THE GALOIS THEORY OF ÉTALE ALGEBRAS

ESZTER ROBIN
SUPERVISOR: ÁRPÁD TÓTH

This paper is a brief summary of Chapter 8 of J. S. Milne's notes on Fields and Galois theory. We focus on its main theorem (Theorem 2.1) discussing the connection of étale algebras and finite G-sets. We also provide the information necessary to understand these concepts from the previous chapters of the book.

1. Background

This section is to be used as a black box. It is a collection of propositions (and the definitions needed for them) that we will refer back to in the sections to come. Still, it presumes some knowledge of algebra. For the complete picture, we recommend reading the introductory chapters of the book.

1.1. Galois theory.

We begin by briefly looking at the foundations of our setting.

Definition 1.1. A polynomial is called **separable** if it is nonzero and has only simple roots.

An algebraic extension E/F is separable if the minimal polynomial of every element of E is **separable**; otherwise, it is **inseparable**.

We can also characterize inseparable extensions in a more explicit way, which will prove to be helpful in the upcoming proofs.

Proposition 1.2. *An algebraic extension E/F is inseparable if F has characteristic $p \neq 0$ and there exists $\alpha \in E$ such that its minimal polynomial is of the form $g(X^p)$ for some $g \in F[X]$.*

An other basic definition we need to get us to our goal, the definiton of Galois groups:

Definition 1.3. An algebraic extension E/F is **normal** if it is algebraic and the minimal polynomial of every element of E splits in $E[X]$.

Definition 1.4. An extension E/F of fields is **Galois** if it is finite, normal, and separable.

In this case, $\mathrm{Aut}(E/F)$ is called the **Galois group** of E over F, and denoted by $\mathrm{Gal}(E/F)$.

And to finish this section, we consider the following statement, which will come in handy later on.

Definition 1.5. For $f \in F[X]$, an E field containing F is called a **splitting field** if $f(X) = a\prod_{i=1}^{m}(X - \alpha_i)$ for some $a \in F, \alpha_i \in E$ and E is generated by the roots of f.

Proposition 1.6. *Let $f \in F[X]$. Let E be an extension of F generated by the roots of f in F and Ω an extension of F splitting f. There exists an F-homomorphism $\varphi : E \to \Omega$; the number of such homomorphisms is at most $[E : F]$, and equals $[E : F]$ if f has distinct roots in Ω.*

1.2. **Category theory.** Our main theorem is a statement of category theory, so we list the most important definitions we need.

Definition 1.7. $\mathcal{C} = (\text{Ob } \mathcal{C}, \text{Mor } \mathcal{C}, \circ, \text{id}_{\mathcal{C}})$ is a **category**, where

- Ob $\mathcal{C}$ is a class called the objects of the category,
- Mor $\mathcal{C}$ consists of sets denoted by $\text{Hom}(A, B)$, the set of morphisms from A to B for every $A, B \in \text{Ob } \mathcal{C}$,
- $\circ$ is the composition on the union of Hom-sets,
- $\text{id}_{\mathcal{C}}$ assigns to each object $A \in \text{Ob } \mathcal{C}$ the identity morphism $\text{id}_A \in \text{Hom}(A, A)$ (the morphism that behaves like the identity w.r.t. composition).

Definition 1.8. For arbitrary categories $\mathcal{C}, \mathcal{D}$, we call $F : \mathcal{C} \to \mathcal{D}$ a **functor** if $F : \text{Ob } \mathcal{C} \to \text{Ob } \mathcal{D}$, for every $A, B \in \text{Ob } \mathcal{C}$ it defines a map from $\text{Hom}(A, B)$ to $\text{Hom}(F(A), F(B))$ such that it preserves the composition of morphisms and the identity mappings.

A **contravariant functor** $F : \mathcal{C} \to \mathcal{D}$ is an $F : \text{Ob } \mathcal{C} \to \text{Ob } \mathcal{D}$, such that for every $A, B \in \text{Ob } \mathcal{C}$ it defines a map from $\text{Hom}(A, B)$ to $\text{Hom}(F(B), F(A))$ that preserves the composition of morphisms ($F(f \circ g) = F(g) \circ F(f)$) and the identity mappings.

