\tau(t)$:

$$\tau(t)=\sum_{n\geq 0}\frac{t^{2^{n+1}-1}}{(1+t)^{3\cdot 2^n-2}}\,.$$

Remark 4.2.3. In the case of order p elements in $\mathcal{N}(\mathbf{F}_p)$ we know by the theorem of Klopsch that knowing the initial coefficient and the depth of an order p element is enough to determine it conjugacy class. In the order p^2 this is not the case any more. There

is however something to salvage. Lubin remarks in Observation 6 in [14] that there are up to conjugacy only finitely many elements of a given depth sequence. We saw already that in the case $p = 2$ there are only two conjugacy class of order 4 elements of $\mathcal{N}(\mathbf{F}_2)$ having depth sequence $(1, 3)$. This shows that there are many pairs of power series in Theorem 4.2.2 that are conjugated.

Example 4.2.4. Consider the same degree 4 extension as before. The uniformizer t defined by $(y + 1)t = x^2 + y$ yields the following algebraic equation for $\tau = \sigma^{\circ 3}$:

$$(1 + t)^3\tau^3 + (t + t^3)\tau^2 + (1 + t + t^3) + \tau + t^3 + t = 0$$

Which corresponds to a 2-automaton on 5 vertices, which is shown on the first page of this thesis.

Remark 4.2.5. We will construct a 2-automaton generating a power series of order 4 with depth sequence $(1, 3)$. Consider the element $(z^{-1}, z^{-3}) \in W_2(\mathbf{F}_2(z))$, clearly $z^{-1} \notin \wp(\mathbf{F}_2(z))$ so we get a Galois extension $F/\mathbf{F}_2(z) = \mathbf{F}_2(z, x, y)/\mathbf{F}_2(z)$ of cyclic degree 4. Here x and y satisfy

$$\begin{cases} x^2 - x &= z^{-1} \\ y^2 - y &= xz^{-1} + z^{-3} \end{cases}$$

and a generator of the Galois group is defined by

$$\sigma(x) = x + 1 \text{ and } \sigma(y) = y + x + 1\,.$$

Consider the place $(z) = P$ of $\mathbf{F}_2(z)$. In the same way as before we find that P totally ramifies in the extension $\mathbf{F}_2(z, x)/\mathbf{F}_2(z)$, let P' be the unique place above P then $v_{P'}(x) = -1$ and $v_{P'}(z) = 2$. Consider the element $w = y + x^3 + x^2$, it satisfies

$$w^2 - w = x^5 + x^3$$

so by Theorem 1.3.19 the place P' totally ramifies in the extension $F/\mathbf{F}_2(z, x)$, if Q denotes the unique place above it then we know that $v_Q(w) = -5$, $v_Q(x) = -2$ and that Q totally ramifies in $F/\mathbf{F}_2(z)$. The element σ is a Galois automorphism of $\mathbf{F}_2(z, x, y)$ so it is also a Galois automorphism of $\mathbf{F}_2(z, x, w)$, it is defined by

$$\sigma(x) = x + 1 \text{ and } \sigma(w) = w + x^2 + 1\,.$$

Consider the uniformizer $t = \frac{x^2}{w}$ of Q, eliminating z, x and w from the system

$$\begin{cases} x^2 - x &= z^{-1} \\ w^2 - w &= x^5 + x^3 \\ tw &= x^2 \\ \sigma(t)(w + x^2 + 1) &= x^2 + 1 \end{cases}$$

gives us the following minimal polynomial of $\sigma(t)$ over $\mathbf{F}_2(t)$:

$$t^2\sigma(t)^3 + (1 + t)^3\sigma(t) + t + t^3 = 0\,.$$

The corresponding 2-automaton is shown in Figure 4.1.

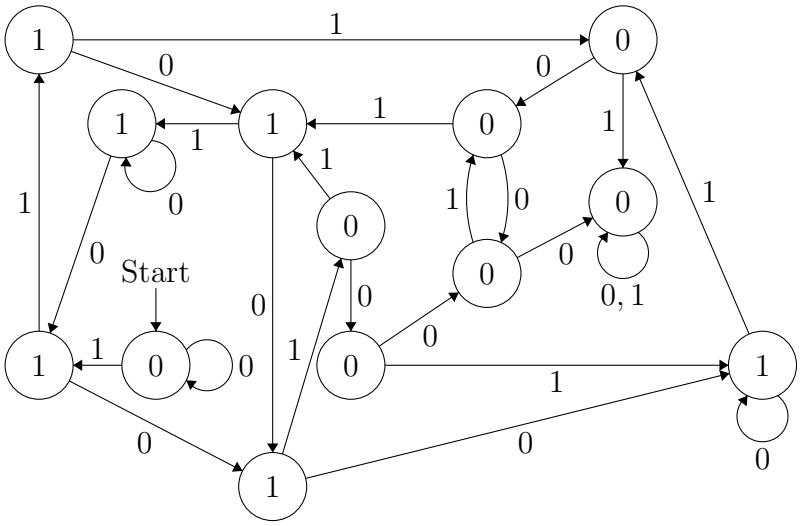


Figure 4.1: A 2-automaton of an order 4 power series in $\mathcal{N}(\mathbf{F}_2)$ with depth sequence $(1, 3)$.

