Universiteit Utrecht

Opleiding Wiskunde

Galois theory for inseparable extensions

Constructing a Galois-type correspondence for finite purely inseparable field extensions of exponent one

Bachelor Thesis

Lara Timmers

Figure 1: "Improved Orion Nebula" by Abner, 2017, on allrgb.com, which has exactly one pixel for every RGB colour.

Supervisor:

Dr. Gijs Heuts First Supervisor

Institute for Mathematical Sciences

June 16th, 2024

Contents

1 Introduction

In field theory, one of the most elegant theorems is the fundamental theorem of Galois theory, which was originally introduced by Évariste Galois. It states a connection between the theory of field extensions and group theory, which makes it less complicated to study the structure of certain extensions. In the course 'Fields en Galois Theory' we have seen that such extensions must be finite, normal and separable. The latter means that the minimal polynomial of any element in the extension can be factored into distinct linear terms. The theorem then states that for such extensions, there is a one-to-one correspondence between intermediate fields and subgroups of its group of automorphisms, where a subgroup corresponds to its fixed field, and an intermediate field corresponds to the subgroup of automorphisms that fix that field [2]. The diagram below shows the correspondence more clearly.

$$\left\{\begin{array}{c}\text{intermediate field}\\ E\end{array}\right\} \longrightarrow \left\{\begin{array}{c}\text{elements of the}\\ \text{automorphism}\\ \text{group that fix } E\end{array}\right\}$$

$$\left\{\begin{array}{c}\text{the fixed field of}\\ H\end{array}\right\} \longleftarrow \{\quad \text{subgroup } H \quad\}$$

In Galois theory, it is very important that the extension is separable. In practice, applying the theorem means finding maps that permute the roots of the minimal polynomial of the extension. If a polynomial is inseparable, then roots appear multiple times. This causes the correspondence to collapse, because the index of the extension is larger then the cardinality of its automorphism group, among other, quite equivalent, reasons.

The question naturally arises if there is a similar theory for the case that the extension is inseparable. The goal of this thesis is to treat that case, and develop a correspondence similar in nature to Galois theory. For this, we use the book 'Lectures in Abstract Algebra' written by N. Jacobson [1], who developed this theory in the 20th century. The theory that we will study is about purely inseparable extensions of exponent one. The restriction of having just exponent one makes it so that the subject is accessible. There is theory for higher exponents out there, but that goes beyond this thesis. With these requirements we will formulate a Galois-type correspondence between intermediate fields and subalgebras of the restricted p-Lie algebra of derivations. In this correspondence, the restricted p-Lie algebra of derivations plays a similar role as the group of automorphisms that fix the base field of a Galois extension in Galois theory. The theory of derivations will be discussed in chapter two of this thesis. There, we define the restricted p-Lie algebra of derivations and discuss the field of D-constants, which has quite a similar role to that of the fixed field of an automorphism subgroup in Galois theory. In the third chapter we state the main theorem of the Galois-type correspondence and give some examples. We then prove that theorem after discussing the notion of p-independence and stating some needed lemmas.

Finite purely inseparable field extensions are finite extensions for which the minimal polynomial of every element is not separable. This narrows down the type of fields that we can apply the Galois-type correspondence to. To illustrate, a perfect field always has separable extensions, so such perfect fields are ruled out. This includes finite fields and fields with a characteristic of zero, so we will always be discussing infinite fields of characteristic p for some prime. An example of such fields are fields of fractions, like

$$\mathbb{F}_2(x),$$

which has elements of the form $f(x)/g(x)$ with $f(x), g(x)$ polynomials over $\mathbb{F}_2$. In this example the characteristic is equal to $p = 2$.

Preliminaries

We expect the reader to be familiar with groups, rings, fields and Galois theory, as given in the courses 'Fields en Galois Theory' and 'Introduction to Groups and Rings', for example. These subjects can also be consulted in the book 'Abstract Algebra' by D.S. Dummit and R.M. Foote [2].

2 Derivations

In this chapter we will discuss derivations, which will turn out to be very useful for the study of purely inseparable extensions. To study the properties of derivations we relate them to homomorphisms between an algebra and its dual space. We introduce D-constants, the elements that are "fixed" by a derivation D. We will also discuss extensions of derivations and the structure on all derivations of an algebra. Lastly, we take a look at restricted p-Lie algebras and specifically the restricted p-Lie algebra of derivations. With this, we will have developed most of the tools needed to state the Galois-type correspondence for purely inseparable extensions of exponent one in the next chapter.

Recall that an algebra A over a base field F is a vector space over F equipped with a distributive and associative binary operation $\cdot : A \times A \to A$ such that $(ax) \cdot (by) = (ab)(x \cdot y)$ for all $a, b \in F$ and $x, y \in A$. For example, the field of polynomials over F, written as $F[x]$, is an algebra over F. We may now define the concept of a derivation.

Definition 2.1. *Let U be a subalgebra of A over a base field F. A derivation D of U into A is an F-linear mapping $U \to A$ such that for all $a, b \in U$*

$$D(ab) = (Da)b + a(Db). \tag{1}$$

If $U = A$ then we say that D is a derivation in U (or A).

Intuitively, a derivation is am F-linear map that satisfies the Leibniz identity. The classical derivative map $f(x) \to f'(x)$ is an example of a derivation in $F[x]$. Notice that this derivative satisfies the product rule, which is the same as the Leibniz rule, and that its linearity is trivial. Notice that the set of derivations of an algebra is also a module over that algebra, since it includes the zero-mapping, which is F-linear and satisfies the Leibniz rule.

2.1 Dual space

In this section we relate the notion of derivations to homomorphisms. It gives us a way to derive statements on derivations without having to work with them, but instead their respective homomorphism. Consider the algebra $F[x]/(x^2)$ over a base field F. Then given the coset $t = x + \langle x^2 \rangle$, we have a basis for $F[x]/(x^2)$ given by $(1, t)$ where $t^2 = 0$. We use this structure to define the dual numbers of an algebra.