If $F, G : \mathcal{C} \to \mathcal{D}$, then η is a **natural isomorphism** if

$$\forall A \in \text{Ob } \mathcal{C} : \eta(A) \in \text{Hom}(F(A), G(A))$$

is an isomorphism and

$$\forall A, B \in \text{Ob } \mathcal{C}, \forall f \in \text{Hom}(A, B) : \eta(A) \circ G(f) = F(f) \circ \eta(B).$$

(Notation: $F \sim G$.)

A **quasi-inverse functor** for a functor $F : \mathcal{C} \to \mathcal{D}$ is a functor $G : \mathcal{D} \to \mathcal{C}$ such that $F \circ G \sim \text{id}_{\mathcal{C}}$.

Definition 1.9. The categories $\mathcal{C}$ and $\mathcal{D}$ are **equivalent** if there exist functors $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ such that $G \circ F \sim \text{id}_{\mathcal{C}}$ and $F \circ G \sim \text{id}_{\mathcal{D}}$.

2. Classification of étale algebras

In this section, we focus on proving our main theorem which can be read as follows.

Theorem 2.1. *The functor $\mathcal{F}$ from the category of étale F-algebras to finite G-sets is a contravariant equivalence with quasi-inverse $\mathcal{A}$.*

To prove this equivalence, we now introduce the objects of the statement.

2.1. **Étale algebras.** The category of étale algebras is at the center of our attention. There are many ways to define them, as we will see shortly.

Definition 2.2. Let A be an F-algebra. A is **étale** if for some L containing F the tensor product $L \otimes A$ is diagonalizable[1].

Remark 2.3. Unless otherwise noted, a tensor product is considered to be over the field F.

Note that from the definition it immediately follows that an étale algebra must be finite dimensional over F.

Proposition 2.4. *For a finite F-algebra A the following are equivalent:*

[1]An F-algebra is diagonalizable if it is isomorphic to F^n for some n.

(1) *A is étale*
(2) *$L \otimes A$ is reduced*[2] *for all fields L containing F*
(3) *A is a product of separable field extensions*

Proof. (1) $\implies$ (2) : Since A is étale, there exists some L' containing F that $L' \otimes A$ is diagonalizable over F. Let L'' be a field containing both of L and L'. Then $L'' \otimes A \simeq L'' \otimes_{L'} L' \otimes A$ must also be diagonalizable, by the associativity of the tensor product and the fact that $L'' \simeq L'' \otimes_{L'} L'$ (infact they are connected by a natural isomorphism). The map $L \otimes A \to L'' \otimes A$ defined by the inclusion map $L \to L''$ takes nilpotents to nilpotents, so to 0. The map is injective, the only nilpotent in $L \otimes A$ is 0, so $L \otimes A$ is reduced.

(2) $\implies$ (3) : By assumption $A \simeq A \otimes F$ is reduced, so by the Classical Wedderburn-Artin theorem for algebras it follows that it is a product of fields. Assume the contrary that one of the fields in the product is not separable. This by Proposition 1.2 means that F has characteristic $p \neq 0$ and there exists an element u in that field whose minimal polinomial is of the form $g(X^p)$ for some $g \in F[X]$. Choose L to be a field containing F such that the coefficients of $g(X)$ in L are p-powers. Since the characteristic is p, we have $g(X^p) = h(X)^p$ for some $h \in L[X]$. And so $h(X) \neq 0$ is nilpotent in

$$L[X]/(h(X)^p) \simeq L[X]/(g(X^p)) \simeq L \otimes (F[X]/g(X^p)) \simeq L \otimes F[u].$$

Thus, $L \otimes F[u] \subset L \otimes A$ is not reduced.

