Universiteit Utrecht

Faculteit Bètawetenschappen

Drinfeld modules of rank two and Galois theory of some additive polynomials

Bachelor Thesis

Eva van Ammers

Mathematics

Supervisor:

Prof. Dr. Gunther Cornelissen
Mathematical Institute

January 18, 2018

Abstract

This thesis is about Galois theory of additive polynomials over the field of rational functions with coefficients from a finite field. When the characteristic of a field K is $p > 0$ the additive polynomials have the form $c_0x + c_1x^p + \ldots + c_nx^{p^n}$ with all $c_i \in K$. The roots of these polynomials are studied using Drinfeld modules, a certain kind of algebra homomorphisms that can be used to prove that the set of roots of an additive polynomial have a special kind of module structure. After providing some general theory, we will examine the Galois groups of two polynomials more closely, namely the Galois groups of $Tx + x^{q^2}$ and $Tx + Tx^q + x^{q^2}$ with q the number of elements in our finite field, and both of these polynomials in $\mathbb{F}_q(T)[x]$.

Contents

1 Introduction

We algebraists like to think about what we can achieve only using operations like addition, subtraction, multiplication, division and taking roots. One of the things that is possible is to determine the roots of a quadratic polynomial. The roots of $x^2 + bx + c$ are given by $\frac{-b \pm \sqrt{b^2-4c}}{2}$. As we can read in chapter 7 of [1], one of the first proofs of this formula was given around 830 by Musa al-Khowarizmi. Now [2] tells us that the formula for the roots of the cubic polynomial was found around 1535 by various people. Gerolamo Cardano published his method, together with the formula for the quartic polynomial, which one of his students, Lodovico Ferrari, found.
Around 1770 Joseph Louis Lagrange published a paper in which he analyzed the solutions of Cardano and Ferrari by considering them as permutations of roots. This method couldn't be generalized to higher degree polynomials. In 1799 Paolo Ruffini came with an imcomplete proof that the quintic polynomials don't have a general solution, and Niels Hendrik Abel published the complete proof in 1824. The key insight in this proof was to look at the permutation group of the roots.
It was still unclear why we can determine the roots of certain quintic polynomials, like $(x-1)^5$, and not of others. Évariste Galois came with the main insight what made some polynomials different. He showed that whether or not we could determine the roots of a certain polynomial is equivalent to whether or not the permutation group of the roots has a certain structure, namely whether the group is solvable.
Galois provided us with a new language to talk about the roots of a polynomial, namely via group theory. And although we now have an abstract correspondence, we may also be interested in finding the Galois group of certain polynomial. Or vice versa, we may have a group and then want to find a polynomial which has a Galois group equal to this group. Both questions are interesting to consider, and we will provide some answers to specific cases.

2 Preliminaries and definitions

We will assume the reader is familiar with linear algebra and abstract algebra, especially group theory, fields and galois theory. We will state some definitions and theorems that are related to the objects that we will study. Most of this section is inspired by the first chapter in [3].
In this thesis $\mathbb{F}_q$ will always denote a finite field with $q = p^f$ elements for some prime number p. We let $A := \mathbb{F}_q[T]$ denote the polynomial ring over $\mathbb{F}_q$. For some $f \in A$ we let $\deg(f)$ denote the degree of f. If we can write $f = a_0 + a_1T + \ldots + a_nT^n$ with all $a_i \in \mathbb{F}_q$ and $a_n \neq 0$, then $\deg(f) = n$. If we cannot write f in this way, we have $f = 0$ and we let $\deg(f) = -\infty$. We can see that for all $f, g \in A$ we have $\deg(fg) = \deg(f) + \deg(g)$. For $-\infty$ we use the convention that $-\infty + n = -\infty$ if n is finite or $-\infty$. We also have $\deg(f+g) \leq \max(\deg(f), \deg(g))$, because $\deg(f+g)$ can clearly not be bigger than $\max(\deg(f), \deg(g))$, but it can be very small, for example when $g = -f$.
A is a very nice ring to work with, because we know many things about it. Let us first state the properties that we want to prove.

Definition 2.1. A *Euclidean domain* R is a commutative domain with a Euclidean algorithm. If $N\colon R \to \mathbb{N} \cup \{-\infty\}$ is a function such that $N(fg) = N(f) + N(g)$ for all $f, g \in R$, then a Euclidean algorithm is an algorithm such that for every $f, g \in R$ with $g \neq 0$ we have that there exists unique $q, r \in A$ such that $f = qg + r$ and $N(r) < N(g)$.
A *principal ideal domain* is a domain for which every ideal is principal, which means that every ideal is generated by one element.
A *unique factorization domain* is a domain in which every element has a unique factorization into irreducible elements. An *irreducible element* is a $\pi \in A$ such that π is not a unit and if $\pi = ab$, then either a or b is a unit.

Proposition 2.2. *A is a Euclidean domain, and thus a principal ideal domain and a unique factorization domain.*

Proof. We first notice that deg indeed satisfies $\deg(fg) = \deg(f) + \deg(g)$. We will prove by induction on $\deg(f)$ that we can write $f = qg + r$ for all $g \neq 0$. If $\deg(f) < \deg(g)$, set $q = 0$ and $r = f$. If $\deg(f) \geq \deg(g) \geq 0$, we will first look at the case that $\deg(f) = 0$. Then $\deg(g) = 0$, and we set $q = fg^{-1}$ and $r = 0$, which we can do, because both $f, g \in \mathbb{F}_q \setminus \{0\}$, so this satisfies our condition.
Suppose $\deg(f) > 0$ and $\deg(f) \geq \deg(g)$. If we let $f = a_0 + a_1T + \ldots + a_nT^n$ and $g = b_0 + b_1T \ldots + b_mT^m$ with $a_n \neq 0$ and $b_n \neq 0$, then we know that for $f_1 := f - \frac{a_n}{b_n}T^{n-m}g$ it is the case that $\deg(f_1) < \deg(f)$, so we know by induction that there exist $q_1, r_1 \in A$ such that $f_1 = q_1g + r_1$ with $\deg(r_1) < \deg(g)$. If we set $q = q_1 + \frac{a_n}{b_n}T^{n-m}$ and $r_1 = r$, then we have $qg + r = (q_1 + \frac{a_n}{b_n}T^{n-m})g + r_1 = f_1 + \frac{a_n}{b_n}T^{n-m}g = f$, so this works.
To see that q and r are unique, write $f = qg + r = q'g + r'$. We see that $g \mid r - r'$, but since $\deg(r - r') \leq \max(\deg(r), \deg(-r')) < \deg(g)$, we see that $r - r' = 0$. We can subtract r from both sides, and since $g \neq 0$, we can divide by g and we get $q = q'$.
To prove that we have a principal ideal domain, we first notice that if we have an ideal I, then $m = \min_{i \in I \setminus \{0\}} \deg(i)$ exists, because deg is on $A \setminus \{0\}$ a function to the natural numbers. Let $i \in I$ be an element with $\deg(i) = m$. We claim $I = (i)$. Suppose $j \in I$ and $i \nmid j$. With the Euclidean algorithm we can write $j = qi + r$. We have $r \neq 0$, because $i \nmid j$. We also have $r = j - qi$, so $r \in I$. But $\deg(r) < \deg(i)$, and this a contradiction with $\deg(i) = m$, so we indeed have $I = (i)$.
To prove that we have a unique factorization domain, first notice that a factorization will always end in irreducible elements, because the degree of the elements in a factorization is always decreasing, and all elements of degree 0 are units. Suppose that we have two factorizations into irreducibles $P_1^{e_1} \ldots P_n^{e_n} = Q_1^{f_1} \ldots Q_m^{f_m}$ with all $e_i, f_j > 0$, and all the P_i, Q_j are different. If we have a factorization that isn't unique, this can be done, because we can remove the factors that appear on both sides. Now we know that $(P_1, Q_1), \ldots, (P_1, Q_m)$ are all principal ideals. Because the irreducibles are all different, these principal ideals should all be equal to 1. So then we have $(P_1, Q_1^{f_1} \ldots Q_m^{f_m}) = (1)$, but we clearly have $(P_1, Q_1^{f_1} \ldots Q_m^{f_m}) \subset (P_1)$, and this is a contradiction with the fact that P_1 is not a unit. □

If we have an $f \in A = \mathbb{F}_q[T]$, $f \neq 0$, we can look at quotient ring A/fA. The Euclidean algorithm can be used to determine the number of elements in this ring.

Proposition 2.3. *Suppose that $f \in A$ and $f \neq 0$, then A/fA is a finite ring with $q^{\deg(f)}$ elements.*

Proof. We can see that all elements in the set $\{r \mod f \colon r \in A, \deg(r) < \deg(f)\}$ are in A/fA. They are all different, because if we have r, r' such that $\deg(r) < \deg(f)$, $\deg(r') < \deg(f)$ and $f \mid r - r'$, then $\deg(r - r') \leq \max(\deg(r), \deg(r')) < \deg(f)$, so $r - r' = 0$. We can also see that these are all the representatives, because we can use the Euclidean algorithm to write a polynomial g as $qf + r$, and then r is the corresponding representative.
A polynomial with degree smaller than f has the form $a_0 + a_1 T + \ldots + a_{\deg(f)} T^{\deg(f)}$ (notice that $a_{\deg(f)}$ may be 0). We have q choices for all the a_i, so the number of polynomials is indeed equal to $q^{\deg(f)}$. □

We can use the proposition above to define the norm of a polynomial.

Definition 2.4. Let $f \in A$, then we define the *norm* of f as $|f| := q^{\deg(f)}$. Here we use the convention that $q^{-\infty} = 0$. If we want to specify our finite field, we write $|f|_{\mathbb{F}_q}$.

If $f \neq 0$, the norm is indeed defined as the the number of elements in A/fA. We can see that for all $f, g \in A$ we have that $|fg| = q^{\deg(fg)} = q^{\deg(f)+\deg(g)} = |f| \cdot |g|$. By expanding our definition to 0 as stated above, we can use this multiplication rule for any 2 polynomials.
Now we will look some more at the primes and units in A.

Proposition 2.5. *The primes in A are the irreducible polynomials.*

Proof. All irreducible polynomials are prime, because if we have an ideal such that $ab \in (P)$, then $ab = c \cdot P$, and because P is irreducible, we have that $P \mid a$ or $P \mid b$, so $a \in (P)$ or $b \in (P)$. All primes correspond to irreducible elements because we work in a principal ideal domain. □

Proposition 2.6. *The group of units in A is equal to $\mathbb{F}_q^*$, and this is a cyclic group with $q - 1$ elements.*

Proof. If we have $v \cdot u = 1$, then it is clearly the case that $v \neq 0$ and $u \neq 0$. We also have that $\deg(v) \cdot \deg(u) = \deg(1) = 0$, so $\deg(v) + \deg(u) = 0$. Since v, u are both not equal to 0, we have that $\deg(v) \geq 0$ and $\deg(u) \geq 0$, so both u, v have degree 0, and thus are in $\mathbb{F}_q \setminus \{0\} = \mathbb{F}_q^*$. $\mathbb{F}_q$ is field, so all elements except 0 are units, so the number of elements in A is indeed equal to $q - 1$.
If our group isn't cyclic, we know by Lagrange that there exists a $n \mid q - 1$, $n \neq q - 1$ with $v^n = 1$ for all $v \in \mathbb{F}_q^*$. Let n be the smallest number such that $v^n = 1$. We see that the number of roots of $x^n - 1$ over $\mathbb{F}_q$ is at most equal to n, because this is a polynomial in A and this give unique factorization, so $n \geq q - 1$. But with $n \mid q - 1$ and $n \neq q - 1$ we know that $n < q - 1$, so we have a contradiction, and our group is indeed cyclic. □

By the two propositions above we see that we can write any $f \in A \setminus \{0\}$ as $f = \alpha P_1^{e_1} \ldots P_t^{e_t}$ with all P_i monic irreducibles and $\alpha \in \mathbb{F}_q^*$. We can also assume $P_i \neq P_j$ if $i \neq j$, which we can use to state our next proposition, namely the Chinese Remainder Theorem. The CRT may be a familiar theorem from modular arithmetic, where it states that that the value of a certain integer mod ab can be uniquely determined from its values mod a and mod b if $\gcd(a, b) = 1$.

