Galois Theory and G-sets

Facultad de Ciencias
Universidad Zaragoza

Universidad
Zaragoza
1542

Fernando Barrera Esteban
Trabajo de fin de grado en Matemáticas
Universidad de Zaragoza

Director del trabajo: Fernando Montaner Frutos
28 de Noviembre de 2016

Prologue

The following text discusses the Galois Theory in a non-classical way. It consists of two chapters.

- The first one establish some results about algebras. Here the reader can find what algebras and algebras over a field are; what we call trivial, separable algebras, etc. The reader will find at some points how the classical theory of algebraic extensions fits in this context.
- The second chapter is divided in two parts. First, I give some basic results of G-sets. Then I state the theorems and propositions which will allow us to establish and prove the *Galois Theorem*, which will be displayed at the end.

This text is based on [1], which in turn is based on the course taught by Prof. García Loygorri at University of Salamanca in 1974. In [2] and [3] the reader will find definitions and results of concepts that have not been explained properly because they are out of the main topic, in a sense. For a discussion in a more *categorical* way, [7] can be used. In this text it has been used just to complet some proofs that are not clear in [1]. In [4], [5] and [6] the reader can find an exhaustive explanation of concepts in classical algebraic extensions theory that are only mentioned as examples here.

Summary

El presente texto se pregunta qué quiere decir la teoría de Galois. Una respuesta frecuente suele mencionar el estudio de la resolución de ecuaciones polinómicas por radicales. Bien es cierto que ésta es la motivación de matemáticos como Ruffini, quien en su libro *Teoria Generale delle Equazioni* defiende la imposibilidad de la resolución de ecuaciones polinómicas de grado cinco mediante radicales; Abel, que da una prueba sobre la idea de Ruffini que es depurada finalmente por Kronecker; y el propio Galois, quien se pregunta en general, no solamente para las quínticas que habían sido estudiadas por sus predecesores, cuándo existe y cuándo no una solución por radicales [8, Historical Introduction]. Sin embargo, éste se muestra ahora como un problema menor dada la magnitud del impacto que supone la aparición de una noción tan ubicua como es la de grupo.

La teoría de Galois clásica, explicada ya en términos de Artin, muestra que existe una relación biunívoca entre las extensiones intermedias de un cuerpo y una extensión de Galois y los subgrupos del grupo de Galois, lo que facilita en gran medida el estudio de las extensiones de cuerpos trasladándolo al estudio de sus grupos de automorfismos. La teoría de Galois como aquí se trata pretende ser de algún modo más general. Se puede decir que ésta va a ser una versión intermedia entre la versión clásica y la versión de Grothendieck, quién hace uso de una terminología *categórica* que aquí prácticamente no se usa. Si el lector tiene interés en esta versión, puede consultar [7], capítulo 2. El objetivo de una nueva reformulación de la teoría de Galois de un modo más general es el de preparar el camino a un salto a una teoría de Galois para extensiones infinitas, [7], capítulo 3, que no es tratada aquí.

La primera parte del trabajo introduce la noción de álgebra. Un A-álgebra B será un anillo con un morfismo de anillos $f : A \to B$ que permite definir el producto dado por $ab = f(a)b$ de manera que B adquiere una estructura adicional de A-modulo. Esto es, una A-álgebra es un anillo dotado de la operación por escalares de un anillo A. Siempre y cuando un subanillo de B sea tal que contiene la imagen de A bajo el morfismo f, éste tendrá también estructura de A-álgebra y será llamado subálgebra.

No se define el producto tensorial de módulos ni el producto tensorial de álgebras, que pueden verse en [2, Chapter 2, p.24] y [2, Chapter 2, p.30] respectivamente. Del mismo modo, no se mencionan ni prueban ciertas propiedades fundamentales del producto tensorial que aparecen en [3, Chapter XVI]. En cualquier caso, dadas dos A-algebras B,C podemos considerar su producto tensorial sobre A, que denotamos $B \otimes_A C$ y que jugará un importante rol a lo largo del texto.

Estudiamos también las k-algebras en las que el anillo k es un cuerpo. Llamaremos extensión a las k-álgebras $k \to K$ con K cuerpo. Merece la pena mencionar aquí que lo que llamamos extensión de un cuerpo en la teoría clásica de extensiones algebraicas es de hecho una álgebra sobre un cuerpo. Vemos también que si K es una extensión de k, para toda k-algebra A existe un morfismo de álgebras de manera que $A \otimes_k K$ es una K-álgebra que recibe el nombre de extensión de escalares. La dimensión de esta álgebra sobre K será la misma que la de la k-algebra A sobre k. Del mismo modo tendremos la transitividad del grado de cualquier álgebra de manera que si B es una K-algebra donde K es una extensión de k, entonces $dim_k(B) = dim_K(B)dim_k(K)$.

Como en la teoría clásica de Galois, en la que se estudian las extensiones finitas sobre un cuerpo, nosotros estudiaremos las álgebras finitas. Veremos que un álgebra finita, si es un dominio de integridad, es un cuerpo; que todo ideal primo es maximal y que cualquier cociente de un álgebra por su radical (esto es, la intersección de sus ideales maximales) se descompone en la suma directa de los cuerpos residuales de estos ideales, lo que viene a ser el teorema chino de los restos.

Llamamos álgebra trivial a cualquier álgebra que se descomponga como suma directa de extensiones de grado uno y álgebras reducidas a las álgebras sin elementos nilpotentes no nulos. El Teorema de Descomposición dirá que cualquier álgebra finita y reducida se descompone como suma directa de sus componentes. Esto es claro, ya que, al ser reducida, su radical es nulo.

Estudiamos los puntos de un algebra A sobre una extensión K, que son los morfismos de álgebras de A en K y que, veremos, están unívocamente relacionados con los morfismos de la K-algebra A_K en K, con los ideales maximales m de A_K tales que el cociente A_K/m es isomorfo a K y de aquí, claro, con las componentes de A_K(*).

Introducimos la noción de separabilidad de k-algebras, que es una generalización de la separabilidad de extensiones (de hecho, en el texto vemos que si una extensión es separable en el sentido clásico, entonces es una k-algebra separable) y las caracterizamos. Una k-álgebra separable cumplirá que su extensión de escalares por todo cuerpo K extensión de k será separable.

Para estudiar si una k-algebra es separable o no, haremos uso de la métrica de la traza. Dada una k-algebra A, cualquier elemento $a \in A$ define un endomorfismo de A dado por $x \longmapsto ax$. Llamaremos traza de a a la traza de este endomorfismo. Ocurre que el radical de la k-algebra está contendido en el radical de la métrica, así que para ver si una k-algebra A es reducida, basta con ver si el radical de la métrica de la traza de A_K es nula. De esta manera, la métrica de la traza se revela como una importante herramienta para el estudio de álgebras reducidas.

Finalmente estudiamos los cuerpos finitos para concluir que todo cuerpo finito es perfecto, esto es, que toda extensión de un cuerpo finito es separable.

Decimos que un conjunto X es un G-conjunto si está dotado de una acción de G sobre X. La acción de G define una equivalencia en X a cuyas clases de equivalencia llamamos órbitas. Es claro entonces que todo G-conjunto es isomorfo a la unión disjunta de sus órbitas. Un G-conjunto con una sola órbita se dirá conexo. Se observa que todo G-conjunto conexo X es isomorfo a G/H donde H es el estabilizador de un elemento $x \in X$. Podemos definir aplicaciones entre G-conjuntos que conserven su estructura. Éstas se llaman G-morfismos. El conjunto de G-morfismos entre dos G-conjuntos X e Y se denota $Hom_G(X,Y)$ y se relaciona unívocamente con el conjunto de órbitas de $X \times Y$ isomorfas a X a través de una proyección canónica de $X \times Y$ en X.