(3) $\implies$ (1) : Without loss of generality, let A be a separable field extension of F. $A = F[u]$ for some u with minimal polynomial $f(X)$. Since $F[u]$ is separable, $f(X)$ is separable. Let L be a splitting field of f, then if $f(X) = \prod(X - u_i)$, where $u_i \neq u_j$ if $i \neq j$, by the Chinese remainder theorem we have that

$$L \otimes A \simeq L \otimes F[X]/(f) \simeq L[X]/(f) \simeq \prod L[X]/(X - u_i) \simeq L \times \cdots \times L.$$

□

Our first definition can be more useful in the sense that it easily shows that certain properties of diagonalizable algebras automatically transfer to étale algebras, like the following:

Proposition 2.5. *Finite products, tensor products and quotients of étale F-algebras are étale.*

2.2. **G-sets.** The other category to be considered is the category of G-sets, which is a special case of topological groups. To introduce them we need a few notations. From now on, let Ω be the algebraic closure of F, $G = \mathrm{Gal}(\Omega/F)$. Let $S \subset \Omega$ be finite, and then

$$G(S) := \{\sigma \in G : \sigma s = s \ \forall s \in S\}.$$

Definition 2.6. A **topological group** is a group equipped with a topological structure such that the multiplication and inverse are both continuous.

The **Krull topology** of the group G is the topology such that the sets $G(S)$ form an open neighborhood base for 1.

Definition 2.7. A **G-set** is a set S with an action of G such that the map $G \times S \to S$ is continuous with respect to the Krull topology.

[2]An algebra is reduced if and only if the intersection of its maximal ideals is 0, which is equivalent with 0 being the only nilpotent element of the algebra.

2.3. **The functors $\mathcal{F}$ and $\mathcal{A}$.** The connection between these categories is given by two functors which we will introduce here.

$$\mathcal{F}(A) := \{f : A \to \Omega \ F\text{-algebra homomorphism}\}$$

Let G act on $\mathcal{F}(A)$ by its action on Ω:

$$(\sigma f)(a) := \sigma(f(a)) \quad \sigma \in G, f \in \mathcal{F}(A), a \in A.$$

This action is continuous, so $\mathcal{F}(A)$ is a G-set. In the case of étale algebras it is also finite. To prove this we consider the following property of $\mathcal{F}$.

Proposition 2.8. *$A = \prod_i F_i$ étale, F_i a field $\implies$ $\mathcal{F}(A) \simeq \bigsqcup_i Hom_F(F_i, \Omega)$*

Proof. Let $e_i \in A$ be the idempotent, which is 0 in all coordinates, but the ith, where it is 1. If $f : A \to \Omega$ is a homomorphism, it is zero on all but one F_i, because of the fact that $f(e_i)$ is also an idempotent (i.e. $f(e_i) \in \{0, 1\}$) and the orthogonality of these elements. And so

$$\mathcal{F}(A) = \mathcal{F}(\prod_i F_i) \simeq \bigsqcup_i \mathcal{F}(F_i) = \bigsqcup_i \mathrm{Hom}_F(F_i, \Omega)$$

□

Corollary 2.9. *$\mathcal{F}$ is a functor from the category of étale algebras to finite G-sets.*

Proof. Our previous proposition shows, that when A is étale, $\mathcal{F}(A)$ is of order $[A : F]$ by Proposition 1.6, thus finite. □

The other functor can be given in the following way for a finite G-set S:

$$\mathcal{A}(S) := \{f \in \mathrm{Hom}(S, \Omega) : f(\sigma s) = \sigma f(s) \ \forall \sigma \in G, s \in S\}$$

This is the same as taking elements that are fixed by the action of G on $\mathrm{Hom}(S, \Omega)$ defined as $(\sigma f)(s) = \sigma(f(\sigma^{-1}s))$ for $\sigma \in G, f \in \mathrm{Hom}(S, \Omega), s \in S$.

This concludes the preparations for the proof of our main theorem.

2.4. **Proof of theorem 2.1.** We break the statement down to three parts.

Proposition 2.10.

$$A \simeq \mathcal{A}(\mathcal{F}(A))$$

Proof. Define an action on $\Omega \otimes_F A$ by G by its action on Ω. Let us denote the elements fixed by G as $(\Omega \otimes_F A)^G$.