Proposition 2.7. *Let $m_1, m_2, \ldots, m_t$ be pairwise relatively prime elements of A, and let $m = m_1 m_2 \ldots m_t$, and ϕ_i be the natural homomorphism from A/mA to $A/m_i A$ that reduces some element from A/mA modulo $m_i A$. Then the map $\phi \colon A/mA \to A/m_1 A \oplus A/m_2 A \oplus \ldots \oplus A/m_t A$ given by*

$$\phi(a) = (\phi_1(a), \phi_2(a), \ldots, \phi_t(a))$$

is a ring isomorphism.

Proof. The map ϕ is clearly well-defined and a ring homomorphism. We saw when we defined our norm that $|m| = |m_1| \cdot \ldots \cdot |m_t|$, so the number of elements in both rings is equal. We will prove that ϕ is injective, and since the number of elements is the same, bijectivity follows from injectivity. Because we have a ring homomorphism, we only have to prove that the kernel is trivial. Suppose that $(\phi_1(a), \phi_2(a), \ldots, \phi_t(a)) = (0, 0, \ldots, 0)$. Then we know that $a \in m_i A$ for all $1 \leq i \leq t$. Because $m_1, m_2, \ldots, m_t$ are pairwise relatively prime, we know that $a \in m_1 m_2 \ldots m_t A$, so $a \in mA$, so $a = 0$ in A/mA, so our kernel is indeed trivial. □

Corollary 2.8. *Let $m, m_1, \ldots, m_t$ be defined as above. Then the map ϕ restricted to the units of A gives rise to a group isomorphism*

$$(A/mA)^* \cong (A/m_1A)^* \times (A/m_2A)^* \times \ldots \times (A/m_tA)^*.$$

Proof. Because our map ϕ is a ring isomorphism, it sends units to units, preserves multiplication, and does this in a bijective way, so we indeed have a group isomorphism. □

We can use the corollary to determine the number of elements in a group $(A/mA)^*$ by only looking at the groups of the form $(A/P^eA)^*$ with P prime. But to do that, we first need some lemma's.

Lemma 2.9 (Freshman's dream)**.** *Let R be a ring for which it is the case that $p \cdot r = 0 = r \cdot p$ for all $r \in R$ for a prime number p. Let $a_1, a_2, \ldots, a_n \in R$ be pairwise commuting elements. Then $(a_1 + a_2 + \ldots + a_n)^q = a_1^q + a_2^q + \ldots a_n^q$ where $q = p^f$.*

Proof. We first look at $f = 1$. We can expand $(a_1 + a_2 + \ldots a_n)^p$ using Newton's binomial theorem. Then we have

$$(a_1 + a_2 + \ldots a_n)^p = \sum_{0 \le e_1, \ldots, e_n \le p, e_1 + \ldots e_n = p} \frac{p!}{e_1! \ldots e_n!} a_1^{e_1} \cdots a_n^{e_n}.$$

Suppose that we have a term in which there are two e_j, e_k with $e_j \neq 0$ and $e_k \neq 0$. Then all $e_i < p$, since they sum up to p. So $p \nmid e_i!$ for all $1 \le i \le n$, because p is prime. But $p \mid p!$, so $p \mid \frac{p!}{e_1! \ldots e_n!}$, and this term vanishes. We cannot have all our e_i equal to 0, so suppose that we have one $e_i \neq 0$. Then we have $e_i = p$, so we have $\frac{p!}{e_1! \ldots e_n!} = \frac{p!}{0! \cdots 0! p! 0! \cdots 0!} = 1$, so we indeed have that there is only one term, and this term is of the form a_i^p. We can do this for all a_i, so we see that our Freshman's dream is true for $f = 1$.
In general, we have that if $(a_1 + a_2 + \ldots a_n)^{p^f} = a_1^{p^f} + a_2^{p^f} + \ldots a_n^{p^f}$, then

$$\begin{aligned}(a_1 + a_2 + \ldots a_n)^{p^{f+1}} &= ((a_1 + a_2 + \ldots a_n)^{p^f})^p \\ &= (a_1^{p^f} + a_2^{p^f} + \ldots a_n^{p^f})^p \\ &= a_1^{p^f \cdot p} + a_2^{p^f \cdot p} + \ldots a_n^{p^f \cdot p} \\ &= a_1^{p^{f+1}} + a_2^{p^{f+1}} + \ldots a_n^{p^{f+1}}\end{aligned}$$

So we can prove our theorem for all f by induction. □

Now we can go back to $(A/P^eA)^*$. We will first look at $e = 1$.

Lemma 2.10. *The number of units in A/PA is equal to $|P| - 1$.*

Proof. The number of elements in A/PA is equal to $|P|$, so this lemma says that everything is a unit, except 0. In a principal ideal domain all prime ideals are maximal, so (P) is a maximal ideal, so A/PA is field, and in a field is every element a unit, except 0. □

We see that A/PA is a field with q^d with $d = \deg(P)$ elements. For such field we have a lemma.

Lemma 2.11. *Let $a \in \mathbb{F}_{q^d}$. Then $a^{q^d} = a$.*

Proof. If $a = 0$ we have $0^{q^d} = 0$. If $a \neq 0$, then $a \in \mathbb{F}_{q^d}^*$ and because $|\mathbb{F}_q^*| = q^d - 1$, we have $a^{q^d - 1} = 1$, so $a^{q^d} = a$. □

Proposition 2.12. *The number of elements in $(A/P^eA)^*$ is equal to $|P|^e - |P|^{e-1}$.*

Proof. For $e = 1$ we see that this is true by lemma 2.10. Suppose $e > 1$. First we claim that all elements in (A/P^eA) have unique representants of the form $a_0 + a_1P + \ldots + a_{e-1}P^{e-1} \mod P^e$ with all $a_i \in A/PA$. If we have a polynomial f_1 with $\deg(f_1) < \deg(P^e)$, we can by the Euclidean algorithm find an a_{e-1} such that $f_1 = a_{e-1}P^{e-1} + f_2$ with $\deg(f_2) < \deg(P^{e-1})$. Since $\deg(f_1) < \deg(P^e)$, we have that $\deg(a_{e-1}) < \deg(P)$, so $a_{e-1} \in A/PA$. We can repeat this, and in this way find our coefficients $a_0, a_1, \ldots a_{e-1}$. There are $|P|^e$ elements of this form, and that is exactly the number of elements in A/P^eA. We also see that all these elements of this form are unique, so these are all the elements in A/P^eA.
Let s such that $p^s \geq e$. Suppose $a_0 = 0$, then by the freshman's dream we have $(a_1P + \ldots + a_{e-1}P^{e-1})^{p^s} = a_1^{p^s}P^{p^s} + \ldots + a_{e-1}^{p^s}P^{(e-1)p^s}$. Since all powers of P in this expression are greater than e, we have that $a_1^{p^s}P^{p^s} + \ldots + a_{e-1}^{p^s}P^{(e-1)p^s} \equiv 0 \mod P^e$, and since this element is nilpotent, it cannot be a unit.
Suppose that $a_0 \neq 0$. We have that $|P|^e = p^{e\cdot\deg(P)\cdot f}$, and $e \cdot \deg(P) \cdot f \geq e$, so if we raise $a_0 + a_1P + \ldots + a_{e-1}P^{e-1}$ to the $|P|^e$th power, we get that all terms P^i with $i \geq 1$ vanish mod P^e. We have that $a_0^{|P|} \equiv a_0$, because $a_0 \in A/PA$ and lemma 2.11. So we also have $a_0^{|P|^e} \equiv a_0^{|P|^{e-1}} \equiv \ldots \equiv a_0 \mod P^e$. Now we only need to raise our element to the $|P| - 1$ power, and since all terms except a_0 have already vanished, we only need to look what happens to a_0. For a_0 we have $a_0^{|P|-1} \equiv 1$, because $a_0 \in (A/PA)^*$, so we have that raising our element $a_0 + a_1P + \ldots + a_{e-1}P^{e-1}$ to the $|P|^e - |P|^{e-1}$th power makes it equal to 1, so it is a unit.
The number of elements with $a_0 = 0$ is equal to $|P|^{e-1}$, since we have $|P|$ choices for the coefficients a_i with $1 \leq i \leq e-1$. So the number of units is indeed equal to $|P|^e - |P|^{e-1}$. □

From now on let $k = \mathbb{F}_q(T)$. We will look at $A[x]$ and $k[x]$, and state some lemma's and theorems related to polynomials over A, fields and field extensions. Most are from [1].

Proposition 2.13. *Let K be a field. We write n for adding 1 exactly n times to itself. If $n \neq 0$ for all positive integers n, then K contains an (isomorphic) copy of $\mathbb{Q}$. If $n = 0$ for some integer n, then $p = 0$ for some prime p with $p \mid n$, and K contains an (isomorphic) copy of $\mathbb{Z}/p\mathbb{Z}$.*

Proof. Because $1 \in K$, there is exactly one ring homomorphism $f\colon \mathbb{Z} \to K$. If $\ker(f) = 0$, we have $\mathbb{Z} \hookrightarrow K$, so $n \neq 0$ for all $n \in \mathbb{Z}$ and since K is a field, it should contain the quotient field of $\mathbb{Z}$, so $\mathbb{Q} \hookrightarrow K$. If $n = 0$ for some integer n, we know $\ker(f) \neq 0$ and $f(\mathbb{Z}) \cong \mathbb{Z}/\ker(f)$. Since f is a ring homomorphism, and $\mathbb{Z}$ is an integral domain, $f(\mathbb{Z})$ is an integral domain. So $\ker(f)$ should be a prime ideal, so $\ker(f) = (p)$ for some prime p. Then we know that we have $p = 0$ in K and $\mathbb{Z}/p\mathbb{Z} \cong f(\mathbb{Z}) \hookrightarrow K$. □

We will use this proposition to define the characteristic:

Definition 2.14. The *characteristic* of a field K is 0 if $\mathbb{Q} \hookrightarrow K$, and p if $\mathbb{Z}/p\mathbb{Z} \hookrightarrow K$.

We can see that $k = \mathbb{F}_q(T)$ has characteristic p.
Now we will take a look at polynomials over A and k.

Definition 2.15. Let $x_1, \ldots, x_n \in A$ with factorizations $x_i = \alpha_i P_1^{a_{1,i}} P_2^{a_{2,i}} \ldots P_k^{a_{k,i}}$ with α_i a unit and P_j monic and irreducible, and let $b_j = \max(a_{j,1}, a_{j,2}, \ldots, a_{j,n})$. We define the *greatest common divisor* as $\gcd(x_1, \ldots, x_n) := P_1^{b_1} P_2^{b_2} \ldots P_k^{b_k}$.
A primitive polynomials is a polynomial $f(x) \in A[x]$ such that the gcd of the coefficients is equal to 1.