Definition 2.2. *The algebra of dual numbers of an algebra A over F is defined as $A \otimes F[x]/(x^2)$.*

Notice that A and $F[x]/(x^2)$ are subalgebras of this algebra by considering the elements $a \otimes 1, a \in A$ and $1 \otimes u, u \in F[x]/(x^2)$ respectively. We can define a mapping $s = s(D)$ for any derivation D in the algebra A into the algebra of dual numbers in the following way,

$$s : A \to A \otimes F[x]/(x^2), a \mapsto s(a) \coloneqq a + (Da)t.$$

Let's introduce the projection of $A \otimes F[x]/(x^2)$ into A defined by $\pi : a + bt \mapsto a$. This is the identity mapping on the subalgebra A and clearly a homomorphism because $t^2 = 0$. An overview of the mappings $s(D)$ and π is depicted below.

$$A \xrightarrow{s(D)} A \otimes F[x]/(x^2) \xrightarrow{\pi} A$$

We introduce a theorem that relates derivations to homomorphisms, which will be useful later since we will only have to consider homomorphisms.

Theorem 2.3. *Let A be an algebra over F and D a derivation in A, then $s(D)$ is a homomorphism of A into its algebra of dual numbers $A \otimes F[x]/(x^2)$. Conversely, any homomorphism s of A into $A \otimes F[x]/(x^2)$ such that $\pi(s(a)) = a$ for all $a \in A$, is of the form $a \mapsto a + (Da)t$ for some derivation D in A.*

Proof. Firstly, we will to prove that s is a homomorphism. For any $a, b \in A$ and $u \in F$, we may write

because of the F-linearity of D that

$$\begin{aligned} s(ua+b) &= ua + b + (D(ua+b))t \\ &= ua + b + (uDa + Db)t \\ &= ua + u(Da)t + b + (Db)t \\ &= u(a + (Da)t) + b + (Db)t \\ &= us(a) + s(b). \end{aligned}$$

So it follows that s is a homomorphism. To prove the second statement, let s be any homomorphism of A into $A \otimes F[x]/(x^2)$ such that $\pi(s(a)) = a$ for all $a \in A$. Since $\pi(s(a)) = a$ for $a \in A$, we have $s(a) = a + bt$ for $b \in A$ uniquely determined by a. We call this unique determination the map

$$D : A \to A,\ a \mapsto b.$$

We show that this map is a derivation. It is clearly F-linear since s is. Because s is a homomorphism and $t^2 = 0$ we have

$$\begin{aligned} s(ab) &= s(a)s(b), \\ ab + (D(ab))t &= ab + (a(Db) + (Da)b)t, \end{aligned}$$

so D satisfies the Leibniz identity. We conclude that s is of the form $a \mapsto a + (Da)t$ for a derivation D. □

Here we see that we can relate every derivation to a homomorphism to the algebra of dual numbers. A concrete example of linking derivations to homomorphisms, but not in the algebra of dual numbers, is given in the following example.

Example 2.4. Let A be an algebra. A map D is a derivation in A if and only if the map

$$\phi\colon A \to A_2, a \mapsto \begin{pmatrix} a & Da \\ 0 & a \end{pmatrix} \tag{2}$$

is a homomorphism, where A_2 is the algebra of 2×2 matrices over A.

Proof. First, assume that D is a derivation in A. Then

$$\begin{aligned} \phi(a)\phi(b) &= \begin{pmatrix} a & Da \\ 0 & a \end{pmatrix} \begin{pmatrix} b & Db \\ 0 & b \end{pmatrix} \\ &= \begin{pmatrix} ab & a(Db) + (Da)b \\ 0 & ab \end{pmatrix} \\ &= \begin{pmatrix} ab & D(ab) \\ 0 & ab \end{pmatrix} = \phi(ab), \end{aligned}$$

per Leibniz rule. So ϕ is a homomorphism. On the contrary, if ϕ is a homomorphism then $D(ab) = a(Db) + (Da)b$ according to the calculation above. From linearity of A_2 it is clear that D is linear if ϕ is a homomorphism, so then D is indeed a derivation. □

2.2 D-constants

In this subsection we introduce the D-constants of a derivation and their properties for different cases of the algebra the derivation is in. The role of D-constants is strongly related to the role that fixed fields have in Galois theory.

Definition 2.5. *An element $a \in A$ is called a D-constant for a derivation D in A if $Da = 0$. The D-constants for a set $\mathcal{D}$ of derivations in A are the elements in A that are D-constants for all $D \in \mathcal{D}$.*

For example, 1 is a D-constant of any derivation. For the derivation in the ring polynomials over a field F that maps $f(x) \mapsto f'(x)$, any element in F is a D-constant. Recalling back to the dual space $A \otimes F[x]/(x^2)$, we see that a is a D-constant if and only if $s(a) = a$, with $s = s(D)$ defined earlier. You could say that the D-constants are fixed by $s(D)$, and thus this notion is quite similar to that of

a fixed field. It also follows rather immediately from the definition that the set of D-constants forms a subalgebra of A.

Let's look at the case that A is a commutative algebra. Then the Leibniz rule implies for $a = b$ that

$$(Da^2) = (Da)a + a(Da) = 2a(Da).$$

For any power it follows with induction that $D(a^n) = na^{n-1}(Da)$. So if F has characteristic p, then $D(a^p) = 0$ for all $a \in A$. In other words, then every p-th power is a D-constant for any derivation in A. Consider the case that the algebra $A = P$ is a field over a base field F. We propose that the D-constants of a derivation D in such an algebra is a subfield of P.

Proposition 2.6. *If $A = P$ over F is a field, then the D-constants of a derivation D in P form a subfield E of P.*

Proof. It is clear that the D-constants are a subset of P. Notice for $u \in F, a \in P$ that $D(au) = (Da)u + a(Du)$ because of the Leibniz rule, but also $D(au) = (Da)u$ because of the F-linearity of D. Thus $Du = 0$ for all elements u in F. We conclude that the set of D-constants contains F, and thus is nonempty. If $a, b \in P$ are D-constants it is easy to check that $a - b$ and a/b if $b \neq 0$ are also D-constants. Since the D-constants satisfy the subfield criterion we conclude that they are a subfield of P. □

In the future it will be useful to be able to refer to the D-constants as some subfield E/F of P/F. Remark that in the proof of proposition 2.6 we've come across the following: for a derivation D in P/F, the base field F is always D-constant. This follows from the F-linearity of D and the Leibniz rule.

