The Jacobian Conjecture over finite fields

Author : Kelder, M (0314110)

Date : April 8, 2010

Education Master Mathematics at Radboud University Nijmegen

Supervisor : Maubach, S.

Second supervisor : Essen, A. van den

Contents

Chapter 1

Summary

The main topic of this thesis is the Jacobian Conjecture and the polynomial automorphism group. The focus point lies in the case where we are working over a finite field.

In chapter 2 the neccessary introduction of the Jacobian Conjecture is made. In chapter 3 we consider the finite field case, and prove the J.C. for certain cases. In particular, we want to restrict to dimension 2, and make certain assumptions on the degrees of the components of the automorphism. Besides the conditions as used by Adjamagbo, some additional conditionals were added to create stronger results.

In chapter 4 we futher explore the idea of replacing the "Adjamagbo requirement": $p \nmid |\mathbb{F}_p(X) : \mathbb{F}_p(F)|$ by additional equations on the coefficients. We show that the most obvious choise for this is not the right one.

In chapter 5 we explore the following: if $F = I + H_d + \widetilde{H_{d+1}}$ where H_d is homogenous of degree d and $\widetilde{H_{d+1}}$ has only terms of degree at least $d+1$, what the H_d can be. In particular, the set of such H_d form a vector space. We compute this vector space in dimension 2 for certain F.

Chapter 2

Introduction

2.1 Problem description

2.1.1 Polynomial automorphisms

Let k be a field. Let $n \in \mathbb{N}^*$. A *polynomial map* is a map $F = (F_1, \ldots, F_n) : k^n \to k^n$ where the $F_i \in k[x_1, \ldots x_n]$.

A polynomial map F is called *invertible* if there exists a polynomial map G such that $G \circ F = I$, where I is the identity. Now we can define the Jacobian matrix of F: $JF := (a_{ij})$, where $a_{ij} := \frac{\mathrm{d}}{\mathrm{d}x_j} F_i$. I denote $|JF| := \det(JF)$.

Jacobian conjecture 1. *Suppose that if k is a field with characteristic 0, then F has a polynomial inverse if and only if $|JF| \in k^*$.*

The following is a formulation of the Jacobian Conjecture for characteristic p (in this thesis we restrict to finite fields). This formulation is due to done by Adjamagbo (see [2], proposition 10.3.17).

Notation 2. *By $k(X)$ respectively $k(F)$ we denote the quotient field of $k[X]$ respectively $k[F]$.*

Conjecture 3. *Let $k = \mathbb{F}_p$. If $|JF| \in k^*$ and $p \nmid [k(X) : k(F)]$, then F is invertible over k. This conjecture we denote by $JC(\mathbb{F}_p, n, p)$.*

Theorem 4. *If $JC(\mathbb{F}_p, n, p)$ holds for alle $n \geq 1$ and all primes p, then the Jacobian conjecture holds. (see [2], theorem 10.3.13)*

2.1.2 Tameness

Definition 5. *A polynomial automorphism F is called* elementary *if there exists an i and an $a = a(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ such that*

$$F = (x_1, x_2, \ldots, x_{i-1}, x_i + a(x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n), x_{i+1}, \ldots, x_n)$$

The subgroup of all polynomial automorphisms generated by the elementary automorphisms is called $E_n(k)$.

Definition 6. *A polynomial automorphism F is called* De Jonquières *if for each $1 \leq i \leq n$ there exists $f_i \in k\,[x_{i+1}, \ldots, x_n]$ such that*

$$F = (x_1 + f_1(x_2, \ldots, x_n), x_2 + f_2(x_3, \ldots x_n), \ldots, x_{n-1} + f_{n-1}(x_n), x_n)$$

The subgroup of all polynomial automorphisms generated by the De Jonquières automorphisms is called $J_n\,(k)$.

Definition 7. *A polynomial automorphism is called* affine *if it doesn't contain powers strictly bigger then one. The group of Affine automorphisms $\mathrm{Aff}_n\,(k)$ is defined as the group of all polynomial automorphisms F such that $\deg F_i = 1$ for all $1 \leq i \leq n$.*

Definition 8. *A polynomial automorphisms F is called* tame *if it is a finite composition of elementary maps and elements of the affine subgroup $\mathrm{Aff}_n\,(k)$. The subgroup of all the polynomial automorphisms generated by tame automorphism is called $\mathrm{TA}_n\,(k)$.*

Definition 9. *The group of all polynomial automorphisms is called $\mathrm{GA}_n\,(k)$.*

The Jung - van der Kulk theorem states that if $n = 2$, then every polynomial automorphism is tame (see [2], theorem 5.1.11). For $n > 2$ and $\mathrm{char}(k) = 0$ there are counterexamples (Nagata) (see [2], proposition 5.1.9).

Theorem 10. *(Jung, van der Kulk) If k is a field, then $\mathrm{Aut}_k\, k[X, Y] = \mathrm{TA}_2\,(k)$. Also, $\mathrm{Aut}_k\, k[X, Y]$ is the amalgated free product of $\mathrm{Aff}_2\,(k)$ and $J_2\,(k)$ over their intersection.*

Chapter 3

JC in finite cases

3.1 Generalisation, counterexamples and approach

Lets consider the Jacobian Conjecture if we just replace $\mathbb{C}$ by $\mathbb{F}_p$. I will call this the "wrong Jacobian Conjecture" for finite fields.

Now lets look at the following example:

$$\left\langle \begin{array}{c} x - x^p \\ y \end{array} \right\rangle$$

This obviously isn't an automorphism over $\mathbb{F}_p$, since $x^p = x$ on $\mathbb{F}_p$, so this mapping behaves exactly as $\left\langle \begin{array}{c} 0 \\ y \end{array} \right\rangle$. But what is its Jacobi determinant? That is

$$\left| \begin{array}{cc} 1 - p \cdot x^{p-1} & 0 \\ 0 & 1 \end{array} \right| = \left| \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right| = 1$$

So according to the "wrong Jacobian Conjecture" this should be an automorphism. So for every prime p there exists a counterexample.

So only satisfying the Jacobian requirement $|JF| \in k^*$ is not enough to ensure that F is an automorphism. So an addition condition is neccessary. In the literature, usually the following additional condition is used due to Adjamagbo: a mapping F only needs to be an automorphism if $p \nmid [k(F) : k(X)]$. This will rule out all the examples like above. Also, for each F, this condition only rules out finitely many (because the field extention also is finite). So if the new conjecture is true for all primes p, then the Jacobian Conjecture over $\mathbb{C}$ holds (see [2], theorem 10.3.13).

Unfortualy, this additional condition makes it even harder to say anything on this conjecture, because the field extention is not easily rewritten in other terms. But it is possible to only consider small p (for example, $p = 2$) and small n (where n is the dimention), in particular $n = 2$.

An other way around it is to find an alternative to the Adjamagbo requirement. As long as those conditions rule out only a finite number of primes p for every mapping F, it still implies the Jacobian Conjecture over $\mathbb{C}$. Also, an alternative condition might be more accessible then the "Adjamagbo requirement".

In characteristic zero, the Jacobian condition $|JF| \in k^*$ is a collection of equations on the coefficients of F. In characteristic p this collection is not enough, as we have seen above. This is because certain equations disappear as they are a multiple of p. It seems a good idea, instead of adding the field extention condition, to add additional equations on the coefficients. In section 4 I briefly consider this approach.

At the end I also look to the beginning part of the polynomials in F. So we take F and we throw away any term with a degree bigger then a certain treshold. This obviously would loose too much information to make definitive answer if F is an automorphism, but there is a chance we can say very early if an F will not be a polynomial automorphism. Also I hope to get some information about how the decomposition of F looks like (I will only look to tame automorphisms). So we will have two ways of saying something about F: it isn't a tame automorphism because the lower degrees can't become a tame automorphism and if we can find an actual decomposition (which proves that it is a tame automorphism).

3.2 Degree of field extention

3.2.1 Problem

I will take a non-standard approach to the Jacobian Conjecture. To begin with, I mainly consider finite fields. If I can prove a conjecture simular to the Jacobian Conjecture, but for finite fields, then I can also prove the jacobian conjecture.

So most often I will use a finite field. Near the end of this chapter I will use a even more specific case, namely $\mathbb{F}_2$. Proving the conjecture for $\mathbb{F}_2$ is not enough to prove the Jacobian conjecture over $\mathbb{C}$, but a proof of the theorem over $\mathbb{F}_2$ can lead to an idea for a proof in all finite field cases.

Conjecture 11. *Given $F \in \mathbb{F}_p^n$. If $p \nmid [k(x,y) : k(F_1, F_2)]$ and $|JF| \in k^*$. Then F is injective.*

In this chapter, I will affirmatively answer this conjecture for some specific cases.

3.2.2 Degree extension requirement

We have two if-statements in the problem. I will examine the requirement on the degree extension. First, remark the following:

Remark 12. *If F is a polynomial automorphism, then $[k(x,y) : k(F)] = 1$.*

Proof. Because F is a polynomial automorphism, $x \in k(F)$ and also $y \in k(F)$. □

Remark 13. *If F be a polynomial mapping and G a polynomial automorphism. Then*

$$[k(x,y) : k(F \circ G)] = [k(x,y) : k(F)] = [k(x,y) : k(G \circ F)]$$

Remark 14. *I remark that $[k(x) : k(f)] = \deg_x(f)$ if $f \in k[x]$ and $\deg_x f \geq 1$ (note: k can be any field here) [1]*

3.2.3 Odd degree

We consider a very special case, where there is a term of odd degree in x or y. We will use the following terminology (which isn't completely standard).

Definition 15. *A term of odd degree is a term not of the form $x^{2\cdot i} \cdot y^{2\cdot j}$.*

Now I will define two notations. I will use these notations a lot.