Lemma 2.16 (Gauss)**.** *Let $g(x), h(x) \in A[x]$ be primitive polynomials. Then $f(x) = g(x)h(x)$ is also primitive.*

Proof. We write $f(x) = a_0 + a_1x + \ldots a_{n+m}x^{n+m}$, $g(x) = b_0 + b_1x + \ldots + b_mx^m$ and $h(x) = c_0 + c_1x + \ldots c_nx^n$. Let P be some prime element in A, and let b_s, c_t be the coefficients with s, t maximal such that $P \nmid b_s$, $P \nmid c_t$. This coefficients exist because g, h are primitive. We write $a_{s+t} = b_0c_{s+t} + \ldots + b_{s-1}c_{t+1} + b_sc_t + b_{s+1}c_{t-1} + \ldots + b_{s+t}c_0$ where we take $b_i = 0$ if $i > m$ and $c_j = 0$ if $j > n$. In this sum every term except b_sc_t is divisible by P, because in $b_{s+1}c_{t-1} + \ldots + b_{s+t}c_0$ every b_i is divisible by P, because we chose our coefficients in this way, and in $b_0c_{s+t} + \ldots + b_{s-1}c_{t+1}$ every c_j is divisible by P. But $P \nmid b_sc_t$, so $P \nmid a_{s+t}$.
So for every prime element we can find a coefficient of $f(x)$ that isn't divisible by this element, thus $f(x)$ is primitive. □

Theorem 2.17. *A primitive polynomial $f \in A[x]$ is irreducible in $A[x]$ if and only if it is irreducible in $k[x]$.*

Proof. We will prove that f is reducible in $A[x]$ if and only if it is reducible in $k[x]$. This implication from left to right is trivial. Now suppose f is reducible in $k[x]$. We write $f(x) = c \cdot g(x)h(x)$ with $c \in k$ and g, h primitive polynomials. This can be done, because we can first multiply $g(x), h(x)$ with enough primes to make them polynomials in $A[x]$. If the coefficients have a gcd unequal to 1, then we can divide the gcd out of all coefficients, and we are left with a primitive polynomial.
Now we know that $g(x)h(x)$ is primitive, and since f is also primitive, both c and $\frac{1}{c}$ cannot be divisible by primes, so c is a unit in A, so $cg(x) \cdot h(x)$ is a factorization in $A[x]$. □

This theorem, combined with the following theorem, will be quite useful when we want to determine whether a polynomial is irreducible.

Proposition 2.18 (Eisenstein)**.** *Let $f(x) = a_0 + a_1x + \ldots + a_\ell x^\ell$ be a polynomial in $A[x]$ such that for a prime P we have that $P \nmid a_\ell$, $P \mid a_i$ for $0 \leq i \leq \ell - 1$, and $P^2 \nmid a_0$. Then $f(x)$ is irreducible over $k[x]$.*

Proof. Because we prove irreducibility over $k[x]$, we can without loss of generality assume that $f \in A[x]$ and f is a primitive polynomial. Note that is then enough to prove that $f(x)$ is irreducible over $A[x]$. Let $f(x) = g(x)h(x)$ with $g(x), h(x) \in A[x]$. Note that both $g(x), h(x)$ are primitive, otherwise f wouldn't be primitive. We write $f(x) = a_0+a_1x+\ldots a_{n+m}x^{n+m}$, $g(x) = b_0+b_1x+\ldots+b_mx^m$ and $h(x) = c_0+c_1x+\ldots c_nx^n$. Since $a_0 = b_0c_0$ and $P^2 \nmid a_0$, we have that $P \nmid b_0$ or $P \nmid c_0$. Without loss of generality we assume $P \nmid b_0$. Let c_i be the term with i minimal such that $P \nmid c_i$. This c_i exists, because h is primitive. We then have $a_i = b_0c_i + b_1c_{i-1} + \ldots + b_ic_0$. We have $P \mid b_1c_{i-1} + \ldots + b_ic_0$ because $P \mid c_0, \ldots, P \mid c_{i-1}$. But $P \nmid b_0c_1$, so $P \nmid a_i$. But the only coefficient that isn't divisible by P is a_{n+m}, so $i = n + m$. So either g or h has a degree equal to that of f, and the other is a constant, so we indeed have that f is irreducible. □

Proposition 2.19 (reverse Eisenstein)**.** *Let $f(x) = a_0 + a_1x + \ldots + a_\ell x^\ell$ be a polynomial in $A[x]$ such that for a prime P we have that $P \nmid a_0$, $P \mid a_i$ for $1 \leq i \leq \ell$, and $P^2 \nmid a_\ell$. Then $f(x)$ is irreducible over $k[x]$.*

Proof. Repeat the same proof as above, but take the indices around a_ℓ if the above prove looks around a_0 and vice versa and replace i minimal by i maximal. □

Finally we will state some lemma's and proposition related to field extensions and Galois theory. Recall that a field extension L/K has a Galois group $\mathrm{Gal}(L/K)$, which is the group of all automorphisms of L that leave K fixed. If f is some irreducible polynomial over K then adding a root of f to K can be seen as looking at $K[x]/(f)$, and because f is irreducible and $K[x]$ is a principal ideal domain, (f) is maximal, and $K[x]/(f)$ is indeed a field. We can see that $x \mod f \in K[x]/(f)$ and $f(x \mod f) \equiv f(x) \equiv 0 \mod (f)$, so $K[x]/(f)$ indeed contains a zero of f.
If $L = K(\alpha_1, \ldots, \alpha_n)$ where all α_i are the roots of irreducible polynomials over K, then an element σ of the Galois group is a field automorphism that leaves K invariant. If we know where σ maps all the α_i, we also know where all possible products, sums, quotients, et cetera, map to, because σ is a field automorphism. So the Galois group can be determined by only looking at the images of the α_i.
We can see that if $\sigma \in \mathrm{Gal}(L/K)$ and f_i is the minimal polynomial of α_i with $f_i = a_0 + a_1x + \ldots + a_nx^n$ and $a_j \in K$ for all $0 \leq j \leq n$, then we have the following because σ is a field automorphism

$$\begin{aligned} f_i(\sigma(x)) &= a_0 + a_1\sigma(x) + \ldots + a_n\sigma(x)^n \\ &= a_0 + a_1\sigma(x) + \ldots + a_n\sigma(x^n) \\ &= \sigma(a_0) + \sigma(a_1x) + \ldots + \sigma(a_nx^n) \\ &= \sigma(a_0 + a_1x + \ldots + a_nx^n) \\ &= \sigma(f_i(x)). \end{aligned}$$

So we also have $0 = \sigma(0) = \sigma(f_i(\alpha_i)) = f_i(\sigma(\alpha_i))$. Because f_i is irreducible, we can see that σ only sends α_i to other roots of the minimal polynomials of α_i.

Definition 2.20. A *Galois extension* is an algebraic, normal, separable extension L/K. An element in L is *algebraic* over K if it is the root of some polynomial with coefficients in K. An extension is algebraic if every element in L is algebraic. An extension is called *normal* if for all $\alpha \in L$, then for all β where α, β satisfy the same irreducible polynomial we have $\beta \in L$. An extension is called *separable* if for every irreducible polynomial which has roots in L, all the roots of this polynomial are distinct.

Definition 2.21. Let $K \subset L \subset M$ be a tower of field extensions. Then the *degree* $[L\colon K]$ denotes the dimension of L over K as a K-vectorspace.

We see that $[L\colon K] \geq 1$, because $1 \in L$. We also see that if $[L\colon K] = 1$, then $L = K$, because if $x \in L \setminus K$, then $1, x$ are K-linearly independent.

Lemma 2.22. *Let $K \subset L \subset M$ be a tower of field extensions. Suppose $[L\colon K], [M\colon L] < \infty$. Then $[M\colon K]$ is finite en $[M\colon K] = [M\colon L][L\colon K]$.*

Proof. Suppose $e_1, \ldots, e_m$ is a basis for L/K and $f_1, \ldots, f_n$ is a basis for M/L. We claim that $\{e_i f_j \colon 1 \leq i \leq m, 1 \leq j \leq n\}$ forms a basis for M/K. Note that these are indeed elements in M. If we have some element $x \in M$, we can write $x = x_1 f_1 + \ldots + x_n f_n$ with $x_j \in L$ for all $1 \leq j \leq n$.
Because $e_1, \ldots, e_m$ is basis and $f_j \in L$ for all $1 \leq j \leq n$, we can write $x_j = x_{1,j} e_1 + \ldots + x_{m,j} e_m$ with $x_{i,j} \in K$ for all i, j. So we can write $x = \sum_{i=1}^{m} \sum_{j=1}^{n} x_{i,j} e_i f_j$ with $x_{i,j} \in K$, so all $e_i f_j$ indeed form a spanning set.
Now suppose $\sum_{i=1}^{m} \sum_{j=1}^{n} a_{i,j} e_i f_j = 0$. The f_j now have coefficients from L, because $a_{i,j} \in K$ and $e_i \in L$, and since they form a basis, we have $\sum_{i=1}^{m} a_{i,j} e_i f_j = 0$ for all $1 \leq j \leq n$. Elements in a basis are non-zero, so we also have $\sum_{i=1}^{m} a_{i,j} e_i = 0$. Since $a_{i,j} \in K$, and the e_i are independent, we conclude $a_{i,j} = 0$ for all i, j, so our set is independent.
The number of elements of the form $e_i f_j$ is clearly equal to $mn = [M\colon K]$, and $[M\colon L][L\colon K] = nm = [M\colon K]$, and we indeed have $[M\colon K] < \infty$. □

The degree now has an abstract meaning, but for a simple extension it is indeed equal to the degree of a polynomial.

Proposition 2.23. *Let α be an algebraic element over K and f its minimal polynomial. Then $[K(\alpha)\colon K] = \deg(f)$.*

Proof. We know that $K(\alpha) \cong K[x]/(f(x))$ as fields, and in $K[x]$ we see that $1 \mod f(x), \ldots, x^{\deg(f)-1} \mod f(x)$ form a K-basis. A field isomorphism especially induces an isomorphism of the vector space structure of $K(\alpha)/K$, so $K(\alpha)$ also has a K-basis with n elements. □

So when we add one root to a field, we can determine the degree of the extension. If we know that the degree of a field extension is finite, we know something stronger.

Lemma 2.24. *Let L/K be a field extension such that $[L\colon K] = n < \infty$. Then L/K is an algebraic extension.*

Proof. Let $\alpha \in L$. Because $[L\colon K] = n$, we know that $1, \alpha, \ldots, \alpha^n$ are linearly dependent over K. So there exist $a_0, \ldots, a_n \in K$ such that $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$, and since α was arbitrary, every element in L is algebraic over K. □

We can use algebraic field extension to say something about algebraic elements.

Proposition 2.25. *Suppose α, β are algebraic over a field K. Then $\alpha + \beta$, $\alpha \cdot \beta$ and $-\alpha$ are also algebraic. If $\beta \neq 0$, then $\frac{\alpha}{\beta}$ is algebraic.*

Proof. We know that $\alpha + \beta, \alpha \cdot \beta, -\alpha, \frac{\alpha}{\beta} \in K(\alpha, \beta)$. We also see that if $p_\beta(x)$ is the minimal polynomial of β over K, then β is also a root $p_\beta(x)$ in $K(\alpha)$, so β is algebraic over $K(\alpha)$, so $[K(\alpha, \beta)\colon K(\alpha)] < \infty$. Because α is algebraic, we have $[K(\alpha)\colon K] < \infty$, so $[K(\alpha, \beta)\colon K] = [K(\alpha, \beta)\colon K(\alpha)][K(\alpha)\colon K] < \infty$. We have that $K(\alpha, \beta)$ is an algebraic extension, and thus all these elements are indeed algebraic. □

The degree is also useful to say something about the number of elements in the Galois group.