2.3 Restricted Lie algebra of derivations

In Galois theory the main correspondence is between automorphism subgroups and their fixed fields. Since the automorphism group for the case of inseparable extensions is trivial, this won't suffice. The structure that takes a similar role as the automorphism groups is the restricted p-Lie algebra of derivations. In this subsection we introduce what this means so that we have another concept needed to state the theorem of the Galois correspondence for purely inseparable extensions of exponent one.

We start with describing the structure of a restricted p-Lie algebra. Consider the field P of characteristic $p \neq 0$, without necessarily specifying P as an extension of some other base field. We give the following definition.

Definition 2.7. *A set of endomorphisms $\mathcal{E}$ of P is called a restricted p-Lie algebra if it satisfies the following properties:*

1. *E is closed under addition*
2. *E is closed under multiplication by elements in P*
3. *E is closed under the Lie commutator, so for $E_1, E_2 \in \mathcal{E}$ we have that $E_1E_2 - E_2E_1 \in \mathcal{E}$.*
4. *E is closed under p-th powers*

The first two properties say that such an algebra is a vector space. So in other words, a restricted p-Lie algebra is a vector space over P of endomorphisms of $(P, +)$ closed under the Lie commutator and p-th powers. If we take the field P as an extension of a base field F, we can talk about derivations in P/F. One example of a restricted p-Lie algebra is the restricted p-Lie algebra of derivations. Its structure will be enough for the correspondence later on. We claim that the set of derivations in P is indeed a restricted p-Lie algebra in the following proposition.

Proposition 2.8. *The set $\mathcal{D}$ of derivations in P over F is a restricted p-Lie algebra.*

Proof. Notice that any derivation in P is also an endomorphism of the space P with just the addition operator, $(P, +)$. So we can consider $\mathcal{D}$ as the set of endomorphism of $(P, +)$ such that $D(ab) = (Da)b + a(Db)$ for all $a, b \in P$. We've also seen already that $\mathcal{D}$ is a module over P. We are left to check property 3 and 4 of 2.7. Take any $D_1, D_2 \in \mathcal{D}$. For the third, we need to show that $D \coloneqq D_1D_2 - D_2D_1$

is also a derivation in P. Fist we prove that D is F-linear, which follows by applying the F-linearity of D_1 and D_2. Take $a, b \in P$ and $r \in F$, then

$$\begin{aligned} D(a+rb) &= (D_1D_2 - D_2D_1)(a+rb) \\ &= D_1D_2(a+rb) - D_2D_1(a+rb) \\ &= D_1D_2a + D_1D_2(rb) - D_2D_1a - D_2D_1(rb) \\ &= Da + D(rb) = Da + r(Db), \end{aligned}$$

so D is F-linear. Now we want to show that D follows the Leibniz rule. Because D_1 and D_2 do, we may write for $a, b \in P$

$$\begin{aligned} D(ab) &= (D_1D_2 - D_2D_1)(ab) \\ &= (D_1D_2)(ab) - (D_2D_1)(ab) \\ &= D_1(D_2(ab)) - D_2(D_1(ab)) \\ &= D_1((D_2a)b + a(D_2b)) - D_2((D_1a)b + a(D_1b)) \\ &= D_1((D_2a)b) + D_1(a(D_2b)) - D_2((D_1a)b) - D_2(a(D_1b)) \\ &= (D_1D_2a)b + (D_2a)(D_1b) + (D_1a)(D_2b) + a(D_1D_2b) \\ &\quad - (D_2D_1a)b - (D_1a)(D_2b) - (D_2a)(D_1b) - a(D_2D_1b) \\ &= (D_1D_2a)b + a(D_1D_2b) - (D_2D_1a)b - a(D_2D_1b). \end{aligned}$$

These terms collapse with F-linearity and the definition of D to the expression

$$D(ab) = (Da)b + a(Db),$$

so D is a derivation and $\mathcal{D}$ is closed under the Lie commutator. We are left to prove that $\mathcal{D}$ is closed under p-th powers. Notice that the composition of multiple F-linear maps is still F-linear, so any $D \in \mathcal{D}$ gives that D^p is F-linear. Now for the last part we have to show that D^p follows the Leibniz rule. We propose the following higher order Leibniz formula

$$D^n(ab) = \sum_{i=0}^{n} \binom{n}{i} (D^i a)(D^{n-i} b),$$

for $n \in \mathbb{N}_+$. This can be proved with induction, but we'll skip over it because it is rather trivial. Now notice that $\binom{p}{i} a = 0$ for $i < p$ and $a \in P$, so what is left of the higher order Leibniz formula for $n = p$ is

$$D^p(ab) = (D^p a)b + a(D^p b),$$

so it follows that D^p satisfies the Leibniz rule. We conclude that the set of derivations in P/F is a restricted p-Lie algebra. □

Since this notion is well-defined, we will call this the restricted p-Lie algebra of derivations in P.

3 Galois-type correspondence

This chapter we study the main goal of this thesis: constructing a Galois-type correspondence for the case of finite purely inseparable field extensions of exponent one. We state the theorem and give some examples. Then we prove it step by step and discuss some properties of the correspondence. Throughout we discuss how this correspondence is related to that of the basic Galois theory and their differences.

Let's first define what it means for a field extension to be of exponent one. Recall for example from [2] the following theorem.

Theorem 3.1. *An algebraic field extension E/F with characteristic p is purely inseparable if and only if for all $\alpha \in E$, there exists $n \in \mathbb{N}$ such that $\alpha^{p^n} \in F$.*

Because this n is well-defined for purely inseparable extensions, we may now define the exponent.