Notation 16. *Let $F \in \mathbb{F}_2[x,y]^2$. Then F can be written as*

$$\left\langle \begin{array}{c} f_1(x^2,y^2) + x \cdot f_2(x^2,y^2) + y \cdot f_3(x^2,y^2) + x \cdot y \cdot f_4(x^2,y^2) \\ g_1(x^2,y^2) + x \cdot g_2(x^2,y^2) + y \cdot g_3(x^2,y^2) + x \cdot y \cdot g_4(x^2,y^2) \end{array} \right\rangle$$

Lemma 17. *If F is written as in notation 16, then*

$$|JF| = a(x^2,y^2) + x \cdot b(x^2,y^2) + y \cdot c(x^2,y^2) + x \cdot y \cdot d(x^2,y^2)$$

Where:

$$\begin{aligned}
a(x^2,y^2) &= \begin{vmatrix} f_2(x^2,y^2) & f_3(x^2,y^2) \\ g_2(x^2,y^2) & g_3(x^2,y^2) \end{vmatrix} \\
b(x^2,y^2) &= \begin{vmatrix} f_2(x^2,y^2) & f_4(x^2,y^2) \\ g_2(x^2,y^2) & g_4(x^2,y^2) \end{vmatrix} \\
c(x^2,y^2) &= \begin{vmatrix} f_4(x^2,y^2) & f_3(x^2,y^2) \\ g_4(x^2,y^2) & g_3(x^2,y^2) \end{vmatrix} \\
d(x^2,y^2) &= \begin{vmatrix} f_4(x^2,y^2) & f_4(x^2,y^2) \\ g_4(x^2,y^2) & g_4(x^2,y^2) \end{vmatrix} = 0
\end{aligned}$$

Proof.

$$\begin{aligned}
|JF| &= \left| J \left\langle \begin{array}{c} f_1(x^2,y^2) + x \cdot f_2(x^2,y^2) + y \cdot f_3(x^2,y^2) + x \cdot y \cdot f_4(x^2,y^2) \\ g_1(x^2,y^2) + x \cdot g_2(x^2,y^2) + y \cdot g_3(x^2,y^2) + x \cdot y \cdot g_4(x^2,y^2) \end{array} \right\rangle \right| \\
&= \begin{vmatrix} f_2(x^2,y^2) + y \cdot f_4(x^2,y^2) & f_3(x^2,y^2) + x \cdot f_4(x^2,y^2) \\ g_2(x^2,y^2) + y \cdot g_4(x^2,y^2) & g_3(x^2,y^2) + x \cdot g_4(x^2,y^2) \end{vmatrix} \\
&= \begin{vmatrix} f_2(x^2,y^2) & f_3(x^2,y^2) \\ g_2(x^2,y^2) & g_3(x^2,y^2) \end{vmatrix} + x \cdot \begin{vmatrix} f_2(x^2,y^2) & f_4(x^2,y^2) \\ g_2(x^2,y^2) & g_4(x^2,y^2) \end{vmatrix} + \\
&\quad y \cdot \begin{vmatrix} f_4(x^2,y^2) & f_3(x^2,y^2) \\ g_4(x^2,y^2) & g_3(x^2,y^2) \end{vmatrix} + x \cdot y \cdot \begin{vmatrix} f_4(x^2,y^2) & f_4(x^2,y^2) \\ g_4(x^2,y^2) & g_4(x^2,y^2) \end{vmatrix}
\end{aligned}$$

□

The lemma below is used to cause a contradiction in a later lemma. In notation 16 I introduced some new polynomials ($f_1, f_2, f_3, f_4, g_1, g_2, g_3, g_4$). The following lemmas will tell something about properties of these polynomials.

Lemma 18. *If F is written as in 17 and $|JF| = 1$, then $\left\langle \begin{array}{c} f_4(x^2,y^2) \\ g_4(x^2,y^2) \end{array} \right\rangle = \left\langle \begin{array}{c} 0 \\ 0 \end{array} \right\rangle$*

Proof. Assume that the conclusion isn't true, so $\left\langle \begin{array}{c} f_4(x^2,y^2) \\ g_4(x^2,y^2) \end{array} \right\rangle \neq \left\langle \begin{array}{c} 0 \\ 0 \end{array} \right\rangle$

Because $|JF| = 1$ (using notation 16 and 17) it must follow that $a(x^2,y^2) = 1$ and

$$b(x^2,y^2) = c(x^2,y^2) = d(x^2,y^2) = 0$$

Because $b(x^2,y^2)$ and $c(x^2,y^2)$ are determinants of matrices, the columns of those matrices must depend on each other. I first look at the columns of $c(x^2,y^2)$. Because

$$\left\langle \begin{array}{c} f_4(x^2,y^2) \\ g_4(x^2,y^2) \end{array} \right\rangle \neq \left\langle \begin{array}{c} 0 \\ 0 \end{array} \right\rangle$$

it follows that

$$\left\langle \begin{array}{c} f_3(x^2,y^2) \\ g_3(x^2,y^2) \end{array} \right\rangle = \alpha \cdot \left\langle \begin{array}{c} f_4(x^2,y^2) \\ g_4(x^2,y^2) \end{array} \right\rangle = \left\langle \begin{array}{c} \alpha \cdot f_4(x^2,y^2) \\ \alpha \cdot g_4(x^2,y^2) \end{array} \right\rangle (\alpha \in k)$$

That also works for looking to the columns of $b(x^2,y^2)$: because again

$$\left\langle \begin{array}{c} f_4(x^2,y^2) \\ g_4(x^2,y^2) \end{array} \right\rangle \neq \left\langle \begin{array}{c} 0 \\ 0 \end{array} \right\rangle$$

it follows that

$$\left\langle \begin{array}{c} f_2(x^2,y^2) \\ g_2(x^2,y^2) \end{array} \right\rangle = \beta \cdot \left\langle \begin{array}{c} f_4(x^2,y^2) \\ g_4(x^2,y^2) \end{array} \right\rangle = \left\langle \begin{array}{c} \beta \cdot f_4(x^2,y^2) \\ \beta \cdot g_4(x^2,y^2) \end{array} \right\rangle$$

I use those equalities to simplify the assumption $|JF| = 1$:

$$\begin{aligned} |JF| = 1 \quad &\Leftrightarrow \quad \left| \begin{array}{cc} f_2(x^2,y^2) + y \cdot f_4(x^2,y^2) & f_3(x^2,y^2) + x \cdot f_4(x^2,y^2) \\ g_2(x^2,y^2) + y \cdot g_4(x^2,y^2) & g_3(x^2,y^2) + x \cdot g_4(x^2,y^2) \end{array} \right| = 1 \\ &\Leftrightarrow \quad \left| \begin{array}{cc} (\beta + y) \cdot f_4(x^2,y^2) & (\alpha + x) \cdot f_4(x^2,y^2) \\ (\beta + y) \cdot g_4(x^2,y^2) & (\alpha + x) \cdot g_4(x^2,y^2) \end{array} \right| = 1 \\ &\Leftrightarrow \quad \left| \begin{array}{cc} \beta + y & \alpha + x \\ \beta + y & \alpha + x \end{array} \right| \cdot f_4(x^2,y^2) \cdot g_4(x^2,y^2) = 1 \\ &\Leftrightarrow \quad 0 = 1 \end{aligned}$$

Because $0 \neq 1$ it follows that $|JF| \neq 1$. But $|JF| = 1$ is given. So the assumption must be wrong. So $\left\langle \begin{array}{c} f_4(x^2,y^2) \\ g_4(x^2,y^2) \end{array} \right\rangle = \left\langle \begin{array}{c} 0 \\ 0 \end{array} \right\rangle$ □

Now I can state the most important theorem of this section. If $F \in \mathbb{F}_p[x,y]^2$ and $|JF| = 1$, then it follows that JF can't have a term of odd degree (odd degree as defined in definition 15).

Theorem 19. *Let $F \in \mathbb{F}_2[x,y]^2$. If $|JF| = 1$ then JF has no term of odd degree.*

Proof. We will show that if $|JF| = 1$ and JF has a term of odd degree then $\left\langle \begin{array}{c} f_4(x^2,y^2) \\ g_4(x^2,y^2) \end{array} \right\rangle \neq \left\langle \begin{array}{c} 0 \\ 0 \end{array} \right\rangle$ (using notation 16 and 17). Choose i and j such that $x^i \cdot y^j$ is a term of JF. This term in the Jacobian matrix comes from a derivation of f or g in x or y. Without loss of generatity, I will assume it comes from a derivation to x. I now take the primitive, which is a term in F of the form $x^{i+1} \cdot y^j$. This is only possible if $2 \nmid i+1$, so i is even. Because the term $x^i \cdot y^j$ is odd, j must be odd.

So this means that there exists a term in F of the form $x^{i+1} \cdot y^j$, where $i+1$ and j are odd. This means that this term also has to be in $f_4\left(x^2, y^2\right)$ or $g_4\left(x^2, y^2\right)$. So not both f_4 and g_4 can be zero, a contradiction with lemma 18. $\square$

3.2.4 A zero in JF

In this section, I will consider the case where JF has a zero in one of its four entries. Without loss of generality, I can decide which entry of JF equals zero. I can also rewrite $|JF|$ such that it is a lot simpler.

Remark 20. *I may assume that* $JF = \left\langle \begin{array}{cc} \star & 0 \\ \star & \star \end{array} \right\rangle$.

Proof. If $\frac{\mathrm{d}}{\mathrm{d}x}F_1 = 0$, then I can consider $F' = \left\langle \begin{array}{c} F_1(y,x) \\ F_2(y,x) \end{array} \right\rangle$. If $\frac{\mathrm{d}}{\mathrm{d}x}F_2 = 0$, then I consider $F' = \left\langle \begin{array}{c} F_2(y,x) \\ F_1(y,x) \end{array} \right\rangle$. And the last case, $\frac{\mathrm{d}}{\mathrm{d}y}F_2 = 0$ can be replaced with $F' = \left\langle \begin{array}{c} F_2(x,y) \\ F_1(x,y) \end{array} \right\rangle$.