Proposition 2.26. *Let K be a field and L/K a finite extension. Then $|Gal(L/K)| \leq [L\colon K]$. Moreover, if $|Gal(L/K)| = [L\colon K]$, then L/K is a Galois extension.*

Proof. Let $n = [L\colon K]$. We prove this with induction to n. For $n = 1$ we have that $L = K$, so $\mathrm{Gal}(L/K)$ is trivial, and contains one element, so then the proposition is true. Suppose we have proved the proposition for $1 \leq n \leq m$ for some m. If $[L\colon K] = m+1$, let $\alpha \in L \setminus K$ with minimal polynomial f_1. Then $[K(\alpha)\colon K] > 1$, so $[L\colon K(\alpha)] < m+1$. We see that $\mathrm{Gal}(L/K(\alpha))$ is a subgroup of $\mathrm{Gal}(L/K)$. Let $H = \mathrm{Gal}(L/K(\alpha))$ and $G = \mathrm{Gal}(L/K)$. We consider the right coset decomposition $G = \sum_{i=1}^{r} g_i H$ with $g_i H \cap g_j H = \{e\}$ if $i \neq j$. We see that all $g_i(\alpha)$ are roots of f_1, because field automorphism only send roots to other roots of its minimal polynomial. If $g_i(\alpha) = g_j(\alpha)$, then $g_i g_j^{-1}(\alpha) = \alpha$, so $g_i g_j^{-1} \in H$, but this cannot be the case, so all $g_i(\alpha)$ are distinct. There are at most $\deg(f_1)$ distinct roots of f_1 in L, so we have $r \leq \deg(f_1)$, so we get

$$|\mathrm{Gal}(L/K)| = r|H| \leq \deg(f_1)|H| \leq [K(\alpha)\colon K][L\colon K(\alpha)] = [L\colon K]$$

We used the induction hypothesis on H with $[L\colon K(\alpha)]$. We see that $|\mathrm{Gal}(L/K)| = [L\colon K]$ if $r = d$, and since α was chosen arbitrarily, we see that f_1 has precisely $\deg(f_1)$ zeroes.
We already showed that a finite extension is algebraic. The only way an extension can contain precisely $\deg(f_1)$ distinct roots, is if all roots of f_1 are distinct and we added all these roots, so our extension is indeed separable and normal, so it is a Galois extension. □

Lemma 2.27. *Let $p(x)$ be an irreducible polynomial over a field K and let L be the splitting field of $p(x)$ over K. Then the number of elements in the Galois group greater or equal to* $\deg(p)$.

Proof. Let α be a root of $p(x)$ over K. We know by lemma 2.22 that $[L\colon K] = [L\colon K(\alpha)][K(\alpha)\colon K] = [L\colon K(\alpha)]\deg(p)$. The degree of an extension is always at least 1, so $[L\colon K(\alpha)] \geq 1$ and $[L\colon K] \geq \deg(p)$. We know that the number of elements in the Galois group of a splitting field is equal to the degree of the total extension, so the number of elements in the Galois group is indeed greater or equal to $\deg(p)$. □

3 Additive polynomials and Drinfeld modules

3.1 Additive polynomials

We let K denote a field. In this subsection we will look at a special class of polynomials in $K[x]$, namely the additive polynomials. Much of the theory in this and the other subsection originates from chapter 12 from [3].

Definition 3.1. A polynomial $f \in K[x]$ is called *additive* if, when we look at the polynomial ring in two variables $K[x, y]$, we have $f(x + y) = f(x) + f(y)$.

We can easily see that f is an additive polynomial, then $a \cdot f$ with $a \in K$ is also additive, and if f, g are additive polynomials, then $f + g$ is also an additive polynomial. We also have that $f(g(x + y)) = f(g(x) + g(y)) = f(g(x)) + f(g(y))$, so the composition of 2 additive polynomials is additive. We can see that $f(g + h)(x) = f(g(x) + h(x)) = f(g(x)) + f(h(x))$, so composition is distributive over addition and we even have a ring of additive polynomials.
If the composition of two functions if additive, we do not always know that one of the functions is additive, but we do know this with an additional requirement.

Lemma 3.2. *If $f, g \in k[x]$ are polynomials, $f, f \circ g$ are additive and f is injective, then g is additive.*

Proof. Because f is injective, f has a left inverse as a function, and we can use the additivity of f and the fact that $f^{-1}(f(x)) = x$ to get the following:

$$\begin{aligned} f^{-1}(f(x) + f(y)) &= f^{-1}(f(x + y)) \\ &= x + y \\ &= f^{-1}(f(x)) + f^{-1}(f(y)) \end{aligned}$$

So our function f^{-1} is additive on f. We can use this together with the fact that $f \circ g$ is additive:

$$\begin{aligned} g(x+y) &= f^{-1}(f(g(x+y))) \\ &= f^{-1}(f(g(x)) + f(g(y))) \\ &= f^{-1}(f(g(x))) + f^{-1}(f(g(y))) \\ &= g(x) + g(y) \end{aligned}$$

So g is also additive and we are done. □

Lemma 3.3. *The function $f \in k[x]$ with $f(x) = x^p$ is injective if K has characteristic $p > 0$.*

Proof. Let $a, b \in k$ be 2 elements such that $a^p = b^p$. Then $a^p - b^p = 0$. We can use the freshman's dream to get $(a-b)^p = 0$. We work in a field, so if the product of a number of things is 0, at least one of the factors is 0. All factors are $a - b$, so $a - b = 0$, so $a = b$, so our function is injective. □

After this lemma, we still need one definition:

Definition 3.4. Let $f = a_0 + a_1 x + \ldots + a_n x^n$ be a polynomial. The *formal derivative* with respect to x is $a_1 + 2a_2 x + \ldots + n a_n x^{n-1}$.

This formal derivative looks quite familiar from analysis, and many familiar theorems, like the product rule, quotient rule and chain rule can be proved by just writing out coefficients using the definition. Another theorem about the formal derivative that we will use, is that if a polynomial has a double root, then this root is also a root of the derivative. This follows from the product rule.
We will use the formal derivative to identify all additive polynomials in $K[x]$.

Proposition 3.5. *Let K be a field and $f(x) \in K[x]$ an additive polynomial. If the characteristic of K is zero, then $f(x) = ax$ for some $a \in K$. If the characteristic of K is p, then there are elements $a_i \in K$ with $0 \leq i \leq r$ such that $f(x) = a_0 x + a_1 x^p + \ldots + a_r x^{p^r}$.*

Proof. First notice that ax is always additive, and that $a_0 x + a_1 x^p + \ldots + a_r x^{p^r}$ is additive because of the freshman's dream. Because f is additive, we have $f(x+y) = f(x) + f(y)$. We can take the formal derivative with respect to x, and we get $\frac{d}{dx} f(x+y) = \frac{d}{dx} f(x)$, because $f(y)$ is constant in x. If we evaluate the formal derivative in $x = 0$, we see that $\frac{d}{dx} f(x) \mid_{x=0}$ is a constant (in both x and y). If $f(x+y) = b_0 + b_1(x+y) + \ldots + b_n(x+y)^n$, then $\frac{d}{dx} f(x+y) = b_1 + 2b_2(x+y) + \ldots + n b_n (x+y)^{n-1}$. If we fill in $x = 0$ we get that $b_1 + 2b_2 y + \ldots + n b_n y^{n-1}$ is constant.
If the characteristic is 0, then we have $0 = b_2 = b_3 = \ldots = b_n$, so have $f(x) = b_0 + b_1 x$. We have $b_0 = f(0) = f(0+0) = f(0) + f(0) = 2b_0$, so $b_0 = 0$, so $f(x) = b_1 x$.
If the characteristic is p, then we have that if $p \mid n$, then $n b_n y^{n-1} = 0$, but if $p \nmid n$ and $b_n \neq 0$, then $n b_n y^{n-1} \neq 0$, so have that the only coefficients that possibly aren't 0 are the b_n with $p \mid n$. So we can write

$$f(x) = b_1 x + \sum_{j=1}^{m} b_{pj} x^{pj} = b_1 x + g(x)^p$$

Here $g(x)$ is a polynomial with coefficients in K_1, where K_1 is the field to which we added all the pth roots of our coefficients. Notice that we used the freshman's dream in the last equality.
Be cause of lemma 3.3 we know that x^p is injective, and together with lemma 3.2, we know that if $g(x)^p$ is additive, then $g(x)$ is additive. So with induction to the degree of f we can assume $g(x) = \sum_{h=0}^{r-1} c_h x^{p^h}$, so

$$f(x) = b_1 x + \sum_{h=0}^{r-1} c_h^p x^{p^{h+1}}$$

We know that $c_h^p \in K$, because $c_h \in K_1$, and we only attached pth roots to K to form K_1, and the sum or the product of two pth roots again gives something in K when we raise it to the pth power, because of the freshman's dream and commutativity. So we are done. □

If we want to do Galois theory with additive polynomial, characteristic 0 isn't that interesting, so from now one we will assume that our characteristic is positive.

3.2 Roots of additive polynomials and Drinfeld modules

Now that we are more familiar with additive polynomials, we will start to look at a certain subset of the additive polynomials. But first we need the definition of an algebra.

Definition 3.6. Let K be a field. A is an *K-algebra* if A is an K-vector space, and A has some map from $A \times A$ to A, called multiplication, that is left en right distributive over addition, and has compatible multiplication with scalars, which means that for all $a, b \in K$, $x, y \in A$ we have $(ax) \cdot (by) = ab(x \cdot y)$. An *algebra homomorphism* f is a map that is K-linear and $f(x \cdot y) = f(x) \cdot f(y)$ for all $x, y \in A$.

Fix a finite field $\mathbb{F}_q$, and let $k = \mathbb{F}_q(T)$. Then a certain subset of the additive polynomials is a $\mathbb{F}_q$-algebra.

Definition 3.7. Let $k\langle x^q \rangle$ denote the set of polynomials of the form $a_0x + a_1x^q + \ldots + a_nx^{q^n}$.

Proposition 3.8. *$k\langle x^q \rangle$ is a $\mathbb{F}_q$-algebra with pointwise addition, multiplication given by composition and the multiplication with elements $u \in \mathbb{F}_q$ defined by $u(a_0x + a_1x^q + \ldots + a_nx^{q^n}) = a_0ux + a_1ux^q + \ldots + a_nux^{q^n}$.*

Proof. First we see that $k\langle x^q \rangle$ is clearly closed under addition and multiplication with elements $u \in \mathbb{F}_q$. If we have $f(x) = a_0x + \ldots + a_nx^{q^n}$ and $g(x) = b_0x + \ldots + b_mx^{q^m}$ then $f(g(x)) = f(b_0x + \ldots + b_mx^{q^m}) = a_0b_0x + (a_1b_0^q + a_0b_1)x^q + \ldots + a_nb_m^{q^n}x^{q^{n+m}}$ because of the freshman's dream, so $k\langle x^q \rangle$ is closed under composition.
We can easily see that $k\langle x^q \rangle$ is a $\mathbb{F}_q$-vector space. We also have that for $f, g, h \in k\langle x^q \rangle$ it is the case that $f(g+h)(x) = f(g(x)+h(x)) = f(g(x)) + f(h(x))$, because f is additive, and $(g+h)(f)(x) = (g+h)(f(x)) = g(f(x)) + h(f(x))$, so multiplication is indeed distributive over addition.
Now we only need to check that scalar multiplication and ring multiplication are compatible. Let $u \in \mathbb{F}_q$ and $f(x) = a_0x + a_1x^q + \ldots + a_nx^{q^n} \in k\langle x^q \rangle$. We first claim $uf(x) = f(ux)$. We have $f(ux) = a_0(ux) + a_1(ux)^q + \ldots + a_n(ux)^{q^n}$. We know that $u^q = u$, because $u \in \mathbb{F}_q$, so we also have $u^{q^m} = (u^q)^{q^{m-1}} = u^{q^{m-1}} = \ldots = u$ for all $1 \leq m \leq n$, so $a_0(ux) + a_1(ux)^q + \ldots + a_n(ux)^{q^n} = a_0ux + a_1ux^q + \ldots + a_nux^{q^n} = uf(x)$. Now we have for $u, v \in \mathbb{F}_q$ and $f, g \in k\langle x^q \rangle$ that $(u \cdot f) \circ (v \cdot g) = uf(vg) = uv(f(g)) = (uv) \cdot f \circ g$, so we are done. □

We still have $A = \mathbb{F}_q[T]$. We can see that A is also a $\mathbb{F}_q$-algebra, because we can add and multiply elements in A, multiply elements in A with elements in $\mathbb{F}_q$, and these two kinds of multiplication are clearly compatible and distributive over addition.