This gives us the following theorem.

Theorem 4.2.6. *The 2-automaton in Figure 4.1 describes an element of order 4 and depth sequence* $(1, 5)$ *in* $\mathcal{N}(\mathbf{F}_2)$*. In particular it is not conjugated to any of the 8 explicit power series of order 4 of depth sequence* $(1, 3)$*.*

Remark 4.2.7. Although the 2-automaton in Figure 4.1 is quite small we did not succeed in writing down an explicit power series for it. What makes it difficult is that the graph has multiple directed cycles. So although we cannot write down an explicit power series we can write down the corresponding 2-automaton. We therefore think that it is worthwhile to study the corresponding p-automaton of an order p^n element in $\mathcal{N}(\mathbf{F}_p)$ instead of looking for its power series expansion.

Remark 4.2.8. Using the method in the beginning we can also construct an cyclic order 8 extension of $\mathbf{F}_2(z)$. An example of such an extension is given by $\mathbf{F}_2(z, x, y, w)/\mathbf{F}_2(z)$ where

$$\left\{ \begin{array}{rcl} x^2 - x & = & z^{-1} \\ y^2 - y & = & xz^{-1} \\ w^2 - w & = & x^3(x+1)y \end{array} \right. .$$

a generator of the Galois group is defined by

$$\sigma(x) = x + 1, \sigma(y) = y + x \text{ and } \sigma(w) = w + y(x + 1)\,.$$

Write Q for the place above $P = (z)$ which totally ramifies in this extension, then $v_Q(x) = -4$, $v_Q(y) = -6$ and $v_Q(w) = -11$. Define the uniformizer t by $(w + y)t = x^3 + y$. We then get the following algebraic equation for $\sigma = \sigma(t)$ over $\mathbf{F}_2(t)$:

$$t^6\sigma^6 + (t^2 + t^6)\sigma^4 + (1 + t^2 + t^3 + t^4 + t^5 + t^6)\sigma^2 + (1 + t)^3\sigma + t + t^2 + t^5 + t^6 = 0\,.$$

Applying the algorithm written by Rowland gives us within a reasonable amount of time a 2-automaton for σ consisting of 320 vertices.

Bibliography

[1] Jean-Paul Allouche and Jeffrey Shallit, *Automatic sequences*, Cambridge University Press, Cambridge, 2003, Theory, applications, generalizations.

[2] Laurent Berger and Sandra Rozensztajn, *Composition of power series*, PROMYS research project, `http://perso.ens-lyon.fr/laurent.berger/autrestextes/WildPromys.pdf`, 2016.

[3] Frauke M. Bleher, Ted Chinburg, Bjorn Poonen, and Peter Symonds, *Automorphisms of Harbater-Katz-Gabber curves*, Mathematische Annalen (2016), 126.

[4] Jakub Byszewski and Gunther Cornelissen, private communication, 2017.

[5] Rachel Camina, *Subgroups of the Nottingham group*, J. Algebra 196 (1997), no. 1, 101113.

[6] Ted Chinburg and Peter Symonds, *An element of order 4 in the Nottingham group at the prime 2* arXiv:1009.5135, 2010.

[7] Gilles Christol, *Ensembles presque periodiques k-reconnaissables*, Theoret. Comput. Sci. 9 (1979), no. 1, 141145.

[8] Fernando Q. Gouvêa, *p-adic Numbers An Introduction*, Springer-Verlag, Berlin Heidelberg New York, Corrected 3rd printing 2003.

[9] Sandrine Jean, *Classification à conjugaison près des séries de p-torsion.*, Université de Limoges, PhD-thesis, 2008.

[10] Sandrine Jean, *Conjugacy classes of series in positive characteristic and Witt vectors*, J. Théor. Nombres Bordeaux 21 (2009), no. 2, 263-284.

[11] K.Kanesaka and K.Sekiguchi, *Representation of Witt Vectors by formal power series and its applications.* Tokyo J.Math Vol 2 No 2. (1979), 349-370.

[12] Benjamin Klopsch, *Automorphisms of the Nottingham group*, J. Algebra 223 (2000), no. 1, 3756.

[13] Falko Lorenz, *Algebra, Volume II: Fields with Structure, Algebras and Advanced Topics*, Springer 2008.

[14] Jonathan Lubin, *Torsion in the Nottingham group*, Bull. Lond. Math. Soc. 43 (2011), no. 3, 547560.

[15] Jürgen Neukirch. *Algebraic Number Theory*, Springer-Verlag Berlin Heidelberg, 1999.

[16] Joseph Rabinoff, *The Theory of Witt Vectors*, arXiv:1409.7445, 2014.

[17] Eric Rowland, *IntegerSequences*, Mathematica package, version 1.35, `https://people.hofstra.edu/Eric_Rowland/packages.html`, 2016.

[18] Henning Stichtenoth *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin Heidelberg, Second edition, 2009.

[19] Ernst Witt, *Zyklische körper und algebren der characteristik p vom grad p^n. struktur diskret bewerteter perfekter körper mit vollkommenem restklassen körper der charakteristik p*, J. Reine Angew. Math. (1936), no. 176, 126140.