For these three cases F is an automorphism if and only if F' is an automorphism and $\frac{\mathrm{d}}{\mathrm{d}y}F'_1 = 0$. $\square$

Remark 21. *If* $\frac{\mathrm{d}}{\mathrm{d}y}F_1 = 0$ *then* $|JF| = \left(\frac{\mathrm{d}}{\mathrm{d}x}F_1\right) \cdot \left(\frac{\mathrm{d}}{\mathrm{d}y}F_2\right)$.

Proof.

$$\begin{aligned} |JF| &= \left| \begin{array}{cc} \frac{\mathrm{d}}{\mathrm{d}x}F_1 & 0 \\ \frac{\mathrm{d}}{\mathrm{d}x}F_2 & \frac{\mathrm{d}}{\mathrm{d}y}F_2 \end{array} \right| \\ &= \left(\frac{\mathrm{d}}{\mathrm{d}x}F_1\right) \cdot \left(\frac{\mathrm{d}}{\mathrm{d}y}F_2\right) \end{aligned}$$

$\square$

The following corollary follows directly from the previous remark.

Corollary 22. *If* $\frac{\mathrm{d}}{\mathrm{d}y}F_1 = 0$ *and* $|JF| \in k^*$, *then* $\frac{\mathrm{d}}{\mathrm{d}x}F_1 \in k^*$ *and* $\frac{\mathrm{d}}{\mathrm{d}y}F_2 \in k^*$.

Proof. From remark 21 follows that $|JF| = \left(\frac{\mathrm{d}}{\mathrm{d}x}F_1\right) \cdot \left(\frac{\mathrm{d}}{\mathrm{d}y}F_2\right)$. It is given that $|JF| \in k^*$. Because $|JF|$ is a product, and the result is a non-zero element of that field, both sides needs to be a non-zero element of the field. So it follows easily that

$$\begin{aligned} \frac{\mathrm{d}}{\mathrm{d}x}F_1 &\in k^* \\ \frac{\mathrm{d}}{\mathrm{d}y}F_2 &\in k^* \end{aligned}$$

$\square$

I want to use the knowledge about the derivatives of a polynomial to say something about the polynomial (for note that in characteristic p, the conclusions of the previous collary are not enough to ensure that F is an automorphism by themselves).

Lemma 23. *Let k be a field of characteristic p, and $f \in k[x,y]$ such that the following hold:*

- $p \nmid \deg_x f, p \nmid \deg_y f$
- $\frac{\mathrm{d}}{\mathrm{d}x} f \in k$, $\frac{\mathrm{d}}{\mathrm{d}y} f \in k$

Then $f = \left(\frac{\mathrm{d}}{\mathrm{d}x} f\right) \cdot x + \left(\frac{\mathrm{d}}{\mathrm{d}y} f\right) \cdot y + c$, where $c \in k$.

Proof. Write $f = c + p(x) + q(y) + \sum_{i,j \geq 1} a_{ij} \cdot x^i \cdot y^j$ $(p(0) = q(0) = 0)$. $k \ni \frac{\mathrm{d}}{\mathrm{d}x} f = \frac{\mathrm{d}}{\mathrm{d}x} p + \sum_{i,j \geq 1} i \cdot a_{ij} \cdot x^{i-1} \cdot y^j$ implies that $p = a \cdot x + p^\star(x^p), a_{ij} = 0$ if $p \nmid i$.

Similarly, $\frac{\mathrm{d}}{\mathrm{d}y} f \in k$ implies that $q = b \cdot y + q^\star(y^p), a_{ij} = 0$ if $p \nmid j$.

Thus, $f = c + a \cdot x + b \cdot y + p^\star(x^p) + q^\star(y^p) + \sum_{i,j \geq 1, p|i, p|j} a_{ij} \cdot x^i \cdot y^j$ which implies $f \in c + a \cdot x + b \cdot y + k[x^p, y^p] x^p + k[x^p, y^p] y^p$. Because of $p \nmid \deg_x f$, $p \nmid \deg_y f$, f must equal $a \cdot x + b \cdot y + c$. □

In conjecture 11, the degree extention is used. So if we want to say anything about that conjecture, we need to know something about the degree extionsion. So it is time to use that assumption. I want to simplify that assumption such that I can use it. For that, I reduce it to a statement on the degree. This reduction loses information, but for now it will be enough.

Condition 24. *I will add another condition to the Adjamagbo condition. This additional condition makes it still possible to prove the Jacobian Conjecture if it is proved for finite fields for every p.*

$$\begin{aligned}
\deg_x(F_1) > 0 &\Rightarrow p \nmid \deg_x(F_1) \\
\deg_y(F_1) > 0 &\Rightarrow p \nmid \deg_y(F_1) \\
\deg_x(F_2) > 0 &\Rightarrow p \nmid \deg_x(F_2) \\
\deg_y(F_2) > 0 &\Rightarrow p \nmid \deg_y(F_2)
\end{aligned}$$

Theorem 25. *Let k be a field of characteristic $p > 0$. Let $|JF| \in k^*$. Assume that JF does contain a zero in a position and that condition 24 is satisfied. Then F is invertible over k.*

Proof. Bij remark 20 we may assume that $\frac{\mathrm{d}}{\mathrm{d}y} F_1 = 0$. Then by corollary 22 we get at $\frac{\mathrm{d}}{\mathrm{d}x} F_1 \in k^*$ and $\frac{\mathrm{d}}{\mathrm{d}y} F_2 \in k^*$. It then follows from lemma 23 that $F_1 = \left(\frac{\mathrm{d}}{\mathrm{d}x} F_1\right) \cdot x + c$ for some $c \in k$. Let $\lambda = \frac{\mathrm{d}}{\mathrm{d}x} F_1 \in k^*$. So $F_1 = \lambda \cdot x + c$. Since $\frac{\mathrm{d}}{\mathrm{d}y} F_2 = \mu \in k^*$ we get $F_2 = \mu \cdot y + a(x, y^p)$. Since $p \nmid \deg_y(F_2)$ we deduce that $F_2 = \mu \cdot y + a(x)$. So $F = (F_1, F_2) = (\lambda \cdot x + c, \mu \cdot y + a(x))$ which is invertible over k. □

3.2.5 Constant entry in JF

Because we know how to deal with the problem if there is a zero in JF, I can now assume that JF doesn't contain a zero on any position. The next step is the case where there is a constant on a position in JF.

If there is a constant in JF, then I can make a very similar $\widetilde{F}$ such that $J\widetilde{F}$ contains a one on a position. Without loss of generality, I can again decide in which position that entry is.

Remark 26. *If JF has an entry in k^*, and $|JF| \in k^*$ then there exist a linear transformation L_1 and L_2 such that $G = L_1 \circ F \circ L_2$ satisfies $|JF| \in k^*$ and $\frac{\mathrm{d}}{\mathrm{d}y} G_1 = 1$.*

Remark 27. *If f is a polynomial and $\frac{\mathrm{d}}{\mathrm{d}x} f = a$, where $a \in k$. Then there exists an l such that $f = a \cdot x + l(x^p, y)$.*

I again have to use the assumption on the extention degree. Again, I make a reduction and I throw away part of the information, because that information is difficult to use. What is left are some easy degree demands.

The only tricky part of this lemma is that the degrees of the polynomials can be zero. So I also need to prove that that doesn't happen because JF doesn't contain a zero.

Lemma 28. *If JF doesn't contain a zero on a position, then*

- $[k(x)(y) : k(x)(F_1)]$ *is finite.*
- $[k(y)(x) : k(y)(F_1)]$ *is finite.*
- $[k(x)(y) : k(x)(F_2)]$ *is finite.*
- $[k(y)(x) : k(y)(F_2)]$ *is finite.*

Proof. I prove the first case, as the proof of the other cases is simular.

If $\deg_y(F_1) > 0$, then $[k(x)(y) : k(x)(F_1)] = \deg_y F_1$, so it is clearly finite. This means that we only have to prove that $\deg_y(F_1) > 0$. So suppose $\deg_y F_1$ is at most zero. Then $F_1(x, y) = F_1(x, 0)$. So I can write $F_1 = F_1'(x)$. Now I consider $\frac{\mathrm{d}}{\mathrm{d}y} F_1 = \frac{\mathrm{d}}{\mathrm{d}y} F_1'(x) = 0$. But one of the conditions was that there isn't a zero on a position in the Jacobian. Contradiction, so $\deg_y(F_1) > 0$ hence $[k(x)(F_1) : k(x)(y)] = \deg_y(F_1)$ is finite. □

Corollary 29. *If JF doesn't contain a zero on a position, then*

- $\deg_x F_1 > 0$
- $\deg_y F_1 > 0$
- $\deg_x F_2 > 0$
- $\deg_y F_2 > 0$

Proof. This is already proven in the proof of lemma 28. □

I can now use the above corollary to say something substancial about the degree:

Lemma 30. *($k = \mathbb{F}_p$) If $JF = 1$, JF doesn't contain a zero on a position, $p \nmid [k(F,:)\, k(x,y)]$ and condition 24 holds, then:*

- $p \nmid \deg_x F_1$
- $p \nmid \deg_y F_1$
- $p \nmid \deg_x F_2$
- $p \nmid \deg_y F_2$

Proof. This is proved imediately from the consequence of condition 24 with that remark that the depends in that condition are satisfied by the conclusions of lemma 29. □

Theorem 31. *Let k be a field of characteristic $p > 0$ and $|JF| \in k^*$. Assume that condition 24 is statisfied and that the Adjamagbo condition is statisfied. If JF contains a constant in any position, then F is invertible over k.*