Definition 3.9. A *Drinfeld module* for A defined over k will be an $\mathbb{F}_q$-algebra homomorphism $\rho\colon A \to k\langle x^q \rangle$ such that for all $a \in A$ the constant term of $\rho_a := \rho(a)$ is a and, moreover, for at least one $a \in A$, $\rho_a \notin k$.

We have a homomorphism, so when we know where T maps to, we know where T^n maps to, because our map is multiplicative. Multiplication with elements from $\mathbb{F}_q$ is compatible, so if we know where T^n maps to, we know where vT^n maps to with $v \in \mathbb{F}_q$. Our maps is additive, so when we know where T maps to, we know where all elements in A map to.
So in general we have something of the form

$$\rho_T = Tx + c_1x^q + \ldots + c_rx^{q^r} \text{ with } c_1, c_2, \ldots, c_n \in k$$

The number r is called the rank of the Drinfeld module. It turns out that the roots of a polynomial ρ_a have a quite interesting structure. But first we need some other lemma.

Lemma 3.10. *The polynomial $ax + c_1x^q + \ldots + c_rx^{q^r}$ with $a \neq 0$ is separable.*

Proof. We take the derivative, and since the characteristic is $p \mid q$, the derivative is equal to $a \neq 0$, so our polynomial is separable. □

So when we add all the roots of a polynomial of this form, we indeed get a Galois extension.

Definition 3.11. We define $\Lambda_\rho[a] := \{\lambda \in \overline{k} \mid \rho_a(\lambda) = 0\}$.

One of the reasons that our map is called a module, is that the set of roots $\Lambda_\rho[a]$ has a module structure. Let us first define a module.

Definition 3.12. Suppose R is a ring with identity 1_R. A *left R-module* M consists of an abelian group $(M, +)$ and an operation $\cdot\colon R \times M \to M$ such that for all $r, s \in R$ and $x, y \in M$ we have the following:

$$\begin{aligned} r \cdot (x + y) &= r \cdot x + r \cdot y \\ (r + s) \cdot x &= r \cdot x + s \cdot x \\ (r \cdot s) \cdot x &= r \cdot (s \cdot x) \\ 1_R \cdot x &= x \end{aligned}$$

Right R-modules are defined in a similar way.
If M, N are left R-modules, then a *left module homomorphism* is a map $f\colon M \to N$ such that

$$f(r \cdot m + s \cdot n) = r \cdot f(m) + s \cdot f(n)$$

This definition looks like the definition of a vector space, and this is indeed the same definition if R is a field.

Lemma 3.13. *$\Lambda_\rho[a]$ is a left A-module with multiplication defined by $(a, \lambda) \mapsto \rho_a(\lambda)$.*

Proof. First we will show that the roots indeed form an abelian group with the addition from $\overline{k}$, which is clearly associative and commutative. Because our polynomials takes the form $p(x) = c_0x + c_1x^q + \ldots + c_nx^{q^n}$, we can see that 0 is a root. This polynomial is additive, so if λ, μ are roots, then $\lambda + \mu$ is also a root. We also have that if λ is a root, and if the characteristic is 2, then $\lambda + \lambda = 0$, so we have an additive inverse. If the characteristic isn't equal to 2, it is odd, and all exponents in $c_0x + c_1x^q + \ldots + c_nx^{q^n}$ are odd, so $p(-\lambda) = c_0 \cdot -\lambda + c_1 \cdot (-\lambda)^q + \ldots + c_n \cdot (-\lambda)^{q^n} = -c_0\lambda - c_1\lambda^q - \ldots - c_n\lambda^{q^n} = -p(\lambda) = 0$, so we have additive inverses.
Let $b \in A$, then ρ_b maps to an additive polynomial, so $\rho_b(\lambda + \mu) = \rho_b(\lambda) + \rho_b(\mu)$.
Let $b, c \in A$, then because ρ is an algebra homomorphism mapping A to something, we have $\rho_{b+c}(\lambda) = \rho_b(\lambda) + \rho_c(\lambda)$.
The third and fourth property also follow because ρ in an algebra homomorphism mapping A to something. □

Now that we know that we have a module structure, we will identify this module structure in general. Note that from now on we will only work with powers of T instead of general elements in A. The reason for this is that the proofs become less abstract, and we can more clearly see the roots we are working with.

Proposition 3.14. *Let ρ be a Drinfeld module of rank r. Then we have the following isomorphism as A-modules*

$$\Lambda_\rho[T^n] \cong \bigoplus_{i=1}^{r} A/T^nA.$$

Proof. We will prove this with induction to n.
Induction basis For $n = 1$ we have that the number of elements in $\Lambda_\rho[T]$ is equal to q^r. We also know that for $\lambda \in \Lambda_\rho[T]$ we have $\rho_T(\lambda) = 0$, so as a module we have that all elements vanish when you multiply them by T, and since T is irreducible, we get a number of copies of A/TA, and these cannot be split into smaller modules. The number of elements in A/TA is equal to q, so we indeed get the sum of r copies.
Induction step Suppose the above is true for $n = m$. For $n = m + 1$ we first take ρ_T of every element in $\Lambda_\rho[T^{m+1}]$. Then we know we get $\bigoplus_{i=1}^{r} A/T^mA$. So we know that if we multiply all our elements by T, we get $\bigoplus_{i=1}^{r} A/T^mA$, so $\bigoplus_{i=1}^{r} A/T^{m+1}A$ is contained in our module for $n = m + 1$. The degree of our polynomial for $n = m + 1$ is equal to $q^{r(m+1)}$, because a polynomial of degree q^r gets composed $m + 1$ times. But the number of elements in $\bigoplus_{i=1}^{r} A/T^{m+1}A$ is already equal to $q^{r(m+1)}$, so this is our whole module. □

Note that the multiplication of elements in A with elements in A/T^nA is compatible with the canonical multiplication of elements in A/T^nA with other elements in A/T^nA.
Now we can use this module structure to get to know something about the structure of our Galois group.

Proposition 3.15. *Let $K_{\rho,T^n} := k(\Lambda_\rho[T^n])$. Then there is a group monomorphism*

$$Gal(K_{\rho,T^n}/k) \to GL_r(A/T^nA)$$

Proof. We have that $GL_r(A/T^nA)$ is the group of all the invertible $r \times r$-matrices over A/T^nA, which is the same as all automorphisms of $\bigoplus_{i=1}^r A/T^nA$. So this proposition is equivalent to proving that every element of the Galois group gives a unique automorphism of $\bigoplus_{i=1}^r A/T^nA$.
Let $\sigma \in \mathrm{Gal}(K_{\rho,T^n}/k)$. We know that an element of the Galois group permutes the zeroes of the polynomial of which it is the splitting field, and since K_{ρ,T^n} is the splitting field of ρ_{T^n}, we see that if $\rho_{T^n}(\lambda) = 0$, then $\rho_{T^n}(\sigma(\lambda)) = 0$, so σ indeed induces a map from the roots of ρ_{T^n} to itself.
We will now check that σ preserves the module structure, which means that σ is a module homomorphism. We have for $a, b \in A$ and $\lambda, \mu \in \Lambda_\rho[T^n]$ that $\sigma(\rho_a(\lambda) + \rho_b(\mu)) = \sigma(\rho_a(\lambda)) + \sigma(\rho_b(\mu))$ because σ is a field automorphism. We have the following, because σ is a field automorphism that leaves k invariant

$$\begin{aligned}
\sigma(\rho_a(x)) &= \sigma(ax + c_1x^q + \ldots + c_nx^{q^n}) \\
&= \sigma(ax) + \sigma(c_1x^q) + \ldots + \sigma(c_nx^{q^n}) \\
&= a\sigma(x) + c_1\sigma(x^q) + \ldots + c_n\sigma(x^{q^n}) \\
&= a\sigma(x) + c_1(\sigma(x))^q + \ldots + c_n(\sigma(x))^{q^n} \\
&= \rho_a(\sigma(x))
\end{aligned}$$

This works for all x, and works the same for b, so we indeed get $\sigma(\rho_a(\lambda)) + \sigma(\rho_b(\mu)) = \rho_a(\sigma(\lambda)) + \rho_b(\sigma(\mu))$.
Now we need to check that σ induces an automorphism, so we need to prove that is bijective. But σ is field automorphism on K_{ρ,T^n}, which contains all elements in our module $\Lambda_\rho[T^n]$, so it is especially bijective on a subset of K_{ρ,T^n} that it preserves.
Finally we need to check that every element in $\mathrm{Gal}(K_{\rho,T^n}/k)$ gives rise to a unique element in $GL_r(A/T^nA)$. We know that an element of the Galois group is uniquely determined by its action on the roots of the polynomial of which it is the splitting field, so if we have that two elements in $GL_r(A/T^nA)$, then they determine different elements in $\mathrm{Gal}(K_{\rho,T^n}/k)$, so our map is indeed injective. □

We will now prove that the map above is a bijection for a certain Drinfeld module, namely $T \mapsto Tx + x^q$. But before we do that, we need a lemma.

Lemma 3.16. *Let $\kappa\colon T \mapsto Tx + x^q$ be a Drinfeld module. Then $\frac{\kappa_{T^n}}{\kappa_{T^{n-1}}}$ is an Eisenstein polynomial at T.*

Proof. First we see that T is an irreducible polynomial, so indeed a prime. We will prove this lemma by induction to n. We will not only prove that $\frac{\kappa_{T^n}}{\kappa_{T^{n-1}}}$ is an Eisenstein polynomial at T, but also that in κ_{T^n} every coefficient except the leading coefficient is divisible by T.
Induction basis $T^0 = 1$, and 1 maps to x. So for $n = 1$ we have $\frac{Tx+x^q}{x} = T + x^{q-1}$, which is clearly an Eisenstein polynomial. We also have that in $Tx+x^q$ every coefficient except the leading coefficient is divisible by T.
Induction step Suppose that for $n = m$ we have that $\frac{\kappa_{T^m}}{\kappa_{T^{m-1}}}$ is Eisenstein. When we use that κ is an algebra homomorphism, and thus multiplicative, we have the following:

$$\begin{aligned}
\frac{\kappa_{T^{m+1}}}{\kappa_{T^m}} &= \frac{\kappa_T(\kappa_{T^m})}{\kappa_{T^m}} \\
&= \frac{T \cdot \kappa_{T^m} + \kappa_{T^m}^q}{\kappa_{T^m}} \\
&= T + \kappa_{T^m}^{q-1}
\end{aligned}$$

Since in κ_{T^m} every coefficient except the leading coefficient is divisible by T, this is also the case for $\kappa_{T^m}^{q-1}$. T is the new coefficient of x^0, and since $T^2 \nmid T$, we indeed again have an Eisenstein polynomial.