Veremos que dada una k-algebra A y una extensión K de k, todo automorfismo g de K induce un automorfismo $id \otimes g$ de A_K. Es decir, el grupo $G = Aut_k(K)$ actúa sobre A_K, luego actúa también sobre sus ideales maximales, así que actúa sobre $Hom_{k-alg}(A,K)$ por (*). De esta manera $Hom_{k-alg}(A,K)$ es un G-conjunto sobre el que G actúa mediante la composición. Es decir, $gf = g \circ f$ para todo $f \in Hom_{k-alg}(A,K)$.

Decimos que una extension $k \to K$ es Galois si la K-álgebra $K \otimes_k K$ es trivial. Al grupo de automorfismos de K se le llama su grupo de Galois. Ocurre que si K es Galois con grupo de Galois G, entonces $K^G = k$, lo que demuestra que nuestra definición de extensión de Galois contiene a la definición clásica ya que una extensión se dice de Galois si ésta es normal y separable, lo que es equivalente a que $K^G = k$. El Teorema de Artin dirá que si G es el grupo de automorfismos de una extensión finita y separable K de k, entonces $K^G = k$ y G será el grupo de Galois de K. Desde el teorema de Prolongación veremos que si G es el grupo de Galois de una extensión de Galois K sobre k, para toda otra extensión finita L de k, G actúa transitivamente sobre $Hom_k(L,K)$. Finalmente definimos lo que es una k-algebra trivial sobre la extensión de Galois K, que es aquella tal que su extensión escalar es una K-álgebra trivial. El **Teorema de Galois** *establecerá una relación biunívoca entre la categoría de k-álgebras triviales sobre K y la categoría de G-conjuntos finitos.* La función vendrá dada por los funtores contravariantes P y R que llevan la k-algebra A a $P(A) = Hom_k(A,K)$ y el G-conjunto X a $R(X) = (\oplus_X K)^G$. Veremos que, nuevamente, esta versión del teorema de Galois es una generalización porque contiene el teorema de Galois clásico que relaciona las extensiones intermedias de k y K y los subgrupos del grupo de Galois de K. Citaremos finalmente la envoltura de Galois de una k-algebra finita y separable A como la extensión de Galois más pequeña sobre la que A es trivial.

Contents

Chapter 1

Finite Algebras

1.1 Algebras

Definition 1.1.1. Let A, B be two rings and let $f : A \to B$ be a ring morphism. We define a product

$$ab = f(a)b$$

which makes B into an A-module. The ring B together with the structure of A-module is said to be an *A-algebra.*

Definition 1.1.2. Given two ring morphisms $f : A \to B$ and $g : A \to C$, the ring morphism $h : B \to C$ is said to be an *A-algebra morphism* or *morphism of A-algebras* if it is also an A-module morphism. It is easy to see that h is an A-algebra morphism if and only if $h \circ f = g$.

Definition 1.1.3. Let $f : A \to B$ be a ring morphism. Any subring C of B such that $f(A) \subset C$ has a structure of A-algebra. C is called *subalgebra* of the algebra B.

Let B and C be two A-algebras, since they can be seen as A-modules we may form their *tensor product* $B \otimes_A C$ which is an A-algebra, as well. This A-algebra is endowed with two A-algebra morphisms $u : B \to B \otimes_A C$ and $v : C \to B \otimes_A C$ such that

$$\begin{gathered} Hom_{A-alg}(B \otimes_A C, D) = Hom_{A-alg}(B, D) \times Hom_{A-alg}(C, D) \\ f \longleftrightarrow (f \circ u, f \circ v) \end{gathered}$$

for any A-algebra D. We will write $b \otimes c = u(b)v(c)$. It is worth saying that any pair of A-algebra morphisms $f : A \to X$ and $g : B \to Y$ define an A-algebra morpshism $f \otimes g : A \otimes B \to X \otimes Y$ given by $(f \otimes g)(a \otimes b) = f(a) \otimes g(b)$.

1.2 Algebras over a field

Let k be a field.

Definition 1.2.1. We will say that a k-algebra $k \mapsto K$ is an extension whenever the ring K is a field.

If K is an extension and A is a k-algebra, their tensor product $A \otimes_k K$ is endowed with a k-algebra morphism

$$\begin{gathered} u : K \longmapsto A \otimes_k K \\ \lambda \longmapsto 1 \otimes \lambda \end{gathered}$$

such that $A \otimes_k K$ has a structure of K-algebra. This new K-algebra will be denoted by A_K and called *extension of scalars*.

If A is a k-algebra, it can be seen as a vector space over k. We will say that the k-algebra A is finite if it is finite as a k-vector space. Since a tensor product is free if its factors are free and A_K is generated by the elements of the form $a_i \otimes \lambda$, where $\{a_i\}$ is a basis of A, the k-algebra A will be finite if and only if A_K is finite. In this conditions we will have:

$$dim_k(A) = dim_K(A_K).$$

Moreover, if $k \mapsto K$ is a finite extension and B is a finite K-algebra, B will have a structure of k-algebra through the composition $k \longmapsto K \longmapsto B$ and it is verified that

$$dim_k(B) = dim_K(B)dim_k(K).$$

If K is a finite extension of k, its dimension over k will be called *degree*.
Let us notice that, since any morphism between fields is injective, any morphism between finite extensions is an automorphism.

The reader must have noticed that it has not been necessary to talk about irreducible polynomials and algebraic extensions as it is done in the classical Galois Theory. However, it is easy to see that from our new definitions we can reach the same results. It is straightforward that finite extensions are finite k-algebras and it is already known that an extension is finite if and only if it is algebraic. Therefore when we talk about finite k-algebras in particular we are considering algebraic extensions.

Let k be a field and A be a k-algebra. It is clear that the ring of polynomials $k[x]$ is a k-algebra as well. Take an element $a \in A$. It induces the mapping

$$\phi_a : k[x] \to A \text{ given by } X \longmapsto a$$

which clearly is a k-algebra morphism. The image of this mapping will be $k[a]$ which is the smallest subalgebra which contains a. Since k is a field, $k[x]$ is a principal ideal domain so $ker\phi_a$ will be generated by just one polynomial and we can choose a monic one. This polynomial is called the *irreducible polynomial of a* and we denote it by $Irr(a,k)$. By the First Isomorphism Theorem we have that:

$$k[x]/(Irr(a,k)) \simeq k[a].$$

Given an extension $k \to K$ and the elements $a_1, \dots, a_n \in K$, we denote by $K(a_1, \dots, a_n)$ the smallest subfield of K containing both the image of k and the given elements. If K is finite, for any $a \in K$ it happens that

$$k(a) = k[a]$$

because a is algebraic over k so $Irr(a,k)$ is irreducible and therefore $k[a] \simeq k[x]/(Irr(a,k))$ is a field. This in particular give us the following

Proposition 1.2.2. *If K is an extension $k \to k(a)$, then $deg_k(k(a)) = deg(Irr(a,k))$.*

Definition 1.2.3. Let K, K' and E be extensions of a field k. Given the field morphisms $K \to E$ and $K' \to E$ we call the *composite* of K and K' to the smallest subfield of E which contains the image of the induced morphism $K \otimes_k K' \to E$.

1.3 Finite algebras

Let k be a field.

Lemma 1.3.1. *If the finite k-algebra A is an integral domain, then it is a field.*

Proof. Any element $a \in A$ defines an endomorphism $\phi_a : A \longmapsto A$ given by $\phi_a(x) = ax$. Since A is an integral domain there is no x such that $ax = 0$ so ϕ_a is a monomorphism. But A is a finite k-algebra so ϕ_a is an epimorphism. This implies that for any $a \in A$ there is an inversible element, thus A is a field. ■

Remark. It is trivial that ϕ_a is an isomorphism because it is a monomorphism between finite dimensional k-vector spaces with the same dimension.

Theorem 1.3.2. *Any prime ideal of a finite k-algebra is maximal.*

Proof. Let p be a prime ideal of the finite k-algebra A. Then A/p is an integral domain so, by the lemma above, it is a field thus p is maximal. ■

Lemma 1.3.3. *Let $m_1, \dots, m_r$ be maximal ideals of a ring A. Then the canonical morphism*

$$A/(m_1 \cap \ldots \cap m_r) \to A/m_1 \oplus \ldots \oplus A/m_r$$

is an isomorphism.