Definition 3.2. *The exponent of a purely inseparable field extension E/F of characteristic $p \neq 0$ is the minimal $n \in \mathbb{N}$ such that*

$$e^{p^n} \in F,$$

for all $e \in E$.

In this thesis, we study the case where $n = 1$. From now on we will only be talking about fields of characteristic $p \neq 0$. Also consider from now on the purely inseparable field extension P/F of exponent ≤ 1, then any $e \in P/F$, $e^p \in F$. We will formulate a proposition that states that any intermediate field of P/F is another purely inseparable field extension of F of exponent ≤ 1.

Proposition 3.3. *Let E/F be any subfield of P/F. Then E is purely inseparable of exponent ≤ 1 over F.*

Proof. Consider a derivation

$$D : E/F \to P/F.$$

We want to show that for any $e \in E/F$, $e^p \in F$. We do this by showing that the map D is the same as a derivation from $E/F(E^p)$ to $P/F(E^p)$, so it follows that $E^p \subseteq F$. Denote the set of all D-constants by Δ. By proposition 2.6 this is a subfield of E/F. We claim that D is also a derivation from E/Δ into F/Δ, because if we take $\delta \in \Delta$ and $e \in E$, then $D(\delta e) = \delta(De) + (D\delta)e = \delta(De)$, so D is Δ-linear. Notice that the set E^p is always D-constant because

$$De^p = pe^{p-1}De = 0,$$

for all $e \in E$, hence $F(E^p) \subseteq \Delta$. We now conclude that D is also a derivation from $E/F(E^p)$ into $P/F(E^p)$. The other way around, that any derivation from $E/F(E^p)$ into $P/F(E^p)$ is also a derivation like D, follows trivially because $F \subseteq F(E^p)$. We conclude that any derivation like D is equal to a derivation from $E/F(E^p)$ into $P/F(E^p)$, so F is replaceable by $F(E^p)$. Hence $e^p \in F$ for all $e \in E/F$.

□

This will make our main theorem in this thesis more powerful and generalized, since we won't have to specify further what kind of subfields the Galois-type correspondence holds for, as you will see in the next section.

3.1 Theorem and examples

In this section we present the main theorem of this thesis, which gives a Galois-type correspondence for the case of finite purely inseparable field extensions of exponent one. We will also discuss some examples. In the next section you may find the proof.

Theorem 3.4. *Let P over F be a finite purely inseparable field extension of exponent ≤ 1 and $\mathcal{D}$ the restricted p-Lie algebra of derivations in P/F. Then there is a bijection*

$$\left\{ \begin{array}{c} \text{subfields } E \text{ of } P \\ \text{containing } F \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{subalgebras } D \text{ of} \\ \mathcal{D} \end{array} \right\} \tag{3}$$

given by the correspondences

$$\left\{ \begin{array}{c} \text{intermediate field} \\ E \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{the restricted} \\ p\text{-Lie algebra of} \\ \text{derivations in} \\ P/E \end{array} \right\} \tag{4}$$

$$\left\{ \begin{array}{c} \text{the field of} \\ D\text{-constants} \end{array} \right\} \longleftarrow \{ \quad \text{subalgebra } D \quad \} \tag{5}$$

which are each-others inverses.

Later this section, we will talk about more of the properties of this correspondence. But first, we will give some examples of theorem 3.4.

Example 3.5 (Extension of dimension p). Take for instance the field of fractions $P = \mathbb{F}_p(t)$ as an extension of the field of fractions $F = \mathbb{F}_p(x)$, where $t^p = x$. In other words, we extend the field F with the p-th root of x. It is clear that this is an extension of finite dimension p. Also, for any $f(t)/g(t) \in P$ we see with the Frobenius homomorphism that

$$(f(t)/g(t))^p = f(t^p)/g(t^p) = f(x)/g(x) \in P$$

because for all coefficients $a^p = a$. Since $f(x)/g(x) \in F$, it follows that P/F is an extension of exponent ≤ 1. We conclude that P/F is a finite purely inseparable field extension of exponent ≤ 1, so we may apply theorem 3.4. Notice also that the exponent is certainly not 0, because $t \notin P$.

We would like to find the restricted p-Lie algebra of derivations in P/F. Consider the derivation given by

$$D_t \colon P/F \to P/F, \quad f(t) \mapsto f'(t),$$

with $f'(t)$ being the common derivative in t. Then for any $f \in F$ we see with the chain rule that

$$D_t(f(x)) = D_t(f(t^p)) = f'(t^p)pt^{p-1} = 0,$$

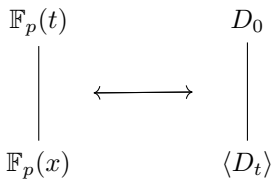
so elements of F are D_t-constants. Then we see with the Leibniz rule that D_t is F-linear:

$$f \in F, g \in P \quad \Longrightarrow \quad D_t(fg) = fD_t(g) + D_t(f)g = fD_t(g).$$

Since any p-th power of D_t and derivation of the form $aD_t, a \in F$ is also a derivation, we conclude that D_t is an element of $\mathcal{D}$ and that $\mathcal{D}$ is at least generated by D_t. To know whether $\mathcal{D} = \langle D_t \rangle$ we refer to corollary 3.12 of theorem 3.11 that gives us information about the degree of $\mathcal{D}$ as a vector space over P, namely