Proof. By theorem 25, we may assume that the constant is non-zero and hence by remark 26 we may assume that $\frac{\mathrm{d}}{\mathrm{d}x}F_1 = 1$. So $F_1 = x + a(x^p, y)$. Since $p \nmid \deg_x(F_1)$ (follows from lemma 30) we get that $F_1 = x + a(y)$. Replace F by $F \circ (x - a(y), y)$. This replacing does not change the condition that $|JF| \in k^*$. The Adjamagbo condition also is still satisfied. Since in the remainder of this argument, we don't use condition 24 anymore, we may assume that $F_1 = x$. Since $|JF| = 1$ this implies that $\frac{\mathrm{d}}{\mathrm{d}y}F_2 = 1$. So $F_2 = y + b(x, y^p)$. Finally, since $p \nmid [k(x,y) : k(F_1, F_2)] = [k(x,y) : k(x, y + b(x, y^p))] = [k(x)(y) : k(x)(y + b(x, y^p))]$, it follows that $\deg_y (b(x, y^p) = 0$. So $b = b(x)$ hence $F_2 = y + b(x)$, and thus follows that $F = (x, y + b(x))$ which is invertible over k. □

3.2.6 $\mathbf{JF \in M_{2,2}(k\,[x^2, y^2])}$

I will assume here that JF doesn't have a zero entry, because I already proved that case. Using notation 16, the Jacobian of F now looks as follows:

$$JF = \begin{pmatrix} f_2(x^2, y^2) & f_3(x^2, y^2) \\ g_2(x^2, y^2) & g_3(x^2, y^2) \end{pmatrix}$$

I remark that:

$$F = \left(xf_2(x^2, y^2) + yf_3(x^2, y^2) + f_1(x^2, y^2), xg_2(x^2, y^2) + yg_3(x^2, y^2) + g_1(x^2, y^2)\right)$$

The following lemma should make the problem left to solve easier. But this document will not prove the remaining cases. The following lemma say something about how the different degrees are connected.

Lemma 32. *If $JF \in M_{2,2}\left(k\left[x^2, y^2\right]\right)$, $|JF| = 1$, condition 24 is satisfied and JF doesn't have a zero in any position, then the following equalities hold:*

$$\begin{aligned}
\deg_x\left(\frac{\mathrm{d}}{\mathrm{d}x}F_1\right) &\geq \deg_x\left(\frac{\mathrm{d}}{\mathrm{d}y}F_1\right)\\
\deg_y\left(\frac{\mathrm{d}}{\mathrm{d}y}F_1\right) &\leq \deg_y\left(\frac{\mathrm{d}}{\mathrm{d}x}F_1\right)\\
\deg_x\left(\frac{\mathrm{d}}{\mathrm{d}x}F_2\right) &\geq \deg_x\left(\frac{\mathrm{d}}{\mathrm{d}y}F_2\right)\\
\deg_y\left(\frac{\mathrm{d}}{\mathrm{d}y}F_2\right) &\leq \deg_y\left(\frac{\mathrm{d}}{\mathrm{d}x}F_2\right)
\end{aligned}$$

Proof. The proof of every of these equalities are the same. So I only prove the first one.

From lemma 30 follows that $2 \nmid \deg_x(F_1)$. Because

$$\deg_x(F_1) = \deg_x\left(x \cdot f_2(x^2, y^2) + y \cdot f_3(x^2, y^2) + f_1(x^2, y^2)\right)$$

But the last is also equal to: $\max\{1 + 2 \cdot \deg_x f_2(x, y), 2 \cdot \deg_x f_3(x, y), 2 \cdot f_1(x, y)\}$. So it follows that

$$\deg_x f_2(x^2, y^2) \geq \deg_x f_3(x^2, y^2)$$

In the same way follows:

$$\begin{aligned}
\deg_y f_2(x^2, y^2) &\leq \deg_y f_3(x^2, y^2)\\
\deg_x g_2(x^2, y^2) &\geq \deg_x g_3(x^2, y^2)\\
\deg_y g_2(x^2, y^2) &\leq \deg_y g_3(x^2, y^2)
\end{aligned}$$

Now I only need to remark that from notation 16 follows that $\frac{\mathrm{d}}{\mathrm{d}x}F_1 = f_2$, $\frac{\mathrm{d}}{\mathrm{d}y}F_1 = f_3$, $\frac{\mathrm{d}}{\mathrm{d}x}F_2 = g_2$ and $\frac{\mathrm{d}}{\mathrm{d}y}F_2 = g_3$. $\square$

Chapter 4

Alternatives

Definition 33. *Let $F : \mathbb{Z}^n \to \mathbb{Z}^n$ be such that*

$$F_l : (x_1, \ldots, x_n) \mapsto \sum_{i \in \mathbb{N}^n} a_{l,i} \cdot \prod_{j=1}^{n} x_j^{i_j}$$

Let A be defined as

$$A := \{a_{i,j} | 1 \leq i \in \mathbb{N} \leq n \wedge j \in \mathbb{N}^n\}$$

Let J be the Jacobian determinant of F. J can be written down as

$$J = \sum_{i \in \mathbb{N}^n} \left(J_i \cdot \prod_{j=1}^{n} x_j^{i_j} \right)$$

where J_i are coefficients in $\mathbb{Z}[A]$. For all i, I rewrite J_i as follows:

$$J_i = \sum_{k=0}^{\infty} p^k \cdot J_i^{(k)}$$

where $J_i^{(k)}$ in $\{0, 1, \ldots, p-1\}[A]$.

Now let $\overline{J_i^{(k)}} \in \mathbb{F}_p$ be derived from $J_i^{(k)}$ by calculating modulo p.

Then we say $\overline{F} := F \pmod{p}$ satisfies the FZ conditions if and only if

$$\overline{J_i^{(k)}} = \begin{cases} 1 & \text{if } \bar{i} = 0 \text{ and } k = 0 \\ 0 & \text{otherwise} \end{cases}$$

It seemed plausible that FZ met exactly the requirements to replace the Jacobian Condition in characteristic p, but the following example shows otherwise:

Example 34. *If $\overline{F}$ is a tame automorfisme in $\mathbb{F}_p$, then the FZ conditions don't follow automaticly.*

Proof. Consider the following automorphism:

$$\begin{pmatrix} x + y^2 \\ y \end{pmatrix} \circ \begin{pmatrix} x \\ x^2 + y \end{pmatrix} = \begin{pmatrix} x + y^2 \\ x^2 + 2 \cdot x \cdot y^2 + y + y^4 \end{pmatrix}$$

In $\mathbb{F}_2$, this will be

$$\begin{pmatrix} x + y^2 \\ x^2 + y + y^4 \end{pmatrix}$$

I take this F as the base of the conditions. I first look to what the a-variables are.

$$a_{i,j} = \begin{cases} 1 \text{ if } & \begin{array}{l} (i = 1 \wedge (j = (1,0) \vee j = (0,2))) \vee \\ (i = 2 \wedge (j = (2,0) \vee j = (0,1) \vee j = (0,4))) \end{array} \\ 0 \text{ otherwise} \end{cases}$$

I don't write $a_{i,j}$ if $a_{i,j} = 0$. I can do that because they disappear later without using it.

I now examine $J\overline{F}$:

$$J\overline{F} = \begin{vmatrix} 1 & 2 \cdot a_{1,(0,2)} \cdot y \\ 2 \cdot a_{2,(2,0)} \cdot x & 1 + 4 \cdot a_{2,(0,4)} \cdot y^3 \end{vmatrix}$$

$$J\overline{F} = 1 + 4 \cdot a_{2,(0,4)} \cdot y^3 - 4 \cdot a_{1,(0,2)} \cdot a_{2,(2,0)} \cdot x \cdot y$$

I look at the J_i in J. If J_i is zero, then I don't write it down.

$$\begin{aligned} J_{(0,0)} &= 1 \\ J_{(0,4)} &= 4 \cdot a_{2,(0,4)} \\ J_{(1,1)} &= -4 \cdot a_{1,(0,2)} \cdot a_{2,(2,0)} \end{aligned}$$

From here, I write down $J_i^{(k)}$, and again I don't write it down if it zero:

$$\begin{aligned} J_{(0,0)}^{(0)} &= 1 \\ J_{(0,4)}^{(2)} &= a_{2,(0,4)} \\ J_{(1,1)}^{(2)} &= -a_{1,(0,2)} \cdot a_{2,(2,0)} \end{aligned}$$

According to the constrains of FZ, $J_{(0,4)}^{(2)}$ should be zero, but it is nonzero. So this is a counterexample.

Obviously, it is stil an interesting open question to determine the right set of equations defining the set of automorphisms. $\square$

Chapter 5

Compositions

5.1 Lowest non-linear degree

I first want to show what happens if two mappings are composed. I am especially interested in the case where all the lower terms vanish (except the lineair terms). I want to say something about the lowest non-linear part of a F. I hope to say something about a polynomial mapping not being an automorphism by only looking to the lowest non-linear terms. But to do that, I first look at a general case.

I don't make any assumptions about the size of the field k. I start with only the case $n = 2$.

I need a notation which gives me all the terms of a degree a out of a polynomial F:

Definition 35. *Let* $P = \sum_{(i,j)\in\mathbb{N}^2} a_{i,j}x^iy^j$. *Then I define*

$$P^{\ominus a} := \sum_{i=0}^{a} a_{i,a-i}x^iy^{a-i}$$

Because we are interested in polynomial maps, and a mapping can be seen as a collection of polynomials, I also define this notation for polynomial maps. Because I only consider mappings from $k^2 \to k^2$, I restrict my definition to dimension two, but it is easy to see how to extent this to a more general case.

Definition 36. *If* $F = \left\langle \begin{array}{c} f \\ g \end{array} \right\rangle$, *then* $F^{\ominus a} = \left\langle \begin{array}{c} f^{\ominus a} \\ g^{\ominus a} \end{array} \right\rangle$.

5.2 Technical details

If F, G are two polynomial maps, then I want to describe $(F \circ G)^{\ominus c}$ for certain cases. In order to do that, I need some technical definitions.