Proof. It is straightfoward that the mapping is a monomorphism. To see that it is also onto we prove that, without loss of generality, the element $(1,0,\dots,0)$ is in the image.
If $i \neq 1$ then $m_1 + m_i = A$. Otherwise, since the sum of ideals is an ideal, we would have a proper ideal containing both m_1 and m_i which are maximal. Therefore there exist elements $a_i \in m_1$ and $b_i \in m_i$ such that $a_i + b_i = 1$. Let

$$c = \textstyle\sum_{i=2}^{r} \prod b_i$$

Then $c \equiv 1(\text{mod } m_1)$ as $b_i \equiv 1(\text{mod } m_1)$ and $c \equiv 0(\text{mod } m_i)$ for any $i \neq 1$ as $b_i \equiv 0(\text{mod } m_i)$. ■

Definition 1.3.4. A k-algebra is said to be *trivial* if it is isomorphic to the direct sum of extensions of degree 1, *i.e.*, if it is isomorphic to $k \oplus \ldots \oplus k$.

Note that the tensor product of two trivial k-algebras is a trivial k-algebra and that any quotient of a trivial k-algebra is trivial. Also, if A is a trivial k-algebra and $k \to K$ an extension of k then A_K is a trivial K-algebra. Indeed, $A_K = A \otimes_k K \simeq (k \oplus \ldots \oplus k) \otimes_k K = (k \otimes_k K) \oplus \ldots \oplus (k \otimes_k K) = K \oplus \ldots \oplus K$.

Corollary 1.3.5. *The number of maximal ideals of a finite k-algebra is bounded by its dimension. The equality holds if and only if the k-algebra is trivial.*

Proof. If $m_1, \dots, m_r$ are the maximal ideals of a finite k-algebra A then:

$$dim_k(A) \geqslant dim_k(A/(m_1 \cap \ldots \cap m_r)) = dim_k(A/m_1 \oplus \ldots \oplus A/m_r) = \textstyle\sum_{i=1}^{r} dim_k(A/m_i) \geqslant r$$

To have the equality we need that $m_1 \cap \ldots \cap m_r = 0$ and $A/m_i \simeq k$ for any i, that is, we need A to be trivial. ■

Theorem 1.3.6 (Decomposition Theorem). *Any reduced and finite k-algebra decomposes as the direct sum of the residual fields of its maximal ideals.*

Proof. Because of the previous result, the number of maximal ideals of a finite k-algebra is finite. Let A be a reduced finite k-algebra. Its radical is the intersection of all its maximal ideals and, since A is reduced, this is null. Then, applying 1.3.3 the result follows. ■

Corollary 1.3.7. *Any subalgebra of a trivial finite k-algebra is trivial.*

Proof. Let us take a trivial k-algebra A and consider its projections $\pi_i : A \to k$. Let B be a subalgebra of k. Then we can restrict the projections to $\pi_i^B : B \to k$. The kernel of any projection π_i is a maximal ideal m_i so the kernles of π_i^B are also maximal ideals $n_i = m_i \cap B$ but not necessarily different. Moreover $B/n_i \simeq k$. To see this, note that for any i, $k \simeq A/m_i$ so any $\lambda \in k$ can be written as $a + m_i$ with $a \in A$ therefore any $a \in A$ can be written as $\lambda + m_i$. Hence, $A = k + m_i$. But $k + m_i \subset B + m_i$ so $B + m_i/m_i \simeq A/m_i$ and, by the Second Isomorphism Theorem, $B + m/m \simeq B/B \cap m = B/n$ and we have proven that $B/n_i \simeq k$. Then we apply the Decomposition Theorem on B and the result follows. ■

Definition 1.3.8. A field k is said to be *algebraically closed* if all of its polynomials have at least one root in k. Therefore, if k is algebraically closed, all its irreducible polynomials are of degree 1.

Corollary 1.3.9. *Any finite k-algebra which is reduced over an algebraically closed field is trivial.*

Proof. Let k be an algebraically closed field. If A is a reduced finite k-algebra it decomposes in the direct sum of its residual fields. But they are extensions of k through the composition $k \to A \to A/m_i$ for any i so $deg_k(A/m_i) = 1$ hence they are isomorphic to k. ■

Definition 1.3.10. Let A be a reduced finite k-algebra. Its residual fields are called *components*.

According to this definition, the Decomposition Theorem says that a reduced finite k-algebra A decompose in the direct sum of its components. Let us notice that the components of A are not subalgebras of A.

Let us consider the finite k-algebra $k[x]$. By 1.3.2 any prime ideal of $k[x]$ is maximal. But $k[x]$ is a PID, so prime ideals are generated by just one polynomial which is irreducible because in a PID

$$\{maximal\ ideals\ of\ k[x]\} = \{(p)\ with\ p\ prime\} = \{(p)\ is\ irreducible\}.$$

Let $q_1, \ldots, q_n$ be the monic irreducible factors so that $p = q_1^{e_1} \ldots q_n^{e_n}$ for some $e_i \geq 1$ and take $k[x]/(p)$. Whenever the factors q_i are different to each other, it happens that

$$k[x]/(p) = k[x]/(q_1^{e_1} \ldots q_n^{e_n}) = k[x]/\cap_i (q_i).$$

From the *Decomposition Theorem* it follows that

$$k[x]/(p) = \bigoplus_i k[x]/(q_i).$$

1.4 Points of an algebra

Definition 1.4.1. Let K be an extension of k and let A be a k-algebra. The k-algebra morphisms from A into K are called *points of A with values in K*. Points of a k-algebra with values in k are said to be *rational points*.

Lemma 1.4.2. *The rational points of a k-algebra are in 1-1 correspondence with its maximal ideals of residual field k. More precisely:*

$$Hom_{k-alg}(A, k) = \{m \mid m \lhd_{max} A\ and\ A/m \simeq k\}.$$

Proof. Each maximal ideal whose residual field is k is the kernel of a point of A with values in k. To see this, take $m \lhd_{max} A$ such that $A/m \simeq k$ and consider the map $A \to k$ given by $a \longmapsto a + m$.
On the other hand, any k-algebra morphism from A into k is surjective. Indeed, since any k-algebra morphism is a k-module morphism, $f(\lambda) = f(\lambda 1) = \lambda f(1) = \lambda$ for any $f : A \to k$, $\lambda \in k$. Therefore, if two of such morphisms have the same kernel they factorize through the other so they are different, possibly up to an automorphism of k. Since the only automorphism of k is the identity, each rational point is indeed determined by its kernel. ■

Lemma 1.4.3. *The points of a k-algebra A with values in K are in 1-1 correspondence with the rational points of the K-algebra A_K. More precisely:*

$$Hom_{k-alg}(A, K) = Hom_{K-alg}(A_K, K)$$

where any k-algebra morphism $f : A \to K$ is attached to the morphism $f \otimes id : A_K \to K$ given by

$$(f \otimes id)(\sum a_i \otimes \lambda_i) = \sum f(a_i)\lambda_i.$$

Proof. The morphism f is determined by $f \otimes id$ because $f(a) = (f \otimes id)(a \otimes 1)$.
On the other hand, let $g : A_K \to K$ be a K-algebra morphism. Let us take $f : A \to K$ given by $f(a) = g(a \otimes 1)$. It is easy to see that f is a k-algebra morphism. It is verified that:

$$g(\sum a_i \otimes \lambda_i) = g(\sum (a_i \otimes 1)(1 \otimes \lambda_i)) =$$
$$g(\sum \lambda_i (a_i \otimes 1)) = \sum (\lambda_i g(a_i \otimes 1)) =$$
$$\sum \lambda_i f(a_i) = (f \otimes id)(\sum a_i \otimes \lambda_i)$$

thus $g = f \otimes id$. ■

Theorem 1.4.4. *The points of a k-algebra A with values in an extension K of k are in 1-1 correspondence with the maximal ideals of A_K with residual field K. More precisely:*

$$Hom_{k-alg}(A,K) = \{m \mid m \lhd_{max} A_K \text{ and } A_K/m \simeq K\}$$

Proof. We have proven in the lemma above that $Hom_{k-alg}(A,K) = Hom_{K-alg}(A_K,K)$. Applying 1.4.2 to the K-algebra A_K the result follows. ■