$$[\mathcal{D} : P] = 1,$$

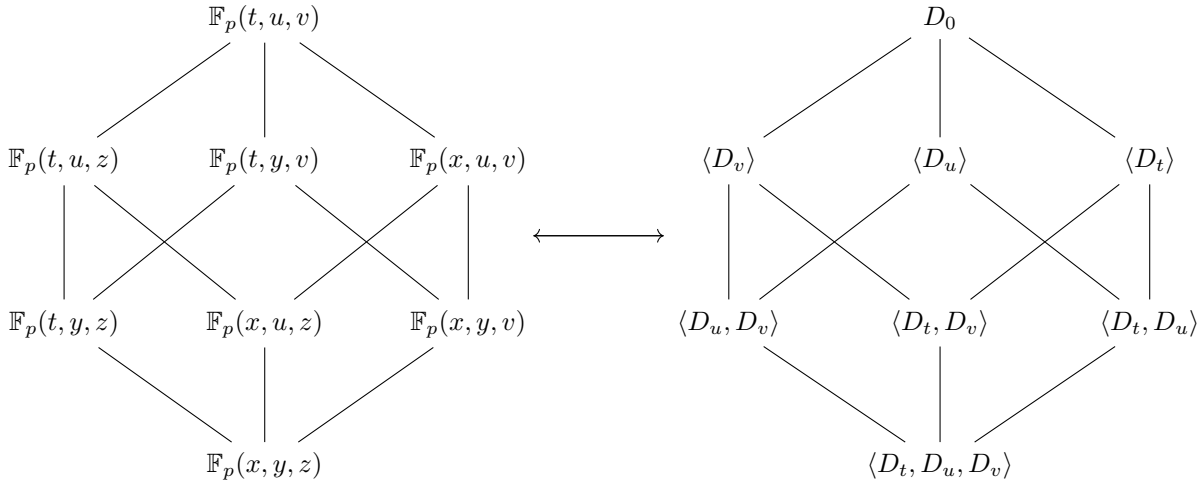
in our case. Since $\langle D_t \rangle$ also has degree one over P as a vector space, it follows that $\langle D_t \rangle$ equals $\mathcal{D}$. The only restricted p-Lie subalgebra of $\langle D_t \rangle$ is the trivial one, since for example, it must be closed under p-th powers. From the correspondence it then is clear that there are no subfields E of P/F such that $P \neq E \neq F$. The diagram of the correspondence then looks as follows:



This diagram represents with the correspondences of the theorem that the restricted p-Lie algebra of derivations in P/F and P/P are $\langle D_t \rangle$ and D_0, the trivial algebra of one derivation that maps everything to zero, respectively. This is what we would have expected, since the only derivations in P over P must send every element to zero as all elements of P are D-constants.

We will now discuss another example that is strongly related to the previous one, but uses more variables. This make the correspondence diagram more interesting, as the extension now contains intermediate fields as well.

Example 3.6 (Extension of dimension p^3). Similarly to the previous example we consider the field of fractions $P = \mathbb{F}_p(t, u, v)$ as an extension of $F = \mathbb{F}_p(x, y, z)$, where $t^p = x$, $u^p = y$ and $v^p = z$. In other words, we extend $\mathbb{F}_p(x, y, z)$ with the three p-th roots of the variables. Just as before, it follows from the Frobenius homomorphism that this is an extension of exponent ≤ 1. Since $F \neq P$, we see with 3.1 that it is a purely inseparable extension of exponent ≤ 1. The restricted p-Lie algebra of P/F is the one generated by derivations over several the variables, so $\mathcal{D} = \langle D_t, D_u, D_v \rangle$. Given below is a diagram of a part of the correspondence, for the subalgebras that are generated by different combinations of the derivation maps D_i, with $i \in \{t, u, v\}$.



Consider $\langle D_t \rangle$ for example. According to the theorem, it is the restricted p-Lie algebra of derivations in $\mathbb{F}_p(t, u, v)$ over $E \coloneqq \mathbb{F}_p(x, u, v)$. Similarly to the previous example, we see that any $f(x, u, v) \in E$ is a D-constant of all derivations in $\langle D_t \rangle$. If $g(t, u, v) \in F$ but $g(t, u, v) \notin E$ then there are terms within the polynomial that have a root of x, so $Dg \neq 0$. We illustrate this with the following calculation for $p = 5$.

$$\begin{aligned} g(t, u, v) &\coloneqq 3t^2u + 2uv, \\ D_t g(t, u, v) &= 6tu \neq 0, \end{aligned}$$

but if the power is $t^5 = x$ in the polynomial instead, then $g \in E$ and

$$D_t g(t, u, v) = 3 \cdot 5t^4 u = 0.$$

Notice that these are not all the subalgebras, since $D_t + D_u$ or $D_u D_v$ also generate subalgebras. The relations between the subalgebras and intermediate fields in the diagram follow from reapplying the theorem. For example, for $P = \mathbb{F}_p(t, u, z)$ over F the proper intermediate fields are $\mathbb{F}_p(t, y, z)$ and $\mathbb{F}_p(x, u, z)$. Then the restricted p-Lie algebras of P over each intermediate field is as given in the diagram above, except $D_v = D_0$ practically in this case, because there is no v to speak of at all.

We can ask ourselves what would happen if the extension is not purely inseparable of exponent one. In the case that the exponent is zero, then $P = F$ so there isn't really any extension to speak of. If the extension is not purely inseparable, we have that the exponent is not well-defined, and we can't apply the theory that follows from having an exponent of one which will be used in the next subsection for the proof.

3.2 Proof

In this subsection we will give the proof for theorem 3.4. The main steps of the proof include showing that the mappings described in the theorem are well-defined and in fact each-others inverses. But first, we need to do some preparations. One of the important lemmas for the main proof claims that a derivation of an extended field is uniquely determined by how it acts on a p-basis of the extension. This gives us information about mapping a field extension to a restricted p-Lie algebra of derivations. Another important building block is Jacobson's theorem in [1], which answers the question "starting with a restricted p-Lie algebra of derivations, what can we say about extensions?".

3.2.1 p-independence

We start with defining the notion of p-(in)dependence, then we may define a p-basis for an extension.

Definition 3.7. *Let P/F be a purely inseparable extension. An element $a \in P$ is p-dependent in P/F on some subset $S \subseteq P$ if $a \in F(P^p)(S)$. In other words, this holds when a is linearly dependent over F on S and p-th powers of P. We call $a \in P$ p-independent in P/F on a subset $S \subseteq P$ if it is not p-dependent in P/F on S.*

Intuitively then, an element is p-independent if it is regularly independent and independent on p-th powers of P. In the definition above S is like a basis, but without necessarily having mutual p-independence for the elements in S, which is what we would like if we had an actual basis. This brings us to define what it means for a set to be p-independent 'on itself'.