If $s \in \mathbb{N}$ and $v \in \mathbb{N}^s$, then denote

$$y^v := y_1^{v_1} \cdot y_2^{v_2} \cdot \ldots \cdot y_s^{v_s}$$

Next to the standard grading deg on $k[y_1, \ldots, y_b]$ we also define the non-standard grading $\widetilde{\deg}$ by $\widetilde{\deg(y_i)} = i$. Hence, if $\nabla := (1, 2, \ldots, n)$ and $\mathbb{1} := (1, 1, \ldots, 1)$, then $\widetilde{\deg}\,(y^v) = \langle \nabla, v \rangle$, $\deg\,(y^v) = \langle \mathbb{1}, v \rangle$.

Now $(y_1 + y_2 + \ldots + y_{c-1})^b$ has several terms of $\widetilde{\deg}$-degree c. These are exactly the terms y^v, where $\langle \mathbb{1}, v \rangle = b$ and $\langle \nabla, v \rangle = c$.

Let us definie

Definition 37.

$$V_{b,c} := \left\{ v \in \mathbb{N}^{c-1} | \, \langle \mathbb{1}, v \rangle = b \text{ and } \langle \nabla, v \rangle = c \right\}$$

The coefficient of the term y^v in $(y_1 + \ldots + y_{c-1})^b$ can be computed and is equal to:

$$\binom{b}{v} = \binom{b}{v_1, v_2, \ldots, v_{c-1}} = \frac{b!}{v_1! \cdot v_2! \cdot \ldots \cdot v_{c-1}!}$$

where $\binom{b}{v}$ is the generalized binomial coefficient.

We now define:

Definition 38.

$$W_{b,c} := \left\{ \binom{b}{c} \cdot y^v | v \in V_{b,c} \right\}$$

I now make some substitutions for $y_1, \ldots, y_{c-1}$.

Remark 39. *Using the definition above, I can now calculate the following:*

$$\left(\left\langle \begin{array}{c} x + y^b \\ y \end{array} \right\rangle \circ G \right)^{\ominus c} = G^{\ominus c} + \sum_{w \in W_{b,c}} \left\langle \begin{array}{c} w\left(G^{\ominus 1}, G^{\ominus 2}, \ldots, G^{\ominus c-1}\right) \\ 0 \end{array} \right\rangle$$

where $G = G^{\ominus 1} + G^{\ominus 2} + \ldots$.

This also gives the usefullness of this definition: I can write an elementary map composed combined with a given map G. Now I will give the object of interest of this chapter:

Definition 40. *If* $F = \left\langle \begin{array}{c} x \\ y \end{array} \right\rangle + F^{\ominus 2} + F^{\ominus 3} + \ldots$ *and* $F^{\ominus 2}, F^{\ominus 3}, \ldots, F^{\ominus i-1} = 0$, *then we say that* F *is of lower-degree* i. *Note that I do not demand that* $F^{\ominus i} \neq 0$.

The next lemma follows directly from this:

Lemma 41. *If* F *is of lower degree* i *and* a *is an invertible lineair mapping, then* $a^{-1} \circ F \circ a$ *is also of lower degree* i.

Proof. This proof is easy. □

From the Jung-van den Kulk theorem, we know that every map in dimension 2 is tame. That means, every mapping can be written as $G_j \circ G_{j-1} \circ \ldots \circ G_1$ and only G_1 is affine, the others are either lineair, or of the form $\left\langle \begin{array}{c} x + \lambda \cdot y^i \\ y \end{array} \right\rangle$ with $i > 1$ and $\lambda \in k$.

Definition 42. *If* $G = G_i \circ \ldots G_2 \circ G_1$ *and* $j \leq i$, *then* $\overline{G}_j := G_j \circ \ldots \circ G_2 \circ G_1$.

5.3 Example

I will go over the definitions above again, but now with an example. That way, it is more clear what happens.

I start with $G := \left\langle \begin{array}{c} x+y^3 \\ y \end{array} \right\rangle$, $F = \left\langle \begin{array}{c} x+y^2+x^2\cdot y^2 \\ y+x^3 \end{array} \right\rangle$. I will use the field $\mathbb{F}_2$. I remark the following about F and G:

- $F^{\ominus 2} = \left\langle \begin{array}{c} y^2 \\ 0 \end{array} \right\rangle$
- $F^{\ominus 3} = \left\langle \begin{array}{c} 0 \\ x^3 \end{array} \right\rangle$
- $F^{\ominus 4} = \left\langle \begin{array}{c} x^2\cdot y^2 \\ 0 \end{array} \right\rangle$
- F is of lower degree 2.
- G is of lower degree 3.
- $V_{1,1} = \emptyset$
- $V_{2,1} = \emptyset$
- $V_{1,2} = \emptyset$
- $V_{2,2} = \{(2)\}$
- $V_{3,2} = \emptyset$
- $V_{1,3} = \emptyset$
- $V_{2,3} = \{(1,1)\}$
- $V_{3,3} = \{(3,0)\}$
- $V_{1,4} = \emptyset$
- $V_{2,4} = \{(1,0,1)\}$
- $V_{3,4} = \{(2,1,0)\}$
- $V_{4,4} = \{(4,0,0)\}$
- $V_{1,5} = \emptyset$
- $V_{2,5} = \{(1,0,0,1)\}$
- $V_{3,5} = \{(2,0,1,0)\}$
- $V_{4,5} = \{(3,1,0,0)\}$
- $V_{5,5} = \{(5,0,0,0)\}$
- $V_{1,6} = \emptyset$
- $V_{2,6} = \{(1,0,0,0,1)\}$

- $V_{3,6} = \{(2,0,0,1,0), (1,1,1,0,0)\}$
- $V_{4,6} = \{(3,0,1,0,0)\}$
- $V_{5,6} = \{(4,1,0,0,0)\}$
- $V_{6,6} = \{(6,0,0,0,0)\}$
- $W_{1,1} = \emptyset$
- $W_{2,2} = \left\{ \begin{pmatrix} 2 \\ 2 \end{pmatrix} x_1^2 \right\}$
- $W_{3,4} = \left\{ \begin{pmatrix} 3 \\ (2,1,0) \end{pmatrix} \cdot x_1^2 \cdot x_2^1 \cdot x_3^0 \right\}$
- $W_{3,6} = \left\{ \begin{array}{l} \begin{pmatrix} 3 \\ (2,1) \end{pmatrix} \cdot x_1^2 \cdot x_4^1, \\ \begin{pmatrix} 3 \\ (1,1,1) \end{pmatrix} \cdot x_1^1 \cdot x_2^1 \cdot x_3^1 \end{array} \right\}$
- $\left(\left\langle \begin{array}{c} x+y^2 \\ y \end{array} \right\rangle \circ G \right)^{\ominus c} = G^{\ominus 2} + \left\langle \begin{array}{c} \begin{pmatrix} 3 \\ 2 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} \cdot \left(G^{\ominus 1}\right)^2 \cdot \left(G^{\ominus 2}\right)^1 \\ 0 \end{array} \right\rangle$

5.4 Vectorspace

Definition 43. *Let* End_i *be the set all polynomial mappings which only contains terms of degree exactly* i.

Definition 44. *Define* $\mathrm{End}_{>i} := \sum_{k=i+1}^{\infty} \mathrm{End}_k$.

Definition 45. *Let* $D \subset \mathbb{N}$. *Then I define*

$$V_D := \left\{ v \in \sum_{i \in D} \mathrm{End}_i \,|\, I + v + H_{>\max(D)} \in GA_n(k), H_{>\max(D)} \in \mathrm{End}_{>\max(D)} \right\}$$

Definition 46. *Let* $d \in \mathbb{N}$. *Then I define* $V_d := V_{\{d\}}$.

Lemma 47. *If* k *is a finite space with* p *elements (*p *prime), and* V *is a subspace of a vector space over* k. *Then* V *is a vector space if and only if* V *is closed under addition.*

Proof. From left to right is easy: if V is a vector space, then it is closed under addition. From right to left I only need to prove that V is closed under scalar multiplication. If V is closed under addtition and scalar multiplication, then V is a vectorspace. Let $\overline{a} \in k$ an element of k, and v an element of V. Let a be the smallest strictly positive number such that $a + p\mathbb{Z} = \overline{a}$. Because V is closed under addition, $b := \sum_{i=1}^{a} v$ is defined. I now remark that $b = a \cdot v$ and $b \in V$, so $a \cdot v \in V$. $\square$

Lemma 48. $(k = \mathbb{F}_2)$ *Let* $b := \left\langle \begin{array}{c} x + p(y) \\ y \end{array} \right\rangle$, *where* $p(y) = a_2 \cdot y^2 + a_3 \cdot y^3 + \ldots + a_d \cdot y^d$ *and let* $F = J_1 + J_2 + J_3 + \ldots$, *where* J_i *is homogenous of degree* i. *Let* $b \circ F$ *be written as* $J_1' + J_2' + \ldots$, *where* J_i' *is homogenous of degree* i. *Now*

- $J_1' = J_1$
- $J_2' = J_2 + \left\langle \begin{array}{c} a_2 \cdot (J_1')_2^2 \\ 0 \end{array} \right\rangle = J_2 + \left\langle \begin{array}{c} a_2 \cdot y^2 \\ 0 \end{array} \right\rangle \circ J_1$
- $J_3' = J_3 + \left\langle \begin{array}{c} a_2 \cdot (J_1')_2^3 \\ 0 \end{array} \right\rangle = J_2 + \left\langle \begin{array}{c} a_2 \cdot y^3 \\ 0 \end{array} \right\rangle \circ J_1$

Proof.

$$\begin{aligned}
b \circ F &= \left\langle \begin{array}{c} x + a_2 \cdot y^2 + a_3 \cdot y^3 + \ldots + a_d \cdot y^d \\ y \end{array} \right\rangle \circ \left(\sum_{i=1}^{\infty} J_i \right)) \\
&= \sum_{i=1}^{\infty} J_i + \left\langle \begin{array}{c} a_2 \\ 0 \end{array} \right\rangle \cdot \left(\sum_{i=1}^{\infty} (J_i)_2 \right)^2 + \sum_{j=3}^{\infty} \left\langle \begin{array}{c} a_j \\ 0 \end{array} \right\rangle \cdot \left(\sum_{i=1}^{\infty} (J_i)_2 \right)^j \\
&= \sum_{i=1}^{\infty} J_i + \sum_{i=1}^{\infty} \left\langle \begin{array}{c} a_2 \cdot (J_i)_2^2 \\ 0 \end{array} \right\rangle + \sum_{j=3}^{\infty} \left(\sum_{i=1}^{\infty} \left\langle \begin{array}{c} a_j \cdot (J_i)_2 \\ 0 \end{array} \right\rangle \right)^j
\end{aligned}$$

Now it is neccessary to carefully find homogeneous parts of degree 1, 2 and 3.