Corollary 1.4.5. *The number of points of a finite k-algebra A with values in an extension K is bounded by its dimension. The equality holds if and only if A_K is a trivial K-algebra.*

Proof. It follows from 1.3.5. The number of ideals of A_K is bounded by $dim_K(A_K)$. Then apply the equality in the theorem above. The second statement follows from 1.3.5, too. ■

Corollary 1.4.6. *The number of rational points of a finite k-algebra is bounded by its dimension. The equality holds if and only if the algebra is trivial.*

Proof. Straightforward from the fact that $Hom_k(A,K) = Hom_K(A_K,K)$ and $dim_k(A) = dim_K(A_K)$. ■

Corollary 1.4.7. *Let K be a finite extension of k. The number of automorphisms of K over k is bounded by the degree of K over k. The equality holds if and only if $K \otimes_k K$ is a trivial K-algebra.*

Proof. By 1.4.5 the number of points of K with values in K is bounded by $dim_k(K)$, which is its degree. We would have the equality if K_K is trivial, that is, if $K \otimes_k K$ is trivial. ■

Definition 1.4.8. Let k be a field. An extension $k \to K$ is said to be an algebraic closure of k if K is algebraically closed and each element of K is the root of a non-zero polynomial in $k[x]$. That is, when K verifies:

i) Any element of K belongs to some subfield of K which is a finite extension of k.

ii) Any polynomial with coefficients in k decomposes in $k[x]$ as product of polynomials of degree 1.

Generally, the algebraic closure of a field k is denoted by $\overline{k}$.

Lemma 1.4.9. *Let k be a field. Then its algebraic closure is unique up to isomorphism.*

Proof. Let K and K' be two algebraic clousures of k. The residual field of any maximal ideal m of $K \otimes K'$ is an extension of K through the composition $K \to K \otimes K' \to K \otimes K'/m$ which is generated by roots of polynomials with coefficients in k. Indeed, the generators of $K \otimes_k K$ are $\alpha \otimes 1$ and $1 \otimes \lambda$ where $\alpha \in K$ and $\lambda \in K'$ are roots of polynomials of $k[x]$ as K and K' are algebraic clousures of k, so it is an extension of K such that $dim_K(K \otimes K'/m) = 1$. An analogous argument can be used for K'. Therefore, any maximal ideal of $K \otimes K'$ defines a k-algebra morphism $K \to K'$ which is obviously injective but also surjective because every element of K is a root of a polynomial with coefficients in k and these polynomials have all their roots in K'. ■

Remark. Note that we are assuming the existence in the previous lemma. To see a proof of existence the reader can check [4, pp.21-22] and [6, pp.47-48].

1.5 Separable finite algebras

Let k be a field and let A be a finite k-algebra.

Definition 1.5.1. A k-algebra A is said to be *separable* if for any extension $k \to K$ its extension of scalars A_K has no nilpotent elements.

Remark. Let A be a *separable* finite k-algebra. Then, A_K is finite and reduced so, by the Decomposition Theorem, A_K decomposes as a direct sum of fields. Moreover, let A be a trivial k-algebra. It is clear that A_K has no nilpotent elements because it is a trivial K-algebra so A is separable. That is, any trivial k-algebra is separable.

In *classical Algebraic Extensions of Fields*, given an algebraic extension K/k, an element $a \in K$ is said to be *separable over k* if it is a simple root of its irreducible polynomial. If all the elements in K/k are separable K is said to be *separable*. An element $a \in K$ is said to be *inseparable* if it is not a simple root of $Irr(a,k)$ and it is said *purely inseparable* if $Irr(a,k) = (x-a)^n$ for some $n \in \mathbb{N}$.
Let K/k be a normal extension of charateristic p which is not separable. Then there exists an element $a \in K$ which is purely inseparable over k[1]. Therefore

$$Irr(a,k) = (x-a)^n \text{ for some } n \in \mathbb{N}.$$

This can be written in the following way:

$$Irr(a,k) = (x-a)^n = (x-a)^{p^e m} = h(x)^{p^e}$$

where p and m are coprimes. Let us take the polynomial

$$h(x) = b_0 + b_1 x + \ldots + b_{n-1} x^{n-1} + x^m.$$

Then there exists an element b_i such that $b_i \notin k$ because otherwise $h(x) \in k[x]$. However, the polynomial

$$Irr(a,k) = h(x)^{p^e} = b_0^{p^e} + b_1^{p^e} x^{p^e} + \ldots + b_{n-1}^{p^e} x^{(n-1)p^e} + x^{mp^e}$$

is in $k[x]$ so there exists an element b_i such that $b_i \notin k$ and $b_i^{p^e} \in k$. Therefore we take $s = b_i$. We have proven that if the extension K/k is not separable there exists an element $s \in K$ such that $s^{p^e} \in k$. Now, consider the tensor product $K \otimes_k K$ and take the element $(s \otimes 1) - (1 \otimes s)$. Then:

$$((s \otimes 1) - (1 \otimes s))^{p^e} = s^{p^e} \otimes 1 - 1 \otimes s^{p^e}.$$

But $s^{p^e} \in k$ so we have that

$$s^{p^e} \otimes 1 - 1 \otimes s^{p^e} = s^{p^e} \otimes 1 - s^{p^e} \otimes 1 = 0$$

so the element $s \otimes 1 - 1 \otimes s$ is nilpotent on $K \otimes_k K$ and K is not separable in the sense of k-algebras. Therefore, we have proven that the separability of k-algebras is actually a generalization of the separability of extensions.

The following result gives a characterization of separable k-algebras.

Proposition 1.5.2. *Let A be a finite k-algebra. The following are equivalent:*

i. A is separable.

ii. $A_{\overline{k}}$ is reduced, with $\overline{k}$ is an algebraic clousure of k.

iii. There exists an extension $k \to K$ such that A_K is a trivial K-algebra.

iv. There exists an extension $k \to K$ such that A_K is a separable K-algebra.

[1] Check [4, pp.10-18].

v. A_K is a separable K-algebra for any extension $k \to K$.

Proof. $i \implies ii$) By definition.
$ii \implies iii$) Any finite algebra which is reduced over an algebraically closed field is trivial by 1.3.9 so $A_{\overline{k}}$ is trivial.
$iii \implies iv$) There exists an extension $k \to K$ such that A_K is trivial and any trivial extension is separable.
$iv \implies v$) Let K be an extension of k such that A_K is a separable K-algebra and take L to be an arbitrary extension of k. If we prove that A_L is reduced then we will conclude that A_K is separable because among the arbitrary extensions of k we can find the extensions of K. Then, let us denote by KL the composite of K and L. Then, the morphism

$$A_L \to A_{KL}$$

is injective because $L \to KL$ is injective and, since $A_{KL} = A_K \otimes_K L$ is reduced it follows that A_L so is.
$v \implies i$) Trivial. ■

Proposition 1.5.3. *Any subalgebra of a separable finite algebra is separable.*

Proof. Let B be a subalgebra of A with A separable. Then B_K is a subalgebra of A_K so B_K is reduced whenever so is A_K. ■

Proposition 1.5.4. *Any quotient of a separable finite algebra is separable.*

Proof. If $f : A \to B$ is a surjective morphism of algebras, then B is a quotient of A. We may form the mapping $f \otimes id : A_K \to B_K$ which is onto, too. Indeed, let $\beta \otimes \lambda$ in B_K with $\beta \in B$ then there exists an element $\alpha \in A$ such that $f(\alpha) = \beta$ so there will be an element $\alpha \otimes \lambda$ such that $(f \otimes id)(\alpha \otimes \lambda) = f(\alpha) \otimes \lambda = \beta \otimes \lambda$. Then we can extend by linearity. Therefore, B_K is a quotient of A_K and it will be a trivial K-algebra whenever so is A_K. ■

Remark. Let us notice that in the proof above it is not used that A_K is reduced but trivial over K. In 1.5.2 we can see that the fact that A_K is trivial over K is equivalent to the fact that A is separable. Since A_K K-trivial implies B_K K-trivial we have that B is separable, which is what we wanted to prove.