Definition 3.8. *A subset $S \subseteq P$ is p-independent on P/F if for all $s \in S$, s is p-independent in P/F on $S - \{s\}$.*

We illustrate this concept more with the following example.

Example 3.9. Consider a field F and an element ρ such that $\rho^p \notin F$ and $\rho^{p^2} \in F$. To know if the subset $\{\rho^p\} \subseteq F(\rho^p)$ is p-dependent in $F(\rho^p)/F$, we need to check whether $\rho^p \in F(F(\rho^p)^p)$ according to the definitions above. However, $F(F(\rho^p)^p) = F(\rho^{p^2})$, because for any other $x \neq \rho^p, x \in F$ we have that $x^p = x$. Then because $\rho^{p^2} \in F$ we have that $F(\rho^{p^2}) \subseteq F$. Since $\rho^p \notin F$ we see that $\{\rho^p\}$ is p-independent on $F(\rho^p)/F$. With similar reasoning we see that $\{\rho^p\}$ is p-dependent on $F(\rho)/F$ because $\rho^p \in F(F(\rho)^p) = F(\rho^p)$.

The definition of a p-basis of an extension then follows naturally.

Definition 3.10. *A p-basis of an extension P over F is a p-independent subset $B \subseteq P$ such that every element of P is p-dependent on B. In other words, we have that $F(P^p)(B) = P$.*

The general basis theorem shows that such a basis always exists. Furthermore, it holds that any two p-bases always have the same cardinality. We will now introduce the lemma that states that a derivation between finitely extended fields is uniquely characterized by how it acts on a p-basis of the extension.

Lemma 3.11. *Let $F \subseteq E \subseteq P$ all be fields of characteristic $p \neq 0$ and say that P/F is a finite field extension of exponent ≤ 1. Let B be a p-basis of E over F and τ an arbitrary mapping of B to P. Then there exists exactly one derivation D of E/F into P/F such that $Db = \tau(b)$ for all $b \in B$.*

Proof. Because of lemma 3.3 we have that E is purely inseparable of exponent ≤ 1 over F. We discuss two cases. Firstly, the exponent of E/F is zero, then $a^{p^0} = a \in F$ for all $a \in E$. It follows that $E \subseteq F$ and thus $E = F$. Then the p-basis of E over F must be empty and the situation is rather trivial because the image of τ must be empty, and the only derivation allowed is the zero-mapping. We continue with the case that the exponent of E/F is equal to one. Since B is now nonempty, we can define $B = B_e + \{e\}$. Because of p-independence of the p-basis B, we have that $e \notin F(B_e)$. Since the extension is of exponent one, the minimal polynomial of e over $F(B_e)$ equals $x^p - c$ for some $c \in F(B_e)$. In other words, e is some p-th root of an element in $F(B_e)$. It then follows that there exists a derivation

$$D : F(B_e, e)/F(B_e) \to P/F,$$

that sends e to $\tau(e)$ and any element of $F(B_e)$ to zero. Notice that this derivation is uniquely determinant by the image of e under τ. We can do this for every element e_i of the basis, which will give us a set of

derivations

$$\{D_i : F(B_{e_i}, e_i)/F(B_{e_i}) \to P/F\}.$$

Consider the derivation defined by the addition of all D_i. It is clear that this is a well-defined derivation. Notice that $e_i \notin F(B_{e_i})$ is always sent to zero by any D_j when $i \neq j$, and when $i = j$ that e_i is send to $\tau(e_i)$. It follows that this derivation has the properties we are looking for. It is also a well-defined derivation of $F(B)/F = E/F$ into P/F. Since the basis unique, the resulting derivation is as well. □

A consequence of this lemma about the degree of the set of derivations as a vector space is given in the following corollary [1].

Corollary 3.12. *Denote by $D_F(E, P)$ the set of derivations of E/F into P/F and consider this as a vector space over P. Let B be the p-basis of E over F. If B is finite, then $[D_F(E, P) : P] = |B|$.*

Proof. Denote by T the set of mappings of B into P. We can consider T as a vector space over P by defining

$$(\tau_1 + \tau_2)b = \tau_1 b + \tau_2 b, \quad (\tau a)b = (\tau b)a,$$

for all $\tau, \tau_1, \tau_2 \in T, b \in B$ and $a \in P$. Define π to be the map from $D_F(E, P)$ into T by mapping any derivation to its restriction to B. Notice that this map is linear. Because $E = F(B)$ per definition, π is injective and lemma 3.11 shows that π is surjective. It follows that T and $D_F(E, P)$ are isomorphic. If $B = \{b_1, \ldots, b_m\}$ is finite with cardinality $|B| = m$, then we can construct a basis for $[\tau : P]$ with m amount of maps δ_i defined by $\delta_i(b_j) = \delta_i^j$, the Kronecker delta. We then see that $|B| = [T : P] = [D_F(E, P) : P]$, which concludes the proof. □

In other words, the corollary says that the index of the set of derivations of E/F into P/F as a vector space over P is equal to the cardinality of the p-basis if it is finite. Coming back to example 3.6, we see that the index of $\mathcal{D}$ over P should be equal to the cardinality of the p-basis of P/F. Since we extended F with one p-th root of an element in F the p-basis has size 1.

In the case that $P = E$ the lemma above has another interesting result which is stated in the next corollary.