$\sum_{\mathbf{i=1}}^{\infty} \mathbf{J_i}$**:** This parts means that $J_i' = J_i + \ldots$.

$\sum_{\mathbf{i=1}}^{\infty} \left\langle \begin{array}{c} a_2 \cdot (J_i)_2^2 \\ 0 \end{array} \right\rangle$**:** This contains only terms of even degree. So J_1' and J_3' are not affected by this part. $J_2' = \left\langle \begin{array}{c} a_2 \cdot J_1^2 \\ 0 \end{array} \right\rangle + \ldots$, so so far, we have $J_2' = J_1 + \left\langle \begin{array}{c} a_2 \cdot J_1^2 \\ 0 \end{array} \right\rangle + \ldots$.

$\sum_{\mathbf{j=3}}^{\infty} \left(\sum_{\mathbf{i=1}}^{\infty} \left\langle \begin{array}{c} a_j \cdot (J_i)_2 \\ 0 \end{array} \right\rangle \right)^{\mathbf{j}}$**:** Because every part on the inside of power has at least degree 1, every j strictly bigger then 3 only contribute terms of degree 4 and higher. Because we are only interested in what happens to J_1', J_2' and J_3', only the case $j = 3$ is left.

To get terms of degree 3 when taking a power of 3 without a affine part, we only need to look at those terms inside the power of degree exactly one. This means that $J_3' = \left\langle \begin{array}{c} a_3 \cdot (J_1)_2 \\ 0 \end{array} \right\rangle + \ldots$. This means that so far, we have $J_3' = J_3 + \left\langle \begin{array}{c} a_3 \cdot (J_1)_2 \\ 0 \end{array} \right\rangle + \ldots$.

That's all Because we have discussed all parts of $b \circ F$, there cannot be other things contributing to J_i'. So we can make a conclusion:

- $J_1' = J_1$
- $J_2' = J_2 + \left\langle \begin{array}{c} a_2 \cdot (J_1')_2^2 \\ 0 \end{array} \right\rangle = J_2 + \left\langle \begin{array}{c} a_2 \cdot y^2 \\ 0 \end{array} \right\rangle \circ J_1$
- $J_3' = J_3 + \left\langle \begin{array}{c} a_2 \cdot (J_1')_2^3 \\ 0 \end{array} \right\rangle = J_3 + \left\langle \begin{array}{c} a_2 \cdot y^3 \\ 0 \end{array} \right\rangle \circ J_1$

□

Lemma 49. *Let $k = \mathbb{F}_2$ and let F and G automorphisms of the form $F = H_1(x,y) + H_2(x,y) + \ldots$ where $H_1(x,y) = I$ and $G = J_1(x,y) + J_2(x,y) + \ldots$, where H_i and J_i are homogenous of degree i.*

Lets write $G \circ F = K_1(x,y) + K_2(x,y) + \ldots$. Now the following conditions hold:

- $K_1(x,y) = J_1(x,y) \circ H_1(x,y)$
- $K_2(x,y) = J_1(x,y) \circ H_2(x,y) + J_2(x,y)$
- $K_3(x,y) = J_1(x,y) \circ H_3(x,y) + J_3(x,y)$

Proof. Because G also is tame, G can also be written as $b_m \circ b_{m-1} \circ \ldots \circ b_1$, where b_i is either linear or Jonquière. I will prove this by induction to m. Define $G_i := b_i \circ \ldots \circ b_1 \circ \left\langle \begin{array}{c} x \\ y \end{array} \right\rangle$. The induction will be that all the conditions hold for $G_i \circ F$.

Base step I will prove the conditions hold for G_0. Note that $G_0 = \left\langle \begin{array}{c} x \\ y \end{array} \right\rangle$. That means that $G_0 \circ F = F$, so $K_i = H_i$. Also, $J_1(x,y)$ is the identity, so $J_1(x,y) \circ H_i(x,y) = H_i(x,y)$. Also, $J_i = 0$ if i is 1 or bigger. This is enough to prove the equations above.

Induction step Suppose the equations hold for $G_i \circ F$. I hope to prove that the conditions also hold for G_{i+1}. To avoid using the same names for different objects, I will add accents to K and J in the induction step. Because $G_{i+1} = b_{i+1} \circ G_i$, I will say something about the two possibilities for b_{i+1}.

$\mathbf{b_{i+1}}$ is linear Because b_{i+1} is linear, $b_{i+1} \circ (J_1(x,y) \circ H_2(x,y) + J_2(x,y)) = b_{i+1} \circ J_1(x,y) \circ H_2(x,y) + b_{i+1} \circ J_2(x,y)$. I note that $b_{i+1} \circ J_2(x,y) = J_2'(x,y)$, so $K_2'(x,y) = J_1'(x,y) \circ H_2(x,y) + J_2'(x,y)$. The case for K_3' is essentially the same as K_2'. The case K_1' is obvious, because it only contains compositions.

$\mathbf{b_{i+1}}$ is Jonquière I can now assume

$$b_{i+1} = \left\langle \begin{array}{c} x + p(y) \\ y \end{array} \right\rangle = \left\langle \begin{array}{c} x + \sum_{i=2}^{\infty} a_i \cdot y^i \\ y \end{array} \right\rangle$$

Note that $J_1' = J_1$

$$
\begin{aligned}
G_{i+1} \circ F &= b_{i+1} \circ G_i \circ F \\
&= \left\langle \begin{array}{c} x + p(y) \\ y \end{array} \right\rangle \circ G_i \circ F \\
&= \left\langle \begin{array}{c} x + p(y) \\ y \end{array} \right\rangle \circ (K_1(x,y) + K_2(x,y) + \ldots) \\
&= K_1(x,y) + K_2(x,y) + \ldots + \\
&\quad \left\langle \begin{array}{c} p\left(K_1(x,y)_2 + K_2(x,y)_2 + \ldots\right) \\ 0 \end{array} \right\rangle \\
&= K_1(x,y) + K_2(x,y) + \ldots + \\
&\quad \left\langle \begin{array}{c} \sum\limits_{j=1}^{\infty} a_2 \cdot K_j(x,y)_2^2 + \sum\limits_{i=3}^{\infty} a_i \cdot \left(\sum\limits_{j=1}^{\infty} K_j(x,y)_2 \right)^i \\ 0 \end{array} \right\rangle \\
K_1'(x,y) &= K_1(x,y) \\
K_2'(x,y) &= K_2(x,y) + \left\langle \begin{array}{c} \left([K_1(x,y)]_2\right)^2 \\ 0 \end{array} \right\rangle \\
&= J_1(x,y) \circ H_2(x,y) + J_2(x,y) + \left\langle \begin{array}{c} \left([K_1(x,y)]_2\right)^2 \\ 0 \end{array} \right\rangle \\
&= J_1'(x,y) \circ H_2(x,y) + J_2'(x,y) \\
K_3'(x,y) &= K_3(x,y) + \left\langle \begin{array}{c} \left([K_1(x,y)]_2\right)^3 \\ 0 \end{array} \right\rangle \\
&= J_1(x,y) \circ H_3(x,y) + J_3(x,y) + \left\langle \begin{array}{c} \left([K_1(x,y)]_2\right)^3 \\ 0 \end{array} \right\rangle \\
&= J_1'(x,y) \circ H_3(x,y) + J_3'(x,y)
\end{aligned}
$$

□

I will prove the same lemma in a different way. For that, I need some lemma's to make the addition proof go smoothly.

Lemma 50. *Let F and G be polynomial automorphisms of the form $F = H_1(x,y) + H_2(x,y) + \ldots$ and $G = J_1(x,y) + J_2(x,y) + \ldots$, where $H_1(x,y) = I$ and H_i and J_i are homogenous of degree i. Let $a, b \in \mathbb{N}$ such that $b < a$.*

Then $\left(G^{\ominus a} \circ F\right)^{\ominus b} = 0$

Proof. Note that $F_1^{\ominus 0} = 0$ and $F_2^{\ominus 0} = 0$. Therefor, the degree of every term in $x^i \cdot y^j \circ F$ is at least $i + j$. So for every term g in $G^{\ominus a}$, $g \circ F$ is of degree at least a. So that also goes for the sum of the terms, which means that $G^{\ominus a} \circ F$ only contains terms of degree at least a. Because $b < a$, it means that it doesn't contain any term of degree b, and thus $\left(G^{\ominus a} \circ F\right)^{\ominus b} = 0$. □

Lemma 51. *Let F and G be polynomial automorphisms of the form $F = H_1(x,y) + H_2(x,y) + \ldots$ and $G = J_1(x,y) + J_2(x,y) + \ldots$, where $H_1(x,y) = I$ and H_i and J_i are homogenous of degree i. Let $a \in \mathbb{N}$.*

Then $\left(G^{\ominus a} \circ F\right)^{\ominus a} = G^{\ominus a}$

Proof. Let g be a term of $G^{\ominus a}$. Let $c \in k$, $i \in \mathbb{N}$ such that $g = c \cdot x^i \cdot y^{a-i}$. Now I look at $g \circ F$. $g \circ F = c \cdot \left(F_1^{\ominus 1} + F_1^{\ominus 2} + \ldots\right)^i \cdot \left(F_2^{\ominus 1} + F_2^{\ominus 2} + \ldots\right)^{a-i}$. From here it follows that $(g \circ F)^{\ominus a} = c \cdot \left(F_1^{\ominus 1}\right)^i \cdot \left(F_2^{\ominus 1}\right)^{a-i}$.