Proposition 1.5.5. *The direct sum of two separable finite algebras is separable if and only if both summands are separable.*

Proof. $\Rightarrow$) It is a consecuence of the proposition above. The canonical morphisms $A \oplus B \to A$ and $A \oplus B \to B$ are epimorphisms, therefore A and B are quotients of $A \oplus B$ and the result follows.
$\Leftarrow$) Let A, B be finite k-algebras. Then $(A \oplus B)_K = A_K \oplus B_K$ is reduced if A_K and B_K are reduced. ■

Proposition 1.5.6. *The tensor product of two finite k-algebras is separable if and only if so are its factors.*

Proof. $\Rightarrow$) Let us take the separable k-algebra $A \otimes B$. Since A and B are its subalgebras they are separable as well.
$\Leftarrow$) Let A and B be two finite k-algebras. Then $(A \otimes_k B)_K = A_K \otimes_k B_K$ is trivial whenever so are A_K and B_K. ■

Proposition 1.5.7. *Any composite of two separable finite extensions is a separable finite extension.*

Proof. Each composite of two finite extensions is a quotient of its tensor product. So applying the previous propositions the result follows. ■

1.6 Metric of the trace

In this section we study a useful tool to determine whether a k-algebra is separable.

Let A be a finite k-algebra. Any element $a \in A$ defines a mapping $\phi_a : A \to A$ given by $\phi_a(x) = ax$, which is an endomorphism of k-algebras, that is, an endomorphism of k-vector spaces.

Definition 1.6.1. Let a be an element of the finite k-algebra A. We call the *trace* of a to the trace of the endomorphism ϕ_a:

$$tr_{A/k} : A \to k \text{ given by } tr_{A/k}(a) = tr(\phi_a).$$

which verifies $tr_{A/k}(1) = dim_k(A)$.

The trace is a linear form, so we can define the metric T in A given by:

$$T(a,b) = tr_{A/k}(ab)$$

which induces a *polarity* in A, *i.e.*, a linear form from A into its dual space A^*.

$$\omega : A \to A^* \text{ given by } a \longmapsto \omega(a) = T(a,-)$$

whose kernel is the radical of the linear form T.
Let K be an extension of k, the polarity above induces a polarity over the K-vector space A_K.

$$\overline{\omega} : A_K \to (A^*)_K$$

Remark. The dual space A^* of A is the set of linear functions $A \to k$. But linear functions are homomorphisms of vector spaces so $A^* = Hom_k(A,k)$. Let us note that $(A^*)_K = (A_K)^*$ which is a consequence of the natural isomorphism $Hom_k(V,W) \otimes K = Hom_K(V \otimes K, W \otimes K)$ with V,W k-vector spaces.

Proposition 1.6.2. *The polarity associated to the metric in A_K is $\omega \otimes id$.*

Proof. Let $a \in A$, then the endomorphism $\phi_{a\otimes 1}$ of A_K is $\phi_a \otimes id$. Indeed, let $\alpha = x \otimes y \in A_K$. $\phi_{a\otimes 1}(\alpha) = (a \otimes 1)(x \otimes y) = (ax \otimes y) = \phi_a(x) \otimes y = (\phi_a \otimes id)(x \otimes y)$. Since the trace of endomorphisms is invariant by changing the base field we get $tr_{A/k}(a \otimes 1) = tr_{A/k}(a) \otimes 1$. Then, the mapping $\omega \otimes id : A_K \to A_K^*$ is $(\omega \otimes id)(a \otimes b) = \omega(a) \otimes b = T(a,-) \otimes b$. ■

Proposition 1.6.3. *Let R be the radical of the metric of the trace of A, then $R \otimes_k K$ is the radical of the metric of the trace of the K-algebra A_K.*

Proof. Consider the following sequence of k-modules:

$$0 \to R \to A \xrightarrow{\omega} A^*$$

The kernel of ω is R which is also the image of the inclusion of R in A, hence the sequence is exact[2]. Since any free module is flat[3] and any vector space is free, any vector space is flat so K is flat as a k-vector space and preserves the exactness of sequences by tensorizing. Therefore, the following sequence is also exact:

$$0 \to R \otimes_k K \to A \otimes_k K \xrightarrow{\omega\otimes id} A_K^*$$

By exactness, $R \otimes_k K$ is the kernel of $\omega \otimes id$. ■

Proposition 1.6.4. *$Rad(A) \subset R$. Where $Rad(A)$ is the radical of the k-algebra A and R is the radical of the metric of the trace.*

[2] A sequence of morphisms $\ldots \to M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} \ldots$ is said to be exact if $Imf_i = Kerf_{i+1}$. [3, p.15;p.120]

[3] A module is said to be flat if it preserves exactness by tensorizing. [3, p.612]

Proof. Let $a \in A$ be nilpotent. Then $a^n = 0$ for some $n \in \mathbb{N}$. Take $b \in A$. Then ab is nilpotent, so, since the trace of a nilpotent endomorphism is null, $T(a,b) = tr_{A/k}(ab) = 0$. ■

Remark. The fact that $Rad(A) \subset R$ is the key point in this section. Indeed, what it says is that to find out whether an algebra A is reduced it is enough to check if the radical of its trace is zero.

Theorem 1.6.5. *A finite k-algebra is separable if and only if the radical of the trace is zero.*

Proof. $\Rightarrow$) Let A be a finite k-algebra which is separable. Then there exists an extension $k \to K$ such that A_K is trivial, so $A_K \simeq K \oplus \ldots \oplus K$. Its components K are ortogonal to each other with respect to the metric of the trace. The radical of the metric of trace of extensions with degree 1 is zero so the radical of the metric of A_K is zero. Therefore, because of 1.6.3, the radical of the metric of the trace of A is zero as well.
$\Leftarrow$) If the radical of the metric of A is zero, the radical of the metric of A_K is zero for any extension $k \to K$. Since the radical of the algebra is contained in the radical of the metric, we get that A_K is reduced. ■

Corollary 1.6.6. *A finite extension $k \to K$ is separable if and only if $tr_{K/k}$ is not zero.*

Proof. The radical of the metric of the trace of A is an ideal. Indeed, if $a \in A$ belongs to the radical, $T(a,b) = 0$ for any $b \in A$ so $T(ca,b) = T(a,cb) = 0$ for any $c \in A$. Therefore, if the radical of the metric of the trace of an extension K is not zero, it has to be K so the bilinear form $tr_{K/k} : K \to k$ is zero.
On the other hand, if $tr_{K/k}$ is zero, the metric of the trace is zero. By the theorem above, the extension is inseparable. ■

Corollary 1.6.7. *Any finite extension of a field with characteristic 0 is separable. Therefore, any reduced finite algebra over a field with characteristic 0 is separable.*

Proof. Let K be a finite extension of k with $char(k) = 0$. We have that $tr_{K/k}(1) = dim_k(A) \neq 0$ so K is separable.
By the Decomposition Theorem, any reduced finite k-algebra decomposes as a direct sum of its residual fields. It is already known that the direct sum of two finite algebras is separable if and only if its summands are separable. This can be easily extended to n summands. Then the result follows. ■

Corollary 1.6.8. *Let K be an inseparable finite extension. Then its degree is divisible by the characteristic of the base field.*

Proof. Let $k \to K$ to be such an inseparable finite extension. By 1.6.6 we have that $0 = tr_{K/k}(1) = \overline{dim_k(K)}$, where $\overline{dim_k(K)} = dim_k(K) + (p)$. So, since p divides $tr_{K/k}(1)$ then p divides $dim_k(K)$. ■

1.7 Finite fields

Let k be a field with characteristic p. It is clear that if the degree of k over $\mathbb{Z}/p\mathbb{Z}$ is n then k has p^n elements. Let us call $q = p^n$. The non-zero elements of k form a group with the multiplication whose order is $q-1$. Therefore, for any element x in this group, $x^{q-1} = 1$, that is, $x^{q-1} - 1 = 0$. So any element $x \in k$ verifies that $x^q - x = 0$.