Corollary 3.13. *Let P/F be a field extension. Then for all $a \in P$ it holds that $a \in F(P^p)$ if and only if $Da = 0$ for all derivations D in P/F.*

Proof. Notice that $a \in F(P^p)$ if and only if $a \notin B$, the p-basis of P over F. Assume first that $Da = 0$ for all derivations D in P/F. Then a can't be in B, because if that were the case we could construct a map $\tau : B \to P$ with $\tau(a) \neq 0$. The lemma then states that there exists a derivation such that $Da = \tau(a) \neq 0$, which is a contradiction. Thus if $Da = 0$ for all derivations D in P/F, then $a \notin B$, so $a \in F(P^p)$. Now assume that for all $a \in P$, $a \in F(P^p)$. Then a can be expressed as a linear combination of elements in F and p-th powers of elements in P. Since any derivation is an F-linear map and

$$D\rho^p = p\rho^{p-1} D\rho = 0,$$

for all $\rho \in P$ and derivations, it follows that $Da = 0$ for all derivations D in P/F. □

3.2.2 Jacobson's theorem

In this section we discuss two big theorems from [1]. Jacobson's theorem views the correspondences of theorem 3.4 from right to left, so to say. It starts with a restricted p-Lie algebra of derivations $\mathcal{D}$ and then implies that any derivation in P over $\mathcal{D}$-constants is again a derivation in $\mathcal{D}$. It is proved by considering the ring of endomorphisms of $(P, +)$, and uses the Jacobson-Bourbaki theorem. This theorem also implies the usual Galois correspondence for Galois extensions. We will only state the Jacobson-Bourbaki theorem and not prove it, since it is beyond the scope of this thesis. However, if you wish to read more about it, you can consult [1].

Theorem 3.14 (Jacobson-Bourbaki)**.** *Let P be a field, $\mathcal{E}$ the ring of endomorphisms of $(P, +)$. Let U a subring of $\mathcal{E}$ and a subspace of $\mathcal{E}$ as a vector space over P such that $[U : P] = n < \infty$. Let F be the subset of P of elements a such that $A(ab) = aA(b)$ for all $b \in P$ and $A \in U$. Then F is a subfield of P, $[P : F] = n$ and U is the complete set of all F-linear transformations of P over F.*

We will now move on to Jacobson's theorem, where we apply the theorem given above.

Theorem 3.15 (Jacobson)**.** *Let P be a field of characteristic $p \neq 0$ and $\mathfrak{D}$ a restricted p-Lie algebra of derivations in P such that its dimension over P as a vector space $[\mathfrak{D} : P] = m$ is finite, then:*

1. *if F is the subfield of $\mathfrak{D}$-constants, then P is purely inseparable of exponent less than one over F and its index over F equals $[P\colon F] = p^m$;*
2. *any derivation in P over F is contained in $\mathfrak{D}$;*
3. *if $\{D_i\}$ for $1 \leq i \leq m$ is a right basis for $\mathfrak{D}$ over P, then the set*

$$\{D_1^{l_1} D_2^{l_2} \cdots D_m^{l_m} \mid 0 \leq l_i < p\} \tag{6}$$

is a right basis for the ring of F-linear transformations of P over F considered as a right vector space over P.

Proof. This proof is based on the proof given in [1]. We won't show every detail, for that we refer to the source.

Firstly, we would like to apply the Jacobson-Bourbaki theorem 3.14. Recall that the elements of $\mathcal{D}$ can be considered as endomorphisms on $(P, +)$. Notice that it is also a vector space over P of finite dimensions m. Define a sub- vector space U of $\mathcal{D}$ over P by the set of linear combinations of the endomorphisms as given in equation (6). Then its dimensions over P as a vector space adheres to

$$[U : P] \leq p^m,$$

with equality if and only if the set in equation (6) is a p-independent set, and thus if it forms a basis of U. Because of this inequality, U is a finite sub- vector space of $\mathcal{D}$ over P. Assume that we have proven that U is a subring of the endomorphisms $\mathcal{D}$ [1]. We may now apply the Jacobson-Bourbaki theorem. We find that the subset F of P of elements a such that $aA = Aa$ for all endomorphisms $A \in U$ satisfies

$$[P : F] = [U : P]$$

] and U contains all F-linear transformations of P over F. Notice that all elements $A \in U$ are derivations, so the criterion that $A(ab) = aA(b)$ for all $b \in P$ and $A \in U$ implies with the Leibniz rule that $A(a) = 0$. It follows that F is the subfield of D-constants for $D \in \mathcal{D}$. Notice that a^p is a D-constant for any $a \in P$ because of characteristic p, so we see that P is purely inseparable of exponent ≤ 1 over F.

We will now proof that $[P : F] = p^m$. Let $B = \{b_1, b_2, \ldots b_{m'}\}$ be the p-basis of P/F of cardinality m'. Notice that the elements $b_1^{k_1} b_2^{k_2} \ldots b_{m'}^{k_{m'}}$ form a p-basis for the extension P/F. Hence, $[P : F] = p^{m'}$. Combining what we know gives that $m' \leq m$ since $[P : F] = [U : P] \leq p^m$ from the Jacobson-Bourbaki theorem. Corollary 3.12 shows that if $D(P/F)$ is the set of derivations in P/F, then $[D(P/F) : P] = m'$. If $a \in F$ then a is a D-constant for any $D \in \mathcal{D}$. Hence any such D is F-linear and $\mathcal{D} \subseteq D(P/F)$. Since $[\mathcal{D} : P] = m$ we conclude that $\mathcal{D} = D(P/F)$, so any derivation in P over F is contained in $\mathcal{D}$. Furthermore, it follows that $m = m'$, thus $[P : F] = p^m$. With this we conclude the proof of the theorem. □

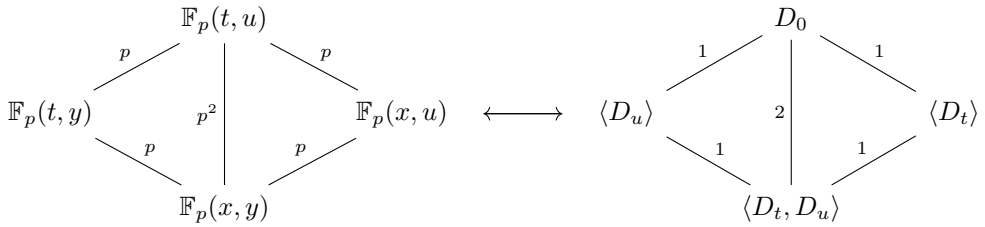
In this proof, we have uncovered information about the dimension of the field extension. We see that it is related to the size of the restricted p-Lie subalgebras similarly to how the indices of field extensions and the size of the subgroups of the Galois group are related in the fundamental theorem of Galois theory. To conclude these properties, we state the following corollary.