We have $\kappa_{T^{m+1}}(x) = \kappa_T(\kappa_{T^m}(x)) = T\kappa_{T^m}(x) + (\kappa_{T^m}(x))^q$. In $T\kappa_{T^m}$ every coefficient is divisible by T, and since κ_{T^m} has a degree greater or equal to 2 for $m \geq 1$, we see that $(\kappa_{T^m}(x))^q$ has a larger degree than $T\kappa_{T^m}(x)$, so the leading coefficient can be found in $(\kappa_{T^m}(x))^q$. Since in $\kappa_{T^m}(x)$ every coefficient except the leading coefficient is divisible by T, the same is the case for $(\kappa_{T^m}(x))^q$, so in $T\kappa_{T^m}(x) + (\kappa_{T^m}(x))^q$ every coefficient except the leading coefficient is divisible by T. □

Proposition 3.17. *Let $\kappa_T := Tx + x^q$. Then $Gal(K_{\kappa,T^n}) \cong (A/T^nA)^*$.*

Proof. We know that our map is injective, so the number of elements in $\mathrm{Gal}(K_{\kappa,T^n})$ is less or equal to the number of elements in $(A/T^nA)^*$. We know because of proposition 2.12 that the number of elements in $(A/T^nA)^*$ is equal to $q^n - q^{n-1}$, so the number of elements in $\mathrm{Gal}(K_{\kappa,T^n})$ is less or equal to $q^n - q^{n-1}$.
We also have that $\frac{\kappa_{T^n}}{\kappa_{T^{n-1}}}$ has degree $q^n - q^{n-1}$ and is irreducible and separable, so by lemma 2.27, the number of elements in $\mathrm{Gal}(K_{\kappa,T^n})$ is greater of equal to $q^n - q^{n-1}$. So the number of elements in our Galois group is equal to $q^n - q^{n-1}$, and because the above map is a monomorphism between two finite sets with the same number of elements, the map is an isomorphism. □

Corollary 3.18. *Suppose λ is a root of $\frac{\kappa_{T^n}}{\kappa_{T^{n-1}}}$. Then $K_{\kappa,T^n} = k(\lambda)$.*

Proof. We have that $[k(\lambda)\colon k] = q^n - q^{n-1}$, because this is the degree of our irreducible polynomial. We also have

$$\begin{aligned} q^n - q^{n-1} &= |\mathrm{Gal}(K_{\kappa,T^n}| \\ &= [K_{\kappa,T^n}\colon k] \\ &= [K_{\kappa,T^n}\colon k(\lambda)] \cdot [k(\lambda)\colon k] \\ &= [K_{\kappa,T^n}\colon k(\lambda)] \cdot q^n - q^{n-1} \end{aligned}$$

So $[K_{\kappa,T^n}\colon k(\lambda)] = 1$, so we indeed already have our splitting field when we only add one root. □

4 A non-surjective polynomial of rank 2

In this section we will determine the Galois group of $\sigma\colon T \mapsto Tx + x^{q^2}$ for powers of T. Note that $\frac{\sigma_{T^n}}{\sigma_{T^{n-1}}}$ is irreducible because it is an Eisenstein polynomial at T. This follows via a proof similar to the one for $T \mapsto Tx + x^q$ in lemma 3.16. All of this section is my own work.
First we will determine the number of elements in this Galois group.

Lemma 4.1. *The number of elements in the Galois group of σ_{T^n} is $2(q^{2n} - q^{2n-2})$.*

Proof. We will prove that $[K_{\sigma,T^n}\colon k] = 2(q^{2n} - q^{2n-2})$. First we claim that $\sigma_{T^n}(x)$ is of the form $a_0x + a_1x^{q^2} + \ldots + a_nx^{q^{2n}}$ with $a_n \neq 0$. We see that $Tx + x^{q^2}$ is of this form, and $T(a_0x + a_1x^{q^2} + \ldots + a_nx^{q^{2n}}) + (a_0x + a_1x^{q^2} + \ldots + a_nx^{q^{2n}})^{q^2} = Ta_0x + (a_1 + a_0^{q^2})x^{q^2} + \ldots + a_n^{q^{2n}}x^{q^{2n+2}}$, so with induction we see that all $\sigma_{T^n}(x)$ are of this form.
Let α be the root of an irreducible polynomial of degree 2 over $\mathbb{F}_q$. We know that $\mathbb{F}_{q^2} \cong \mathbb{F}_q[\alpha]$, so $\alpha^{q^2} = \alpha$. Then we have that is λ is root of $\sigma_{T^n}(x)$, then $\alpha\lambda$ is also a root. So $\alpha \in K_{\sigma,T^n}$. We will first add α to $\mathbb{F}_q(T)$, and in this way we get an extension of degree to and get $\mathbb{F}_q(\alpha, T) \cong \mathbb{F}_{q^2}(T)$.
Because we are in $\mathbb{F}_{q^2}(T)$, we see that here σ is the Carlitz module. Because this is the Carlitz module, we know that if we add all the roots of σ_{T^n} to $\mathbb{F}_q^2(T)$ we get an extension of degree $|(\mathbb{F}_{q^2}[T]/T^n\mathbb{F}_{q^2}[T])^*|$, see proposition 3.17. We know because of lemma 2.12 and that $|T|_{\mathbb{F}_{q^2}} = q^{2\deg(T)} = q^2$, that this number is equal $q^{2n} - q^{2n-2}$. We know that if we have a tower of field extensions $K \subset L \subset M$, that $[M : K] = [M : L][L : K]$ (see lemma 2.22), so the degree of our total extension is $2(q^{2n} - q^{2n-2})$.
So by first adding α and then the rest of the roots, we indeed made the splitting field of σ_{T^n} over $\mathbb{F}_q(T)$, so we have a Galois extension, so the number of elements in the Galois group is indeed equal to the degree of our total extension. □

Note that we in general know what an irreducible polynomial of degree 2 looks like. For odd characteristic we have that $\mathbb{F}_q^*$ has an even number of elements, so x^2 is not a bijection, so if we take $w \in \mathbb{F}_q^*$ a generator, we have that $x^2 - w$ is irreducible. For characteristic 2 we have that $x^2 + x$ isn't an injective function over $\mathbb{F}_{2^m}$, because both 0 and 1 map to 0, so it also isn't surjective, and we can find a w that isn't in the image, and then $x^2 + x - w = x^2 + x + w$ is irreducible.
To examine the Galois group, we will first look more closely at the exact structure of $\Lambda_\sigma[T^n]$.

Lemma 4.2. *Let α be a root of an irreducible polynomial of degree 2 over $\mathbb{F}_q$, and λ_m a root of $\frac{\sigma_{T^m}}{\sigma_{T^{m-1}}}$. All roots in $\Lambda_\sigma[T^n]$ have the form $(a_n + \alpha b_n)\lambda_n + \ldots + (a_1 + \alpha b_1)\lambda_1$ with all $a_i, b_j \in \mathbb{F}_q$.*

Proof. First we prove that all expressions of the form $(a_n + \alpha b_n)\lambda_n + \ldots + (a_1 + \alpha b_1)\lambda_1$ are a root. We know that if we take λ_l with $l \leq n$, that $\sigma_{T^n}(\lambda_l) = \sigma_{T^{n-l}}(\sigma_{T^l}(\lambda_l)) = \sigma_{T^{n-l}}(0) = 0$. We also know that multiplying with elements from $\mathbb{F}_{q^2}$ still makes something a root, because all coefficients are an even power of q, and elements of the form $a_i + \alpha b_i$ are exactly the elements in $\mathbb{F}_{q^2} = \mathbb{F}_q(\alpha)$. We know that σ_{T^n} is additive, so $(a_n + \alpha b_n)\lambda_n + \ldots + (a_1 + \alpha b_1)\lambda_1$ is indeed a root.
Now we want to show that all elements of the form $(a_n + \alpha b_n)\lambda_n + \ldots + (a_1 + \alpha b_1)\lambda_1$ are different, which is equivalent to saying that none of these is 0. Suppose $(a_n + \alpha b_n)\lambda_n + \ldots + (a_1 + \alpha b_1)\lambda_1 = 0$. Then we have $(a_n + \alpha b_n)\lambda_n = -(a_{n-1} + \alpha b_{n-1})\lambda_{n-1} - \ldots - (a_1 + \alpha b_1)\lambda_1$, so $\lambda_n \in \mathbb{F}_{q^2}(\lambda_{n-1})$. But we know that λ_n is a root of $\frac{\sigma_{T^l}}{\sigma_{T^{l-1}}}$, so it cannot be contained in $\mathbb{F}_{q^2}(\lambda_{n-1})$, so all elements of the form $(a_n + \alpha b_n)\lambda_n + \ldots + (a_1 + \alpha b_1)\lambda_1$ are different.
We see that there are q^{2n} elements of the form $(a_n + \alpha b_n)\lambda_n + \ldots + (a_1 + \alpha b_1)\lambda_1$, because there are $2n$ numbers a_i, b_j and we have q choices for each of these. We also see that the number of elements in $\Lambda_\sigma[T^n]$ is equal to q^{2n}, because the the polynomial $\sigma_{T^n}(x)$ is of the form $a_0 x + \ldots + a_n x^{q^{2n}}$, and this polynomial has q^{2n} roots. Combining this with the fact that all elements of the form $(a_n + \alpha b_n)\lambda_n + \ldots + (a_1 + \alpha b_1)\lambda_1$ are different roots, we see that all roots are of this form. □

Now that we know the structure of the roots, we can define our isomorphism as modules explicitly.

Proposition 4.3. *Let Y be some transcendental element over $\mathbb{F}_q$, and $B = \mathbb{F}_q[Y]$. There is an isomorphism $\Lambda_\sigma[T^n] \cong B/Y^nB \oplus B/Y^nB$ given by the map f with $f((a_n + \alpha b_n)\lambda_n + \ldots + (a_1 + \alpha b_1)\lambda_1) = (a_n + a_{n-1}Y + \ldots + a_1 Y^{n-1}, b_n + b_{n-1}Y + \ldots + b_1 Y^{n-1})$ for all $a_i, b_j \in \mathbb{F}_q$.*

Proof. We will first check whether f is a homomorphism. f is clearly well-defined. Let $a, b \in A$ and $\lambda, \mu \in \Lambda_\sigma[T^n]$. When we look at $f(\sigma_a(\lambda) + \sigma_b(\mu))$, we know that $\sigma_a(\lambda), \sigma_b(\mu)$ are also elements of $\Lambda_\sigma[T^n]$, because σ is an algebra homomorphism, so $\sigma_{T^n}(\sigma_a(\lambda)) = \sigma_a(\sigma_{T^n}(\lambda)) = \sigma_a(0) = 0$, and the same for $\sigma_b(\mu)$. So we can write $\sigma_a(\lambda) = (c_n + \alpha d_n)\lambda_n + \ldots + (c_1 + \alpha d_1)\lambda_1$ and $\sigma_b(\mu) = (r_n + \alpha s_n)\lambda_n + \ldots + (r_1 + \alpha s_1)\lambda_1$. We can see because $B/YB \oplus B/YB$ has a module structure, that we have the following

$$\begin{aligned}
f(\sigma_a(\lambda) + \sigma_b(\mu)) &= f((c_n + \alpha d_n)\lambda_n + \ldots + (c_1 + \alpha d_1)\lambda_1 + (r_n + \alpha s_n)\lambda_n + \ldots + (r_1 + \alpha s_1)\lambda_1) \\
&= f((c_n + r_n + \alpha(d_n + s_n))\lambda_n + \ldots + (c_1 + r_1 + \alpha(d_1 + s_1))\lambda_1) \\
&= ((c_n + r_n) + \ldots + (c_1 + r_1)Y^{n-1}, (d_n + s_n) + \ldots + (d_1 + s_1)Y^{n-1}) \\
&= (c_n + \ldots + c_1 Y^{n-1}, d_n + \ldots + d_1 Y^{n-1}) + (r_n + \ldots + r_1 Y^{n-1}, s_n + \ldots + s_1 Y^{n-1}) \\
&= f(\sigma_a(\lambda)) + f(\sigma_b(\mu))
\end{aligned}$$