Proposition 1.7.1. *In fields with char(p) $\neq 0$ the map $\phi : k \to k$ given by $\phi(x) = x^p$ is a morphism of fields.*

Proof. Let k be a field such that $char(k) = p \neq 0$ and take $a, b \in k$. Then $(ab)^p = a^p b^p$ and $(a+b)^p = a^p + b^b$ as the coefficients $\binom{p}{i}$ of the series $(a+b)^p$ are all divisible by p when $1 \leq p \leq p-1$. ■

Definition 1.7.2. Let K be a finite extension of k. We call the Fröbenius automorphism of K over k to the automorphism $F : K \to K$ given by $F(x) = x^q$ where q is the number of elements of K.

Remark. Note that this morphism fixes the elements of k: if $x \in k$ then $F(x) = x^q = x$ because $x^q - x = 0$. F is an automorphism because it is a morphism of fields, hence injective, which is also surjective because of the finiteness of K.

Theorem 1.7.3. *Let K be a finite extension of a finite field k. If $deg_k(K) = d$, the group of automorphisms of K over k is cyclic with order d and it is generated by the Fröbenius automorphism. Moreover, K_K is trivial.*

Proof. Let us notice that F may form a cyclic group of automorphisms of K over k. Its order will be the degree of the extension $k \to K$. If $deg_k(K) = 1$ it is clear that $F = id$ and the group will be $\langle 1 \rangle$. If $deg_k(K) = 2$ then it will have q^2 elements and it will be verified that $F(F(x)) = x$ if $x \in k$ and $F(F(X)) = x^{q^2} = x$ for any $x \in K$ so the cyclic group will be $\langle 1, F \rangle$ and this argument can be extended for K with $deg_k(K) = d$.
By 1.4.7 the number of automorphisms of K over k is equal to $deg_k(K)$ if and only if K_K is trivial. ■

Corollary 1.7.4. *Any finite extension of a finite field is separable. Therefore, any reduced finite algebra over a finite field is separable.*

Proof. Let K be a finite extension of k. Then $K \otimes_k K$ is trivial so K is separable.
When it comes about algebras, applying the Decomposition Theorem and 1.5.5 the result follows. ■

Remark. Let us take a look now from the point of view of the classical algebraic extensions theory. It happens that a field k is perfect if and only if either $char(k) = 0$ or $char(k) = p$ and $k^p = k$. The proof can be seen in [4, pp.9-10]. This, in particular implies that any finite field is perfect as we have proven in 1.7.4. Indeed, since the prime field of a field of characteristic 0 has finitely many elements, a finite field has to be of prime characteristic. This together with the fact that in a field of characteristic p the mapping which attaches x^p to any x is an automorphisms implies that a finite field is perfect. Note also that in 1.6.7 it is also proven that a field of characteristic 0 is perfect.

Chapter 2

G-sets and Galois Theory

2.1 G-sets

Definition 2.1.1. Let G be a group and let X be a set. We call *action of G on X* to any group morphism

$$\rho : G \to S(X)$$

where $S(X)$ is the set of bijections of X. If $g \in G$ and $x \in X$, we simply write gx to denote $\rho(g)(x)$. Since ρ is a group morphism, $\rho(gg')(x) = (gg')(x) = g(g'x) = \rho(g)\rho(g')(x)$.

Remark. Actually we call *action of G on X* to the map

$$\phi : G \times X \to X \text{ given by } (g,x) \longmapsto gx$$

which satisfies the following properties:

i $ex = x$ for any $x \in X$ where e is the unit in G.

ii $(gh)x = g(hx)$ for any $g,h \in G$ and $x \in X$

but if ρ is given by $\rho(g) = \phi_g : X \to X$ which takes x to gx then ρ is a group morphism. Indeed, let $x,y \in X$ then $\rho(gh)(x) = \phi_{gh}(x) = ghx = g(hx) = \phi_g(hx) = \phi_g(\phi_h(x)) = \rho(g)(\rho(h)(x))$. On the other hand, let ρ be a group morphism such that $\rho(g) = \phi_g$. The mapping $\phi(g,x) = \phi_g(x)$ is an action of G on X. So therefore we can consider ρ as an action.

Definition 2.1.2. A *G-set* is a set endowed with an action of the group G.

Definition 2.1.3. Let X,Y be G-sets. The mapping $f : X \to Y$ is said to be a *G-set morphism* if it verifies that

$$f(gx) = g(f(x))$$

for any $g \in G$ and $x \in X$. The set of G-set morphisms from X to Y is denoted by $Hom_G(X,Y)$.

For any subgroup $H \leq G$ we can consider an equivalence relation which induces the quotient G/H. This has a strucutre of G-set with the action of G given by $g(g'H) = gg'H$.
The G-sets G/H_1 and G/H_2 are isomorphic if and only if H_1 and H_2 are conjugate. Indeed, let us consider the mapping $G \to G/H_1$ given by $g \longmapsto gH_1g^{-1}$ which is a group morphism whose kernel is H_2 if and only if H_1 and H_2 are conjugate.

Definition 2.1.4. Let $\{X_i\}_{i\in I}$ be a family of G-sets.

i) We call *disjoint union* to the disjoint union $\bigoplus_{i\in I} X_i$ attached to the trivial action of G.

ii) We call *direct product* to their direct product $\prod_{i\in I} X_i$ endowed with the action of G induced by its action on each factor.

Proposition 2.1.5. *For any G-set Y it is verified that*

i) $Hom_G(\bigoplus_{i\in I} X_i, Y) = \prod_{i\in I} Hom_G(X_i, Y)$

ii) $Hom_G(Y, \prod_{i\in I} X_i) = \prod_{i\in I} Hom_G(Y, X_i)$

Proof. It can be easily seen by computing. ■

Any action of the group G on the set X defines an equivalence relation given by $x \sim y$ if there exists $g \in G$ such that $gx = y$. The equivalence classes are called *orbits* and denoted by $Orb(x)$. Since any element is contained in one orbit we get the following

Theorem 2.1.6 (Decomposition Theorem for G-sets)**.** *Any G set is isomorphic to the disjoint union of its orbits.*

Any element $x \in X$ defines a G-set morphism

$$\phi_x : G \to X \text{ such that } \phi_x(g) = gx$$

whose image is $Orb(x)$ and whose kernel is the *stabilizer* of x $G_x = \{g \mid gx = x\} \leq G$. Therefore, by the First Isomorphism Theorem $G/G_x \simeq Orb(x)$.

Definition 2.1.7. A G-set with just one orbit is said to be *connected*.

What have been said above proves the next

Proposition 2.1.8. *Any connected G-set is isomorphic to G/H for some subgroup $H \leq G$ which is the stabilizer of one of its elements.*

Let X be a G-set. We denote by X/G the set of orbits of X. We write X^G to denote the set of invariant elements of X under the action G, that is, those elements whose stabilizer is the whole G. Both X/G and X^G have a structure of G-sets with the trivial action of G, *i.e.*, any element $g \in G$ acts by the identity. This way the canonical morphisms

$$X \to X/G$$

and

$$X^G \to X$$

are G-set morphisms.
Note that if a group G acts on a k-algebra A by k-algebra automorphisms, A^G is a subalgebra of A. Indeed, let $\rho : G \to Aut_k(A)$ given by $g \to \rho(g) : A \to A$ automorphism. Since automorphisms over k are in particular k-module morphisms, $k \subset A^G$ so A^G is a subalgebra of A.