Corollary 3.16. *Let P over F be a finite purely inseparable field extension of exponent ≤ 1. Let E be an intermediate field and denote by B the $p-$basis of the extension P/E with $|B| = m$. Then the dimension of the extension is $[P : E] = p^m$ which is also the size of restricted p-Lie algebra of derivations in P/E.*

To illustrate this property we discuss an example with base field $\mathbb{F}_p(x, y)$. This example is closely related to example 3.6.

Example 3.17 (Extension of dimension p^2). Consider $F = \mathbb{F}_p(x, y)$ and $P = \mathbb{F}_p(t, u)$ with $t^p = x$ and $u^p = y$. With the same logic as in 3.6 we find some, but not all, proper intermediate fields $\mathbb{F}_p(t, y)$ and $\mathbb{F}_p(x, u)$ with according subalgebras $\langle D_u \rangle$ and $\langle D_t \rangle$ respectively. The sizes of these subalgebras are p, since they contain the derivations D_t^i and D_u^i for $1 \leq i \leq p$ respectively. This is the same set as given in

equation 6 in Jacobson's theorem. Since $\mathcal{D}$ contains again exactly their combinations as given in 6, its cardinality is p^2. Applying the corollary above we can depict the indices of some of the field extensions and subalgebras as in the following diagram.



3.2.3 Proof of the Galois-type correspondence

In this section we will prove theorem 3.4. The method includes showing that the maps given in the correspondence are actually each other's inverses. We also show that they are well-defined.

Proof (Theorem 3.4). Denote by $C(D)$ the D-constants of a set of derivations D and by $\mathrm{Der}(P/F)$ the restricted p-Lie algebra of derivations in P over F. If $P = E$ then we are working with the trivial case of the restricted p-Lie algebra of derivations in P/E existing of just the zero-mapping. Therefore, from now on, we assume that $P \neq E$. We will prove that P over E is a finite purely inseparable extension of exponent one. Since E is an intermediate field and P/F is a finite extension, so must P/E. Because $F \subseteq E$ and P/F has exponent ≤ 1 we see that for all $a \in P$, $a^p \in E$. Recall that $a^{p^n} \in E$ for some $n \in \mathbb{N}$ for all $a \in P$ is equivalent to the minimal polynomial of a in P/E being inseparable, see the discussion at the start of the chapter where we define the exponent of an extension. Hence, P/E is a finite purely inseparable extension of exponent one. This fact is used a lot throughout this proof to be able to apply the earlier developed theory in this thesis.

We would like to show that the correspondences stated in the theorem are well-defined. We start with the correspondence given by

$$\left\{ \begin{array}{c} \text{the field of} \\ D\text{-constants} \end{array} \right\} \longleftarrow \{ \quad \text{subalgebra } D \quad \} \tag{7}$$

We need to show that the D-constants of a subalgebra D of $\mathcal{D}$ is a subfield field of P/F, but this is exactly what proposition 2.6 says. Furthermore, since P is a finite extension over F any subfield must be as well, so we conclude that field of D-constants is a subfield of P that contains F. For the correspondence given by

$$\left\{ \begin{array}{c} \text{intermediate field} \\ E \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{the restricted} \\ p\text{-Lie algebra of} \\ \text{derivations in} \\ P/E \end{array} \right\}, \tag{8}$$

we need to show that $\mathrm{Der}(P/E)$ is indeed a subalgebra of $\mathcal{D}$. It is enough to show that $\mathrm{Der}(P/E)$ is also F-linear, because it is clear it is a restricted p-Lie algebra from the definition. This follows immediately from the fact that $F \subseteq E$. Thus we may conclude that both correspondences are well-defined.

Now, we will prove that the correspondences are each-others inverses. From this the bijection between intermediate fields and subalgebras as given in the theorem follows. For the first inverse check, we would like to show that

$$C(\mathrm{Der}(P/E)) = E, \tag{9}$$

for every subfield E of P that contains F. In words, we want to show that the D-constants of derivations in P over a subfield E is again equal to E itself. Because the derivations in P over E are E-linear it follows with the Leibniz rule that $E \subseteq C(\mathrm{Der}(P/E))$, as we have seen before. For the reverse inclusion, we apply corollary 3.13. This gives that the D-constants of $\mathrm{Der}(P/E)$ are contained within $E(P^p)$. Since $P^p \subseteq F \subseteq E$, it follows that

$$C(\mathrm{Der}(P/E)) \subseteq E(P^p) \subseteq E.$$

Hence we may conclude that equation 9 holds.

Lastly, we will show that

$$\mathrm{Der}(P/C(D)) = D, \tag{10}$$

for all subalgebras D of $\mathcal{D}$. In words, this means that for any subalgebra D of $\mathcal{D}$, the restricted p-Lie algebra of derivations in P over the D-constants is equal to D itself. Let $d \in D$, $x \in C(D)$ and $y \in P$ be arbitrary. For the inclusion $D \subseteq \mathrm{Der}(P/C(D))$ it is enough to show that d is $C(D)$-linear, because $D \subseteq \mathrm{Der}(P/F)$ already. We write

$$d(xy) = d(x)y + xdy = xdy,$$

so d is always $C(D)$-linear, as desired. Hence, we conclude that $d \in \mathrm{Der}(P/C(D))$. For the reverse inclusion $\mathrm{Der}(P/C(D)) \subseteq D$, we apply Jacobson's theorem 3.15 to find that any derivation of P over $C(D)$ is contained within D, so we may conclude that equation (10) holds.

We have showed that the correspondences are well-defined and each-others inverses, so we conclude the proof of the Galois-type correspondence in theorem 3.4. □

References

[1] Jacobson, N. (1964) Lectures in Abstract Algebra, III. Theory of Fields and Galois Theory. Springer-Verlag, Berlin. https://doi.org/10.1007/978-1-4612-9872-4

[2] Dummitt, D.S. and Foote, R.M. (2004) Abstract Algebra. 3rd Edition, John Wiley Sons, Inc.