Because $F_1^{\ominus 1} = H_1(x,y)_1 = x$ and $F_2^{\ominus 1} = H_1(x,y)_2 = y$, $(g \circ F)^{\ominus a} = g$. Because $G^{\ominus a}$ is a sum of terms like g, $\left(G^{\ominus a} \circ F\right)^{\ominus a} = G^{\ominus a}$ □

Lemma 52. *Let $k = \mathbb{F}_2$. Let F and G be polynomial automorphisms of the form $F = H_1(x,y) + H_2(x,y) + \ldots$ and $G = J_1(x,y) + J_2(x,y) + \ldots$, where $H_1(x,y) = I$ and H_i and J_i are homogenous of degree i. Write $G^{\ominus 2} = \left\langle \begin{array}{c} b_{20} \cdot x^2 + b_{11} \cdot x \cdot y + b_{02} \cdot y^2 \\ c_{20} \cdot x^2 + c_{11} \cdot x \cdot y + c_{02} \cdot y^2 \end{array} \right\rangle$.*

Then $\left(G^{\ominus 2} \circ F\right)^{\ominus 3} = \left\langle \begin{array}{c} b_{11} \\ c_{11} \end{array} \right\rangle (F_1 \cdot F_2)^{\ominus 3}$

Proof.

$$\begin{aligned}
\left(G^{\ominus 2} \circ F\right)^{\ominus 3} &= \left\langle \begin{array}{c} b_{20} \cdot x^2 + b_{11} \cdot x \cdot y + b_{02} \cdot y^2 \\ c_{20} \cdot x^2 + c_{11} \cdot x \cdot y + c_{02} \cdot y^2 \end{array} \right\rangle \circ F^{\ominus 3} \\
&= \left\langle \begin{array}{c} b_{20} \cdot F_1^2 + b_{11} \cdot F_1 \cdot F_2 + b_{02} \cdot F_2^2 \\ c_{20} \cdot F_1^2 + c_{11} \cdot F_1 \cdot F_2 + c_{02} \cdot F_2^2 \end{array} \right\rangle^{\ominus 3} \\
&= \left\langle \begin{array}{c} b_{20} \cdot F_1^2 \\ c_{20} \cdot F_1^2 \end{array} \right\rangle^{\ominus 3} + \left\langle \begin{array}{c} b_{11} \cdot F_1 \cdot F_2 \\ c_{11} \cdot F_1 \cdot F_2 \end{array} \right\rangle^{\ominus 3} + \left\langle \begin{array}{c} b_{02} \cdot F_2^2 \\ c_{02} + F_2^2 \end{array} \right\rangle^{\ominus 3} \\
&= \left(\left\langle \begin{array}{c} b_{20} \\ c_{20} \end{array} \right\rangle F_1^2\right)^{\ominus 3} + \left(\left\langle \begin{array}{c} b_{11} \\ c_{11} \end{array} \right\rangle F_1 F_2\right)^{\ominus 3} + \left(\left\langle \begin{array}{c} b_{02} \\ c_{02} \end{array} \right\rangle F_2^2\right)^{\ominus 3} \\
&= \left\langle \begin{array}{c} b_{20} \\ c_{20} \end{array} \right\rangle \cdot \left(F_1^2\right)^{\ominus 3} + \left\langle \begin{array}{c} b_{11} \\ c_{11} \end{array} \right\rangle \cdot (F_1 \cdot F_2)^{\ominus 3} + \left\langle \begin{array}{c} b_{02} \\ c_{02} \end{array} \right\rangle \cdot \left(F_2^2\right)^{\ominus 3} \\
&= \left\langle \begin{array}{c} b_{20} \\ c_{20} \end{array} \right\rangle \left(2F_1^{\ominus 1} F_1^{\ominus 2}\right) + \left\langle \begin{array}{c} b_{11} \\ c_{11} \end{array} \right\rangle (F_1 F_2)^{\ominus 3} + \left\langle \begin{array}{c} b_{02} \\ c_{02} \end{array} \right\rangle \left(2F_2^{\ominus 1} F_2^{\ominus 2}\right) \\
&= 0 + \left\langle \begin{array}{c} b_{11} \\ c_{11} \end{array} \right\rangle \cdot (F_1 \cdot F_2)^{\ominus 3} + 0 \\
&= \left\langle \begin{array}{c} b_{11} \\ c_{11} \end{array} \right\rangle \cdot (F_1 \cdot F_2)^{\ominus 3}
\end{aligned}$$

□

Lemma 53. *Let $k = \mathbb{F}_2$ and let F and G be automorphisms of the form $F = H_1(x,y) + H_2(x,y) + \ldots$ where $H_1(x,y) = I$ and $G = J_1(x,y) + J_2(x,y) + \ldots$, where H_i and J_i are homogenous of degree i.*

Lets write $G \circ F = K_1(x,y) + K_2(x,y) + \ldots$. Now the following conditions hold:

- $K_1(x,y) = J_1(x,y) \circ H_1(x,y)$
- $K_2(x,y) = J_1(x,y) \circ H_2(x,y) + J_2(x,y)$
- $K_3(x,y) = J_1(x,y) \circ H_3(x,y) + J_3(x,y)$

Proof. $K_1(x,y) = (G \circ F)^{\ominus 1} = \sum_{i=1}^{\infty} \left(G^{\ominus i} \circ F\right)^{\ominus 1}$. By applying lemma 50 on most parts of this sum, I can conclude that this equals $\left(G^{\ominus 1} \circ F\right)^{\ominus 1}$. By applying lemma 51, this equals $G^{\ominus 1}$. Because $H_1(x,y) = I$, $G^{\ominus 1} = G^{\ominus 1} \circ H_1(x,y)$. By definition of J_1, $G^{\ominus 1} = J_1(x,y)$, so $G^{\ominus 1} \circ H_1(x,y) = J_1(x,y) \circ H_1(x,y)$, so $K_1(x,y) = J_1(x,y) \circ H_1(x,y)$, which is one of the things we want to prove.

$K_2(x,y) = (G \circ F)^{\ominus 2} = \sum_{i=1}^{\infty} \left(G^{\ominus i} \circ F\right)^{\ominus 1}$. By applying lemma 50 on most parts of the sum, I can conclude that $K_2(x,y)$ equals $\left(G^{\ominus 1} \circ F\right)^{\ominus 2} + \left(G^{\ominus 2} \circ F\right)^{\ominus 2}$. I now apply 51 on the right side of this sum. Throu this, $K_2(x,y) = \left(G^{\ominus 1} \circ F\right)^{\ominus 2} + G^{\ominus 2}$. I remark that by definition, $J_1(x,y) = G^{\ominus 1}$ and $J_2(x,y) = G^{\ominus 2}$. By substitution we get $K_2(x,y) = (J_1(x,y) \circ F)^{\ominus 2} + J_2(x,y)$. Because $J_1(x,y)$ is linear, $(J_1(x,y) \circ F)^{\ominus 2} = J_1(x,y) \circ F^{\ominus 2}$, so $K_2(x,y) = J_1(x,y) \circ F^{\ominus 2} + J_2(x,y) = J_1(x,y) \circ H_2(x,y) + J_2(x,y)$, which is one of the things we want to prove.

$K_3(x,y) = (G \circ F)^{\ominus 3} = \sum_{i=1}^{\infty} \left(G^{\ominus i} \circ F\right)^{\ominus 1}$. By applying lemma 50 on most parts of the sum, I can conclude that $K_3(x,y)$ equals $\left(G^{\ominus 1} \circ F\right)^{\ominus 3} + \left(G^{\ominus 2} \circ F\right)^{\ominus 3} + \left(G^{\ominus 3} \circ F\right)^{\ominus 3}$. I first apply lemma 51 to simplify the right part of this sum. Now I proved $K_3(x,y) = \left(G^{\ominus 1} \circ F\right)^{\ominus 3} + \left(G^{\ominus 2} \circ F\right)^{\ominus 3} + G^{\ominus 3}$. Because $G^{\ominus 1}$ is linear, $\left(G^{\ominus 1} \circ F\right)^{\ominus 3} = G^{\ominus 1} \circ F^{\ominus 3}$. I also apply lemma 52 on the middle part of this sum. This proves that $K_3(x,y) = G^{\ominus 1} \circ F^{\ominus 3} + \left\langle \begin{array}{c} b_{11} \\ c_{11} \end{array} \right\rangle \left(F_1^{\ominus 3} + F_2^{\ominus 3}\right) + G^{\ominus 3}$, where b_{11} and c_{11} are defined in lemma 52 and solely depend on $G^{\ominus 3}$.

Because of lemma 19, $G^{\ominus 2}$ doesn't have a term of odd degree and as a consequence, $b_{11} = c_{11} = 0$. This makes it possible to simplify $K_3(x,y)$ even further such that $K_3(x,y) = G^{\ominus 1} \circ F^{\ominus 3} + G^{\ominus 3}$. I can now rewrite it and conclude that $K_3(x,y) = J_1(x,y) \circ H_3(x,y) + J_3(x,y)$, which was the last thing left to prove. □

Theorem 54. *This proves that if $k = \mathbb{F}_2$ and $n = 2$, then $V_{\{2,3\}}$ is a vectorspace.*

Proof. Because of lemma 47, it is enough to prove that V is closed under addition. Addition is proved by lemma 49 because for every element in V, $V^{\ominus 1} = I$, and thus holds the following equality for the variables J_1 and H_1 as used in lemma 49: $J_1(x,y) = H_1(x,y) = I$. That lemma proves the addition, so it follows that V is a vectorspace. □

5.5 Conclusions

I will formulate some conclusions in this section. One important note is the following:

Remark 55. *Let F and G be polynomial maps over $\mathbb{F}_p$. If F, G are of lower degree i. Then $(F \circ G)^{\ominus i} = F^{\ominus i} + G^{\ominus i}$*

This means that the set of maps of lower degree i forms a vector space (see lemma 54). So My goal is to compute these vector space.