Proposition 2.1.9. *Let X be a connected G-set. For any G-set Y it is verified that*

$$Hom_G(X,Y) = \{\textit{Orbits of } X \times Y \textit{ isomorphic to } X \textit{ through the canonical projection } X \times Y \to X\}$$

Proof. Take a G-set morphism $f \in Hom_G(X,Y)$. It induces the morphism $id \times f : X \to X \times Y$ which is a section of the canonical morphism $\rho : X \times Y \to X$ because $\rho(id \times f)(x) = \rho(x, f(x)) = x$ for any $x \in X$. Therefore we get a 1-1 correspondence between the G-set morphisms from X to Y and the sections of the canonical morphism $\rho : X \times Y \to X$. Since X is connected, each section of ρ is an isomorphism between X and an orbit of $X \times Y$ which is isomorphic with X through ρ. Indeed, if X is connected it is an orbit by the *Decomposition Theorem*, so take an element $y \in X$. Then there exists $g \in G$ such that $y = gx$ with $x \in X$. Then $(id \times f)(y) = (y, f(y)) = (gx, g(f(x)))$ because f is a G-set morphism. But $(gx, gf(x)) = g(x, f(x))$ belongs to the orbit $Orb(x, f(x))$ in $X \times Y$, which is isomorphic to X through ρ because $\rho(x, f(x)) = x$ is an isomorphism. Reciprocally, any of such orbits defines a section of ρ. ■

2.2 Actions of $Aut_k(K)$ on $Hom_{k-alg}(A,K)$

We have seen in the previous chapter that the next equalities hold:

$$Hom_k(A,K) = Hom_K(A_K,K) =$$
$$= \{m \mid m \triangleleft_{max} A_K \text{ and } A_K/m \simeq K\} = \{\text{components of } A_K \text{ isomorphic to } K\}$$

Given an automorphism $g : K \to K$ over k, g induces an automorphism of $A \otimes_k K$ given by $\overline{g}(a \otimes \lambda) = (id \otimes g)(a \otimes g(\lambda))$. Therefore, the group of automorphisms of K over k acts on $A \otimes_k K$ hence it acts on its maximal ideals. We conclude that $G = Aut_k(K)$ acts on the four sets above.

Let $\pi : A_K \to K$ be the component of A_K associated to the maximal ideal $m \triangleleft_{max} A_K$. We call $g(\pi) : A_K \to K$ to the canonincal projection of A_K into the component associated to its maximal ideal $(id \otimes g)(m)$ (note that $(id \otimes g)(m)$ is also maximal because, in general, if $f : A \to A$ is an automorphism, B is an ideal if and only if so is $f(B)$). It follows that the following diagram is commutative:

$$\begin{tikzcd}
K \arrow[r] \arrow[d, "g"] & A \otimes_k K \arrow[r, "\pi"] \arrow[d, "id \otimes g"] & K \arrow[d, "g"] \\
K \arrow[r] & A \otimes_k K \arrow[r, "g(\pi)"] & K
\end{tikzcd}$$

It has been said before that $G = Aut_k(K)$ acts on $Hom_{k-alg}(A,K)$. Take $f \in Hom_{k-alg}(A,K)$ such that $\pi(a \otimes \lambda) = f(a)\lambda$ (this can be done because of 1.4.3) and $h \in Hom_{k-alg}(A,K)$ such that $g(\pi)(a \otimes \lambda) = h(a)\lambda$. Then we have

$$h(a) = g(\pi)(a \otimes 1) = (g(\pi) \circ (id \otimes g))(a \otimes 1) = (g \circ \pi)(a \otimes 1) = g(f(a))$$

so G acts on $Hom_{k-alg}(A,K)$ by composition:

$$g(f) = g \circ f.$$

2.3 Galois extensions

Definition 2.3.1. We say that a finite extension $k \to K$ is a *Galois extension* if the K-algebra $K \otimes_k K$ is trivial.

Remark. It is already known that if K_K is trivial, K is separable. Also, $Aut_k(K) = Hom_{k-alg}(K,K) = Hom_K(K_K,K) = \{m \mid m \triangleleft_{max} K_K$ such that $K \simeq K_K/m\}$ but, since K_K is trivial, by 1.3.5 the number of elements in this set is equal to $dim_k(K)$. That is, the number of automorphisms over k of a Galois extension K coincides with its degree over k.

Definition 2.3.2. The group $G = Aut_k(K)$ of the Galois extension K is called the *Galois group of K*.

Proposition 2.3.3. *Let $k \to K$ be a Galois extension with Galois group G. Then $K^G = k$.*

Proof. Since any finite k-algebra which is an integral domain is a field, K^G is a field. Now, any element G is an automorphism of K over K^G, then $G = Aut_k(K) \subset Aut_{K^G}(K) = Hom_{K^G}(K)$ and since $|Hom_{K^G}(K)| = dim_{K^G}(K)$ it follows that the degree of K over K^G is equal or greater than the order of G. But $|G| = |Aut_k(K)| = |Hom_k(K,K)| = deg_k(K)$ so $deg_k(K) \leq deg_{K^G}(K)$ so $K^G \subset k$. Since $k \subset K^G$ it follows that $k = K^G$. ■

Remark. In *classical Galois Theory* a finite extension K/k with Galois group G is said to be *Galois* if it is separable and normal, which is equivalent to the fact that $K^G = k$[1]. Then it is clear that our definition does not have any contradiction with the classical one.

Definition 2.3.4. Let a group G and a set X. We say that G acts transitively on X if for any $x, y \in X$ there exists an element $g \in G$ such that $gx = y$.

Lemma 2.3.5. *Let G be the group of automorphisms of a reduced finite k-algebra A such that A^G is a field. Then G acts transitively on the components of A.*

Proof. Assume G does not act this way. Since A is finite and reduced, by the *Decomposition Theorem* it decomposes as the direct sum of its components. They can be regrouped as the sum $A = B \oplus C$. Since G does not act transitively on A, it is easy to see that $A^G = B^G \oplus C^G$. But this would imply that A^G is not a field because the direct sum of two algebras always has zero divisors. ■

Lemma 2.3.6. *Let k be a field and G be the finite group of automorphisms of the k-algebra B. Then, for any k-algebra A, the morphism*

$$A \otimes_k (B^G) \to (A \otimes_k B)^G$$

is an isomorphism where G acts on $A \otimes_k B$ by $g(a \otimes b) = a \otimes g(b)$.

Proof. The definition of B^G implies the exactness of the following succession:

$$0 \to B^G \to B \xrightarrow{f} \bigoplus_G B$$

where $f(b) = (b - gb)_{g \in G}$. By the same argument used in the proof of 1.6.3 the k-algebra A is flat so it preserves exactness by tensorizing. Therefore the following succession is exact:

$$0 \to A \otimes_k (B^G) \to A \otimes_k B \xrightarrow{id \otimes f} \bigoplus_G (A \otimes_k B),$$

and exactness implies $A \otimes_k (B^G) \simeq (A \otimes_k B)^G$. ■

Corollary 2.3.7. *Let $k \to L$ and $k \to K$ be an extension and a Galois extension respectively. Then the L-algebra $K \otimes_k L$ decomposes as the direct sum of extensions which are isomorphic to each other.*

Proof. The L-algebra $K \otimes_k L$ decompose as the direct sum of extensions because K is a separable extension. To see that the extensions are isomorphic let us note that the Galois group of K acts transitively on them. Indeed, $(K \otimes_k L)^G = (K)^G \otimes_k L = L$ and due to 2.3.5 the result follows. ■

Theorem 2.3.8 (Prolongation Theorem)**.** *Let G be the Galois group of a Galois extension $k \to K$. If L is a finite extension of k it is verified that G acts transitively on $Hom_k(L, K)$ whenever it is not empty. That is, if f, f' are morphisms from L into K, there exists some automorphism g of K such that $f' = g \circ f$.*

Proof. We use the same argument used in the result above. G acts transitively on the components of $L \otimes_k K$ because $(L \otimes_k K)^G$ is a field and then we apply 2.3.5. ■

We have seen during this section that a Galois extension $k \to K$ with Galois group G satisfies that $K^G = k$. The following theorem gives us a sort of reciprocal by assuming that the extension K is separable and that $K^G = k$ where $G = Aut_k(K)$.