To show that we can change the order of σ and f, we will first show that if $\gamma \in \mathbb{F}_q$ and $(u_n + \alpha v_n)\lambda_n + \ldots + (u_1 + \alpha v_1)\lambda_1 = \nu \in \Lambda_\sigma[T^n]$, then there are two cases for $f(\sigma_{\gamma T^l})$. If $l \geq n$, then $\sigma_{\gamma T^l}(\nu) = 0$ for all $\nu \in \Lambda_\sigma[T^n]$. We then also have $\sigma_{\gamma T^l}(u_n + \ldots + u_1 Y^{n-1}, v_n + \ldots + v_1 Y^{n-1}) = \gamma \cdot (u_n Y^l + \ldots + u_1 Y^{n-1+l}, v_n Y^l + \ldots + v_1 Y^{n-1+l}) = (0, 0)$, because $l \geq n$. So we have $f(\sigma_{\gamma T^l}(\nu)) = f(0) = 0 = \sigma_{\gamma T^l}(0) = \sigma_{\gamma T^l}(f(\nu))$.
Now suppose that $l < n$. We have the following because of the actions of σ and f and the fact that $Y^m \equiv 0$

mod Y^n for $m \geq n$.

$$\begin{aligned}
f(\sigma_{\gamma T^l}(\nu)) &= f((\gamma u_n + \alpha\gamma v_n)\lambda_{n-l} + \ldots + (\gamma u_{l+1} + \alpha\gamma u_{l+1})\lambda_1) \\
&= (\gamma u_n Y^l + \ldots + \gamma u_{l+1}Y^{n-1}, \gamma v_n Y^l + \ldots + \gamma v_{l+1}Y^{n-1}) \\
&= \gamma Y^l \cdot (u_n + \ldots + u_{l+1}Y^{n-l-1} + \ldots + u_1 Y^{n-1}, v_n + \ldots + v_{l+1}Y^{n-l-1} + \ldots + v_1 Y^{n-1}) \\
&= \sigma_{\gamma T^l}(u_n + \ldots + u_{l+1}Y^{n-l-1} + \ldots + u_1 Y^{n-1}, v_n + \ldots + v_{l+1}Y^{n-l-1} + \ldots + v_1 Y^{n-1}) \\
&= \sigma_{\gamma T^l} f((u_n + \alpha v_n)\lambda_n + \ldots + (u_1 + \alpha v_1)\lambda_1) \\
&= \sigma_{\gamma T^l} f(\nu)
\end{aligned}$$

We also know that f is additive on all elements in $\Lambda_\sigma[T^n]$, and σ is an algebra homomorphism, so for all $\nu \in \Lambda_\sigma[T^n]$ and $r, s \in A$ for which σ and f commute, we have $f(\sigma_{r+s}(\nu)) = f(\sigma_r(\nu) + \sigma_s(\nu)) = \sigma_r(f(\nu)) + \sigma_s(f(\nu)) = \sigma_{r+s}(f(\nu))$, so in this way we prove from just knowing dat f and σ commute for elements of the form γT^l, that this is the case for all elements in A, so $f(\sigma_a(\lambda)) + f(\sigma_b(\mu)) = \sigma_a(f(\lambda)) + \sigma_b(f(\mu))$, so we indeed have a homomorphism.
Now we still need to prove that our map is a bijection. We know that all elements in $B/Y^nB \oplus B/Y^nB$ have unique representants of the form $(a_n + a_{n-1}Y + \ldots + a_1 Y^{n-1} \mod Y^n, b_n + b_{n-1}Y + \ldots + b_1 Y^{n-1} \mod Y^n)$ with $a_i, b_j \in \mathbb{F}_q$, and these are all reached, because $(a_n + \alpha b_n)\lambda_n + (a_{n-1} + \alpha b_{n-1})\lambda_{n-1} + \ldots + (a_1 + \alpha b_1)\lambda_1$ maps to this element, so f is surjective. Both sets are finite, so f is also bijective, so f is an isomorphism. □

We know that we have a monomorphism $\mathrm{Gal}(K_{\sigma,T^n}/k) \to GL_2(A/T^nA) \cong GL_2(B/Y^nB)$. We will use this and the above isomorphism to see what our Galois group looks like.

Theorem 4.4. *Suppose q is odd, $x^2 - w$ is an irreducible polynomial over $\mathbb{F}_q$ and α is a root of this polynomial. Then the Galois group of K_{σ,T^n} is isomorphic to the subgroup of $GL_2(B/Y^nB)$ generated by the following matrices*

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \begin{pmatrix} a_n + \ldots + a_1 Y^{n-1} & wb_n + \ldots + wb_1 Y^{n-1} \\ b_n + \ldots + b_1 Y^{n-1} & a_n + \ldots a_1 Y^{n-1} \end{pmatrix}$$

with $a_i, b_j \in \mathbb{F}_q$ and a_i, b_j not both 0.
Suppose q is a power of 2 and α is a root of the irreducible polynomial $x^2 + x + w$ over $\mathbb{F}_q$. Then the Galois group of K_{σ,T^n} is isomorphic to the subgroup of $GL_2(B/Y^nB)$ generated by the following matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} a_n + \ldots + a_1 Y^{n-1} & wb_n + \ldots + wb_1 Y^{n-1} \\ b_n + \ldots + b_1 Y^{n-1} & a_n + b_n + \ldots + (a_1 + b_1)Y^{n-1} \end{pmatrix}$$

with $a_i, b_j \in \mathbb{F}_q$ and a_i, b_j not both 0.

Proof. We know that $K_{\sigma,T^n} = k(\alpha, \lambda_n)$, because α gave an extension of degree 2 and λ_n of degree $q^{2n} - q^{2n-2}$ because of 3.18. To determine the Galois group, we only need the images of α and λ_n. We see that is also enough to determine the image of λ_n and $\alpha\lambda_n$. In $B/Y^nB \oplus B/Y^nB$ this is the same as determining where $(1,0)^T$ and $(0,1)^T$ map to.
For α there are only two options, namely sending it to itself or to its conjugate. Sending it to itself gives the identity matrix. If the q is odd, then $-\alpha$ is the conjugate of α, because if $\alpha^2 = w$, then $(-\alpha)^2 = w$, and then we have that λ_n maps to itself and $\alpha\lambda_n$ maps to $-\alpha\lambda_n$, so $(1,0)^T$ maps to itself and $(0,1)^T$ maps to $(0,-1)^T$, so we get the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. If q is a power of 2, then $\alpha + 1$ is the conjugate of α, because if $\alpha^2 + \alpha = w$, then $(\alpha+1)^2 + \alpha + 1 = \alpha^2 + 1 + \alpha + 1 = w$. So λ_n again maps to itself, but $\alpha\lambda_n$ maps to $\lambda_n + \alpha\lambda_n$, so $(1,0)^T \mapsto (1,0)^T$ and $(0,1)^T \mapsto (1,1)^T$, so we indeed get the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.
For λ_n there are $\deg(\frac{\sigma_{T^n}(x)}{\sigma_{T^n}(x)}) = q^{2n} - q^{2n-2}$ options. We know that all roots of σ_{T^n} take the form $(a_n + \alpha b_n)\lambda_n + \ldots + (a_1 + \alpha b_1)\lambda_1$, and all roots of $\sigma_{T^{n-1}}$ take the form $(c_{n-1} + \alpha d_{n-1})\lambda_{n-1} + \ldots + (c_1 + \alpha d_1)\lambda_1$, so all roots that λ_n can be mapped to are of the form $(a_n + \alpha b_n)\lambda_n + \ldots + (a_1 + \alpha b_1)\lambda_1$ with $a_n + \alpha b_n \neq 0$, and since $1, \alpha$ are additively independent, we have $a_n \neq 0$ or $b_n \neq 0$. We see that there are q^{2n} elements of the form $(a_n + \alpha b_n)\lambda_n + \ldots + (a_1 + \alpha b_1)\lambda_1$ and q^{2n-2} elements of the form $(c_{n-1} + \alpha d_{n-1})\lambda_{n-1} + \ldots + (c_1 + \alpha d_1)\lambda_1$, so there are indeed $q^{2n} - q^{2n-2}$ elements of the form $(a_n + \alpha b_n)\lambda_n + \ldots + (a_1 + \alpha b_1)\lambda_1$ with $a_n + \alpha b_n \neq 0$.
When q is odd and we map λ_n to $(a_n + \alpha b_n)\lambda_n + \ldots + (a_1 + \alpha b_1)\lambda_1$, then $\alpha\lambda_n$ maps to $(\alpha a_n + \alpha^2 b_n)\lambda_n + \ldots + (\alpha a_1 + \alpha^2 b_1)\lambda_1$, and since $\alpha^2 = w$, this is equal to $(wb_n + \alpha a_n)\lambda_n + \ldots + (wb_1 + \alpha a_1)\lambda_1$. So in vectors we have

that $(1,0)^T \mapsto (a_n+\ldots+a_nY^{n-1}, b_n+\ldots+b_1Y^{n-1})^T$ and $(0,1)^T \mapsto (wb_n+\ldots+wb_1Y^{n-1}, a_n+\ldots+a_1Y^{n-1})^T$, and this indeed corresponds to

$$\begin{pmatrix} a_n+\ldots+a_1Y^{n-1} & wb_n+\ldots+wb_1Y^{n-1} \\ b_n+\ldots+b_1Y^{n-1} & a_n+\ldots a_1Y^{n-1} \end{pmatrix}.$$

When q is a power of 2 and we map λ_n to $(a_n+\alpha b_n)\lambda_n+\ldots+(a_1+\alpha b_1)\lambda_1$, then $\alpha\lambda_n$ maps to $(\alpha a_n+\alpha^2 b_n)\lambda_n+\ldots+(\alpha a_1+\alpha^2 b_1)\lambda_1$, and since $\alpha^2=\alpha+w$, this is equal to $(wb_n+\alpha(a_n+b_n))\lambda_n+\ldots+(wb_1+\alpha(a_1+b_1))\lambda_1$. So in vectors we get $(1,0)^T \mapsto (a_n+\ldots+a_nY^{n-1}, b_n+\ldots+b_1Y^{n-1})^T$ and $(0,1)^T \mapsto (wb_n+\ldots+wb_1Y^{n-1}, a_n+b_n+\ldots+(a_1+b_1)Y^{n-1})^T$, so this indeed corresponds to

$$\begin{pmatrix} a_n+\ldots+a_1Y^{n-1} & wb_n+\ldots+wb_1Y^{n-1} \\ b_n+\ldots+b_1Y^{n-1} & a_n+b_n+\ldots+(a_1+b_1)Y^{n-1} \end{pmatrix}.$$

So the above matrices are indeed in our Galois group, and they correspond to conjugation of α and mapping λ_n to one of its conjugates. These two operations clearly generate the Galois group. □

We can use this representation to see that we have found a polynomial with as Galois group a special group, namely a semi-dihedral group.

Definition 4.5. The *dihedral group* is the symmetry group of the regular n-polygon, and is given by $\langle r,s\colon r^n=s^2=e, rs=sr^{-1}\rangle$. Here r corresponds to rotation through an angle of $\frac{360}{n}{}^\circ$ degrees and s is a reflection across a line.
The *semi-dihedral group* is a certain group of order 2^n that is also generated by two elements where one of the elements has order 2, and is given by $\langle r,s\colon r^{2^{n-1}}=s^2=e, rs=sr^{2^{n-2}-1}\rangle$.