Lemma 56. *Let G be a tame mapping. Let G be of lower degree 2. Then $G^{\ominus 2}$ is an element of a vector space generated by $\left\{ \left\langle \begin{array}{c} y^2 \\ 0 \end{array} \right\rangle \right\}$ and its linear conjugations.*

Proof. G is a tame mapping, so it is possible to write G as composition of simple automorphisms: $G = G_i \circ \ldots \circ G_2 \circ G_1$. I prove this with induction to $\overline{G}_j$. If j is 0, then $\overline{G}_0^{\ominus 2} = 0$, so the lemma is o.k. for that. Now suppose the lemma is correct for $\overline{G}_j^{\ominus 2}$. Then it is also correct for $\left\langle \begin{array}{c} x + y^a \\ y \end{array} \right\rangle \circ \overline{G}_j$ if $a > 2$. Because the lineair transformations also are not relevant (because conjungation of something in the vector space with a lineair mapping results in somethings which is again in the vector space), the only case left to study is $\left\langle \begin{array}{c} x + \lambda \cdot y^2 \\ y \end{array} \right\rangle \circ \overline{G}_j$. But $\left(\left\langle \begin{array}{c} x + \lambda \cdot y^2 \\ y \end{array} \right\rangle \circ \overline{G}_j \right)^{\ominus 2} = \overline{G}_j^{\ominus 2} + \left\langle \begin{array}{c} \lambda \cdot y^2 \\ 0 \end{array} \right\rangle$, so it again is in the vector space. $\square$

Lemma 57. *For all $a_1, a_2, a_3, a_4 \in \mathbb{N}$, there exists a tame map F of lower degree $a_1 + a_3 - 1$ such that $F^{\ominus a_1 + a_3 - 1} = \left\langle \begin{array}{c} a_1 a_2 x^{a_3} y^{a_1 - 1} \\ -a_2 a_3 x^{a_3 - 1} y^{a_1} \end{array} \right\rangle$.*

Proof. Take the following composition:

$$\left\langle \begin{array}{c} x - a_2 \cdot y^{a_1} \\ y \end{array} \right\rangle \circ \left\langle \begin{array}{c} x \\ y - x^{a_3} \end{array} \right\rangle \circ \left\langle \begin{array}{c} x + a_2 \cdot y^{a_1} \\ y \end{array} \right\rangle \circ \left\langle \begin{array}{c} x \\ y + x^{a_3} \end{array} \right\rangle$$

$\square$

Lemma 58. $I + \left\langle \begin{array}{c} x^{p^2} \\ -y^{p^2} \end{array} \right\rangle$ *with higher order terms is also a tame automorphism.*

Proof. Take the following composition:

$$\left\langle \begin{array}{c} x - y^p \\ y \end{array} \right\rangle \circ \left\langle \begin{array}{c} x \\ y - x^p \end{array} \right\rangle \circ \left\langle \begin{array}{c} x + y^p \\ y \end{array} \right\rangle \circ \left\langle \begin{array}{c} x \\ y + x^p \end{array} \right\rangle$$

$\square$

5.6 Calculations

In this section, I will give some examples on how these compositions look like.

First, I consider to the following example:

$$G_{j+1} := \left\langle \begin{array}{c} x + y^2 \\ y \end{array} \right\rangle \circ G_j$$

Then the following is true:

$$
\begin{array}{lrcl}
1. & G_{j+1}^{\ominus 1} & = & G_j^{\ominus 1} \\
2. & G_{j+1}^{\ominus 2} & = & G_j^{\ominus 2} + \left\langle \begin{array}{c} \begin{pmatrix} 2 \\ 0 \end{pmatrix} \left(G_j^{\ominus 1}\right)_2^2 \\ 0 \end{array} \right\rangle \\
3. & G_{j+1}^{\ominus 3} & = & G_j^{\ominus 3} + \left\langle \begin{array}{c} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \left(G_j^{\ominus 1}\right)_2 \cdot \left(G_j^{\ominus 2}\right)_2 \\ 0 \end{array} \right\rangle \\
4. & G_{j+1}^{\ominus 4} & = & G_j^{\ominus 4} + \left\langle \begin{array}{c} \begin{pmatrix} 2 \\ 0 \end{pmatrix} \left(G_j^{\ominus 2}\right)_2^2 + \begin{pmatrix} 2 \\ 1 \end{pmatrix} \left(G_j^{\ominus 1}\right)_2 \cdot G_j^{\ominus 3} \\ 0 \end{array} \right\rangle \\
5. & G_{j+1}^{\ominus 5} & = & G_j^{\ominus 5} + \left\langle \begin{array}{c} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \left(G_j^{\ominus 1}\right)_2 \cdot \left(G_j^{\ominus 4}\right) + \begin{pmatrix} 2 \\ 1 \end{pmatrix} \left(G_j^{\ominus 2}\right)_2 \cdot \left(G_j^{\ominus 3}\right)_2 \\ 0 \end{array} \right\rangle
\end{array}
$$

Now I consider the following example.

$$G_{j+1} := \left\langle \begin{array}{c} x + y^3 \\ y \end{array} \right\rangle \circ G_j$$

Then the following is true:

$$
\begin{array}{lrcl}
1. & G_{j+1}^{\ominus 1} & = & \left(G_j^{\ominus 1}\right) \\
2. & G_{j+1}^{\ominus 2} & = & G_j^{\ominus 2} \\
3. & G_{j+1}^{\ominus 3} & = & G_j^{\ominus 3} + \left\langle \begin{array}{c} \begin{pmatrix} 3 \\ 0 \end{pmatrix} \left(G_j^{\ominus 1}\right)_2^3 \\ 0 \end{array} \right\rangle \\
4. & G_{j+1}^{\ominus 4} & = & G_j^{\ominus 4} + \left\langle \begin{array}{c} \begin{pmatrix} 3 \\ 1 \end{pmatrix} \left(G_j^{\ominus 1}\right)_2^2 \cdot \left(G_j^{\ominus 2}\right)_2 \\ 0 \end{array} \right\rangle \\
5. & G_{j+1}^{\ominus 5} & = & G_j^{\ominus 5} + \left\langle \begin{array}{c} \begin{pmatrix} 3 \\ 1 \end{pmatrix} \left(G_j^{\ominus 1}\right)_2 \cdot \left(G_j^{\ominus 2}\right)_2^2 + \begin{pmatrix} 3 \\ 1 \end{pmatrix} \left(G_j^{\ominus 1}\right)_2^2 \cdot \left(G_j^{\ominus 3}\right)_2 \\ 0 \end{array} \right\rangle
\end{array}
$$

Now I consider:

$$G_{j+1} := \left\langle \begin{array}{c} x + y^4 \\ y \end{array} \right\rangle \circ G_j$$

Then the following is true:

$$
\begin{array}{lrcl}
1. & G_{j+1}^{\ominus 1} & = & \left(G_j^{\ominus 1}\right) \\
2. & G_{j+1}^{\ominus 2} & = & G_j^{\ominus 2} \\
3. & G_{j+1}^{\ominus 3} & = & G_j^{\ominus 3} \\
4. & G_{j+1}^{\ominus 4} & = & G_j^{\ominus 4} + \left\langle \begin{array}{c} \begin{pmatrix} 4 \\ 0 \end{pmatrix} \left(G_j^{\ominus 1}\right)_2^4 \\ 0 \end{array} \right\rangle \\
5. & G_{j+1}^{\ominus 5} & = & G_j^{\ominus 5} + \left\langle \begin{array}{c} \begin{pmatrix} 4 \\ 1 \end{pmatrix} \left(G_j^{\ominus 1}\right)_2^4 \cdot \left(G_j^{\ominus 2}\right)_2 \\ 0 \end{array} \right\rangle
\end{array}
$$

And the last example:

$$G_{j+1} := \left\langle \begin{array}{c} x + y^5 \\ y \end{array} \right\rangle \circ G_j$$

Then the following is true:

$$\begin{array}{lrcl}
1. & G_{j+1}^{\ominus 1} & = & \left(G_j^{\ominus 1}\right) \\
2. & G_{j+1}^{\ominus 2} & = & G_j^{\ominus 2} \\
3. & G_{j+1}^{\ominus 3} & = & G_j^{\ominus 3} \\
4. & G_{j+1}^{\ominus 4} & = & G_j^{\ominus 4} \\
5. & G_{j+1}^{\ominus 5} & = & G_j^{\ominus 5} + \left\langle \begin{array}{c} \begin{pmatrix} 5 \\ 0 \end{pmatrix} \left(G_j^{\ominus 1}\right)_2^5 \\ 0 \end{array} \right\rangle
\end{array}$$

This is remark 39 written out. This gives a more clear view about what actually happens. So if you now want to know how to make a certain element, we have an idea how to do that. The formulas tell you what the last step must be. That way, it is possible to go back and find a suitable composition.

Bibliography

[1] Campbell, L. A., Essen, A van den (1995) Jacobian pairs, D-resultants, and automophisms of the plane, Journal of Pure and Applied Algebra 104, 9-18 (used in chapter 3)

[2] Essen, A. van den, Polynomial Automorphisms and the Jacobian Conjecture, Progress in Mathematics, Vol. 190, Birkhäuser 2000.