If $x \in (\Omega \otimes_F A)^G, x = \sum c_i \otimes a_i$, then $c_i \in F$, since $\sum \tau(c_i) \otimes a_i = \sum c_i \otimes a_i$ for every $\tau \in G$, $\tau(c_i) = c_i$ for all $\tau \in G$. And so

$$(\Omega \otimes_F A)^G \simeq F \otimes_F A \simeq A.$$

Now, since $c \otimes a \mapsto (\sigma c \cdot a)_{\sigma \in \mathcal{F}(A)}$ defines an isomorphism :

$$\Omega \otimes_F A \simeq \prod_{\sigma \in \mathcal{F}(A)} \Omega$$

we can take the action on the product as well. The fixed elements become:

$$\{f : \mathcal{F}(A) \to \Omega : f(\tau\sigma) = \tau f(\sigma) \ \forall \tau \in G, \sigma \in \mathcal{F}(A)\}.$$

Which by definition is equal to $\mathcal{A}(\mathcal{F}(A))$. Thus

$$A \simeq (\Omega \otimes_F A)^G \simeq (\prod_{\sigma \in \mathcal{F}(A)} \Omega)^G \simeq \mathcal{A}(\mathcal{F}(A)).$$

□

Proposition 2.11.

$$S \simeq \mathcal{F}(\mathcal{A}(S))$$

Proof. Let $\hat{s} : \mathcal{A}(S) \to \Omega$ be the evaluation map:

$$\hat{s}(f) := f(s).$$

It is easy to see that this is an F-algebra homomorphism, since the elements of $\mathcal{A}(S)$ were.

It suffices to prove that all elements of $\mathrm{Hom}(\mathcal{A}(S), \Omega)$ are of this form, because then the hat operation defines the isomorphism we were looking for. And this is true since the characteristic functions of the elements of S

$$\chi_s(t) = \begin{cases} 1 & s = t \\ 0 & s \neq t \end{cases}$$

form an orthogonal base of idempotents in $\mathcal{A}(S)$:

$$f \in \mathcal{A}(S) : \forall s \in S \; f(s) = \sum_{t \in S} f(t)\chi_t(s).$$

And so for $\phi \in \mathrm{Hom}(\mathcal{A}(S), \Omega)$, we have:

$$\phi(f) = \sum_{t \in S} f(t)\phi(\chi_t) = f(s) \cdot 1$$

for a unique $s \in S$, since it maps exactly one of the characteristic functions to 1 and the others to 0. This implies that $\phi = \hat{s}$. □

Proposition 2.12. *The map defined by $\mathcal{F}$ is bijective.*

Proof. Let A, B be étale F-algebras. Let G act on $\mathrm{Hom}_{\Omega\text{-algebra}}(\Omega \otimes A, \Omega \otimes B)$ by $\sigma\alpha := \sigma \circ \alpha \circ \sigma^{-1}$. Then by extending the idea presented at the beginning of the proof of Proposition 2.10, we find that

$$\mathrm{Hom}_{F\text{-algebra}}(A, B) \simeq \mathrm{Hom}_{\Omega\text{-algebra}}(\Omega \otimes A, \Omega \otimes B)^G.$$

Since $\Omega \otimes A \simeq \prod_{i \in \mathcal{F}(A)} \Omega$ and $\Omega \otimes B \simeq \prod_{j \in \mathcal{F}(B)} \Omega$,we can take $\tilde{f} : \mathcal{F}(B) \to \mathcal{F}(A)$ and define a homomorphism $f((a_i)_{i \in \mathcal{F}(A)}) := (b_j)_{j \in \mathcal{F}(B)}$, where $b_j = a_{\tilde{f}(j)}$. Similar reasoning as before shows that all elements of $\mathrm{Hom}_{\Omega\text{-algebra}}(\Omega \otimes A, \Omega \otimes B)$ are of this form. The map $f \mapsto \tilde{f}$ preserves the action of G, hence

$$\mathrm{Hom}_{\Omega\text{-algebra}}(\Omega \otimes A, \Omega \otimes B)^G \simeq \mathrm{Hom}_{G\text{-sets}}(\mathcal{F}(A), \mathcal{F}(B))^G.$$

Which means that

$$\mathrm{Hom}_{F\text{-algebra}}(A, B) \simeq \mathrm{Hom}_{G\text{-sets}}(\mathcal{F}(A), \mathcal{F}(B)).$$

□

References

[1] Milne, J. S. (2003). Fields and Galois theory. Courses Notes, Version, 4.