Corollary 4.6. *The group $Gal(K_{\sigma,T}/\mathbb{F}_3(T))$ isomorphic to the semi-dihedral group with 16 elements.*

Proof. We take x^2-2 as irreducible polynomial. The number of elements in $\mathrm{Gal}(K_{\sigma,T}/\mathbb{F}_3(T))$ is equal to $2(3^2-1)=16$.
We see that the elements $\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1&2\\1&1\end{smallmatrix}\right)$ are in our group. We have $\left(\begin{smallmatrix}1&2\\1&1\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}1&2\\1&1\end{smallmatrix}\right) = \left(\begin{smallmatrix}0&1\\2&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&1\\2&0\end{smallmatrix}\right)^2 = \left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right)^2 = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$, so $\left(\begin{smallmatrix}1&2\\1&1\end{smallmatrix}\right)$ has order 8. We also see that $\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)$ has order 2. We have $\left(\begin{smallmatrix}1&2\\1&1\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&1\\1&2\end{smallmatrix}\right)$, and $\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}1&2\\1&1\end{smallmatrix}\right)^3 = \left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}1&2\\1&1\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}0&1\\2&0\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}1&1\\2&1\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&1\\1&2\end{smallmatrix}\right)$, so we indeed have this semi-dihedral group. □

5 A surjective polynomial of rank 2

In this section we will prove that the Galois group of the splitting field of $Tx+Tx^q+x^{q^2}$ over k is equal to the whole of $GL_2(A/TA)$. We already know that there is a monomorphism from this Galois group into $GL_2(A/TA)$, so to prove this we need to prove that the number of elements is equal. Most of this section is my own work.
We start by determining the number of elements in $GL_2(A/TA)$.

Lemma 5.1. *The number of elements in $GL_2(A/TA)$ is equal to $q(q-1)^2(q+1)$.*

Proof. We need to determine the number of invertible matrices over $A/TA=\mathbb{F}_q$. A matrix is invertible if the first and second row are non-zero, and the second row is not a scalar multiple of the first row. There are q^2-1 options for the the first row, because there are q choice for the first coordinate and q choices for the second coordinate, and the first row is only 0 when both coordinates are 0.
There are $q^2-1-(q-1)$ options for the second row, because we there are again q^2-1 possible non-zero rows, but we cannot take one of the $q-1$ non-zero multiples of the first row. So this gives a total of $(q^2-1)(q^2-q)=q(q-1)^2(q+1)$ invertible matrices. □

Now we state a proposition that will be quite useful to determine a lower bound for the number of elements in the Galois group.

Proposition 5.2. *Let K be a field and $p(x) \in K[x]$ be an irreducible polynomial of degree n. Let $K(\alpha_1, \ldots, \alpha_s)$ be the field obtained by adding s roots of $p(x)$. Let $p_0(x) := p(x)$ and $p_s(x) \in K(\alpha_1, \ldots, \alpha_s)[x]$ be the polynomial that is obtained by throwing away s roots, so*

$$p_s(x) := \frac{p(x)}{(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_s)}$$

The Galois group of the splitting field of $p(x)$ over K contains at least $n(n-1)\cdots(n-m)$ elements if $p_s(x)$ is irreducible in $K(\alpha_1, \ldots, \alpha_s)[x]$ for all $0 \leq s \leq m$.

Proof. We write L for the splitting field of $p(x)$ over K. Because we form L by adding all roots of $p(x)$ to K, we can write $[L\colon K] = [L\colon K(\alpha_1, \ldots, \alpha_m)] \ldots [K(\alpha_1, \alpha_2)\colon K(\alpha_1)][K(\alpha_1)\colon K]$ because of lemma 2.22. We know because of proposition 2.26 that the number of elements in the Galois group is equal to the degree of the extension. We see that $[K(\alpha_1, \ldots, \alpha_s, \alpha_{s+1})\colon K(\alpha_1, \ldots, \alpha_s)] = n-s$, because $p_s(x)$ is irreducible and of degree $n-s$, so $[L\colon K(\alpha_1, \ldots, \alpha_m)] \ldots [K(\alpha_1, \alpha_2)\colon K(\alpha_1)][K(\alpha_1)\colon K] = [L\colon K(\alpha_1, \ldots, \alpha_m)] \cdot (n-m) \ldots (n-1)n \geq n(n-1)\ldots(n-m)$, so we are done. □

Now we will look at $Tx + Tx^q + x^{q^2}$. We can see that $T + Tx^{q-1} + x^{q^2-1}$ is irreducible because of Eisenstein. We also see that if we determine the number of elements in the Galois group of $T + Tx + x^{q+1}$, then the number of elements in the Galois group of $T + Tx^{q-1} + x^{q^2-1}$ is at least equal to the number of elements in the Galois group of $T + Tx + x^{q+1}$ times $q-1$. This is the case because we stay in the subfield of the splitting field of $T + Tx^{q-1} + x^{q^2-1}$ by first making the splitting field of $T + Tx + x^{q+1}$, and then taking the $q-1$ root of one of the roots of $T + Tx + x^{q+1}$, and since this gives an extension of degree $q-1$ and the number of elements in the Galois group is equal to the degree of the extension of the splitting field over the ground field, this indeed gives the right lower bound on the number of elements in the Galois group.
So we want to show that the number of elements in the Galois group of the splitting field of $T + Tx + x^{q+1}$ over k is at least equal to $q(q+1)(q-1)$.

Lemma 5.3. *The Galois group of the splitting field of the polynomial $T + Tx + x^{q+1}$ over k contains at least $(q+1)q(q-1)$ elements.*

Proof. $T + Tx + x^{q+1}$ is irreducible over $k(x)$ because of Eisenstein. Suppose that we have $\lambda \in \overline{k}$ such that $T + T\lambda + \lambda^{q+1} = 0$. Then we see that $T = -\frac{\lambda^{q+1}}{\lambda+1}$, so $T \in \mathbb{F}_q(\lambda)$, so $\mathbb{F}_q(T, \lambda) = \mathbb{F}_q(\lambda)$. We see that λ is transcendental over $\mathbb{F}_q$, because otherwise T would be algebraic, see proposition 2.25, and this isn't the case. So we can substitute $T = -\frac{\lambda^{q+1}}{\lambda+1}$, and look at our polynomial as if it has coefficients in $\mathbb{F}_q(\lambda) \cong \mathbb{F}_q(T)$.
We need to determine whether $\frac{-\frac{\lambda^{q+1}}{\lambda+1} - \frac{\lambda^{q+1}x}{\lambda+1} + x^{q+1}}{x-\lambda}$ is irreducible. For the irreducibility over $\mathbb{F}_q(\lambda)[x]$ it doesn't matter if we multiply with $\lambda + 1$. We get

$$\frac{-\lambda^{q+1} - \lambda^{q+1}x + \lambda x^{q+1} + x^{q+1}}{x-\lambda} = \frac{x^{q+1} - \lambda^{q+1}}{x-\lambda} + x\lambda\frac{x^q - \lambda^q}{x-\lambda}$$

Now we substitute $y = x - \lambda$, then we get the following using the freshman's dream

$$\begin{aligned}
\frac{x^{q+1} - \lambda^{q+1}}{x-\lambda} + x\lambda\frac{x^q - \lambda^q}{x-\lambda} &= \frac{(y+\lambda)^{q+1} - \lambda^{q+1}}{y} + (\lambda y + \lambda^2)\frac{(y+\lambda)^q - \lambda^q}{y} \\
&= \frac{(y+\lambda)(y^q + \lambda^q) - \lambda^{q+1}}{y} + (\lambda y + \lambda^2)\frac{y^q + \lambda^q - \lambda^q}{y} \\
&= \frac{y^{q+1} + \lambda y^q + y\lambda^q + \lambda^{q+1} - \lambda^{q+1}}{y} + \lambda y^q + \lambda^2 y^{q-1} \\
&= y^q + \lambda y^{q-1} + \lambda^q + \lambda y^q + \lambda^q y^{q-1} \\
&= (1+\lambda)y^q + (\lambda + \lambda^2)y^{q-1} + \lambda^q
\end{aligned}$$

This polynomial is irreducible over $\mathbb{F}_q[\lambda][x]$ because of reverse Eisenstein with $\lambda + 1$, so our polynomial is also irreducible over $\mathbb{F}_q(\lambda)[x]$.

To determine the factorization of $(1+\lambda)y^q + (\lambda+\lambda^2)y^{q-1} + \lambda^q$ over k, we can just as well look at the factorization with y substituted by λz. When we do this substitution we get $(1+\lambda)\lambda^q z^q + (1+\lambda)\lambda^q z^{q-1} + \lambda^q$. The factorization over $\mathbb{F}_q(\lambda)$ stays the same if we divide by λ, so we get $(1+\lambda)z^q + (1+\lambda)z^{q-1} + 1$. Suppose that $\mu \in \overline{k}$ such that $(1+\lambda)\mu^q + (1+\lambda)\mu^{q-1} + 1$, then $1+\lambda = -\frac{1}{\mu^q+\mu^{q-1}}$, so $\lambda \in \mathbb{F}_q(\mu)$, so $\mathbb{F}_q(\lambda,\mu) = \mathbb{F}_q(\mu)$. So we can again substitute $\lambda = -\frac{1}{\mu^q+\mu^{q-1}} - 1$ and look at our polynomial as if it has coefficients $\mathbb{F}_q(\mu)$.
So we need to determine whether

$$\frac{-\frac{z^q}{\mu^q+\mu^{q-1}} - \frac{z^{q-1}}{\mu^q+\mu^{q-1}} + 1}{z-\mu}$$

is irreducible over $\mathbb{F}_q(\mu)[x]$. We can just as well multiply with $-(\mu^q+\mu^{q-1})$ and we get

$$\begin{aligned}\frac{z^q + z^{q-1} - \mu^q - \mu^{q-1}}{z-\mu} &= \frac{z^q-\mu^q}{z-\mu} + \frac{z^{q-1}-\mu^{q-1}}{z-\mu} \\ &= z^{q-1} + \mu z^{q-2} + \ldots + \mu^{q-1} + z^{q-2} + \mu z^{q-3} + \ldots + \mu^{q-2} \\ &= z^{q-1} + (\mu+1)z^{q-2} + (\mu^2+\mu)z^{q-3} + \ldots + \mu^{q-2}(\mu+1)\end{aligned}$$

This polynomial is irreducible over $\mathbb{F}_q[\mu][x]$ because of Eisenstein with $\mu+1$, so it is also irreducible over $\mathbb{F}_q(\mu)[x]$, so with proposition 5.2 we are done. □

Theorem 5.4. *Let L be the splitting field over $Tx + Tx^q + x^{q^2}$ over k. Then $Gal(L/k) \cong GL_2(A/TA)$.*

Proof. We know that the Galois group of the splitting field of $T + Tx + x^{q+1}$ over k contains at least $(q+1)q(q-1)$ elements, so adding the roots of this polynomial gives an extension of k of degree at least $(q+1)q(q-1)$. In this extension are only elements that have a minimal polynomial over k of degree at most $q+1$. We know that $T + Tx^{q-1} + x^{q^2-1}$ is irreducible, so when we add a root of this polynomial to the splitting field of $T + Tx + x^{q+1}$ over k we get an extension of degree at least $\frac{q^2-1}{q+1} = q-1$. So $|\mathrm{Gal}(L/k)| = [L:k] \geq q(q-1)^2(q+1)$.
We also know that $\mathrm{Gal}(L/k)$ maps injectively into $GL_2(A/TA)$ and $GL_2(A/TA)$ has $q(q-1)^2(q+1)$ elements, so $|\mathrm{Gal}(L/k)| = q(q-1)^2(q+1)$ and we indeed have $\mathrm{Gal}(L/k) \cong GL_2(A/TA)$. □

References

[1] Frits Beukers et al. *Rings and Galois Theory.* 2017.

[2] Wikipedia contributors. Galois theory — wikipedia, the free encyclopedia, 2017. [Online; accessed 14-January-2018].

[3] Michael Rosen. *Number Theory in Function Fields.* Springer-Verlag, New York Berlin Heidelberg, 1 edition, 2002.