Theorem 2.3.9 (Artin's Theorem)**.** *Let G be a group of automorphisms of a separable finite extension $k \to K$. If $K^G = k$, then $k \to K$ is a Galois extension whose Galois group is G.*

Proof. Let us consider the action of G on $K \otimes_k K$ given by $g(a \otimes b) = g(a) \otimes b = ga \otimes b$. Then, $(K \otimes_k K)^G = (K^G) \otimes_k K = K$ so $(K \otimes_k K)^G$ is a field and, since the component of $K \otimes_k K$ associated to the identity is isomorphic to K, $K \otimes_k K$ is K-trivial. We conclude that K is a Galois extension.
G acts transitively on the components of $K \otimes_k K$ which are in correspondence with the automorphisms of K over k so G is the Galois group of K. ■

[1] [6, p.55].

2.4 The Galois Theorem

In this section we discuss the results which will allow us to formulate the *Galois Theorem* in terms of a particular kind of k-algebras and G-sets. As a consequence, our theorem will be more general than the one in the *classical Galois Theory*.

Let $k \to K$ be a Galois extension with Galois group G.

Definition 2.4.1. A finite k-algebra A such that A_K is a trivial K-algebra is said to be *trivial over* K.

Remark. Note that if A is trivial over K, then A is separable.

Let A be a finite k-algebra and let G be a group which acts on the k-algebra $A \otimes_k K$ by the identity on A and its natural action on K. Then

$$(A \otimes_k K)^G = A \otimes_k (K^G) = A \otimes_k k = A$$

so we can get back the k-algebra A from $A \otimes_k K$ and its action of G. When A is trivial over K it is enough to know the action of G on the components of A_K. Therefore we can recuperate A from the G-set formed by the components of A_K. More precisely, when A is trivial over K:

$$A \otimes_k K = \bigoplus_{P(A)} K$$

where $P(A)$ denotes the set of points of A with values in K. Since $P(A) = \{\text{components of } A_K\}$, under the action of G we get:

$$A = (\bigoplus_{P(A)} K)^G.$$

Definition 2.4.2. Let A be a finite k-algebra which is trivial over K. We will denote by $P(A)$ the finite G-set $Hom_{k-alg}(A,K)$ on which G acts as defined at the begining of this chapter. That is, $g(f) = g \circ f$.

Definition 2.4.3. Let $u : A \to B$ be a k-algebra morphism with A and B finite k-algebras which are trivial over K. We call $P(u) : P(B) \to P(A)$ to the G-set morphism given by $P(u)(f) = f \circ u$.

Remark. Actually, what we have defined is a *contravariant functor* P: $\mathscr{C} \to \mathscr{G}$ where $\mathscr{C}$ is the subcategory of k-algebras containing the finite k-algebras which are trivial over K and $\mathscr{G}$ is the category of G-sets.

Proposition 2.4.4. *P turns direct sums into disjoint unions.*

Proof. Take $\oplus_{i\in I}A$ with $\{A\}_{i\in I}$ a family of finite k-algebras trivial over K. Then $\oplus_{i\in I}A$ is also trivial over K. Indeed, $\oplus_{i\in I}A \otimes_k K = \oplus_{i\in I}(A \otimes_k K) = \oplus_{i\in I}(\oplus_i K)$. Now,

$$P(\oplus_{i\in I}A) = Hom_{k-alg}(\oplus_{i\in I}A, K) = Hom_{K-alg}(\oplus_{i\in I}A_K, K)$$

But $\oplus_{i\in I}(A_K) = \oplus_{i\in I}(\oplus_i K)$, so

$$Hom_{K-alg}(\oplus_{i\in I}A_K, K) = \{\textit{components of } \oplus_{i\in I}(\oplus_i K)\} = \bigsqcup Hom_{K-alg}(\oplus_i K, K) = \bigsqcup Hom_{K-alg}(A_K, K)$$

and the result follows. ■

Lemma 2.4.5. *The canonical k-algebra morphism $\phi : A \to \bigoplus_{P(A)} K$ given by $a \in A \longmapsto (f(a))_{f\in P(A)}$ satisfies that $im\phi = (\bigoplus_{P(A)} K)^G$.*

Proof. Let us first note that this map can be factorize in the following one:

$$A \xrightarrow{\phi} A \otimes_k K \xrightarrow{\alpha} \oplus_{P(A)} K$$

$$a \longmapsto a \otimes 1 \longmapsto (f(a))_{f\in P(A)}.$$

Take ϕ. Since G acts on $A \otimes_k K$ by the identity in A and the natural action on K, we have that $g(a \otimes 1) = a \otimes g(1) = a \otimes 1$. So therefore, A goes to $(A \otimes_k K)^G$ through ϕ. If we prove that the mapping α is a G-isomorphism, then we will have that $(A \otimes_k K)^G$ goes to $(\oplus_{P(A)} K)^G$.
Note that $\oplus_{P(A)} K = K^{P(A)} = K^{Hom_K(A_K,K)}$. Therefore α can be rewritten this way:

$$\theta : A_K \to K^{P(A)}$$

which in turn can be written as

$$\theta : A_K \to Hom(Hom_K(A_K, K), K)$$

given by

$$\alpha \longmapsto \theta_\alpha : Hom(A_K, K) \to K \text{ such that } \theta_\alpha(f) = f(\alpha).$$

We know how G acts on A_K so we translate its action to $K^{P(A)}$ such that

$$\theta_{g\alpha}(f) = g\theta_\alpha(f) = \theta_\alpha(gf)$$

and by the commutativity of the diagram in section 2.2 we know that $gf = g \circ f \circ (id \otimes g^{-1})$. We have therefore our G-isomorphism and $(A \otimes_k K)^G = (\oplus_{P(A)} K)^G$. ■

Definition 2.4.6. Let X be a finite G-set. G acts on the k-algebra $\bigoplus_X K$ in the following way: $g(\lambda_x)_{x \in X} = (g\lambda_{gx})_{x \in X}$. The finite k-algebra $R(X) = (\bigoplus_X K)^G$ is called the *associated algebra* of X.

Definition 2.4.7. Let $u : X \to Y$ be a G-set morphism with X, B finite G-sets. We call $R(u) : R(Y) \to R(X)$ to the k-algebra morphism which takes the succesion (λ_y) to the succession $(\lambda_{u(x)})$.

Remark. As before, R is induced from the contravariant functor $\mathscr{G} \to \mathscr{C}$

$$\begin{tikzcd}
X \arrow[r] \arrow[d, "u"'] & \bigoplus_X K \arrow[r] & (\bigoplus_X K)^G \\
Y \arrow[r] & \bigoplus_Y K \arrow[r] & (\bigoplus_Y K)^G \arrow[u, "R(u)"]
\end{tikzcd}$$

Note that it is being suppossed that $R(X)$ and $R(Y)$ are K-trivial k-algebras because $\mathscr{C}$ is the category of such k-algebras. This is because actually $R(X)$ is a finite k-algebra which is trivial over K for any G-set X. Indeed, since $R(X)$ is a subalgebra of $\oplus_X K$, $R(X) \otimes_k K$ is a subalgebra of $(\oplus_X K) \otimes_k K = \oplus_X (K \otimes_k K)$ which is trivial over K so it is a trivial K-algebra as K is Galois.

Proposition 2.4.8. *R turns disjoint unions into direct sums.*

Proof. $R(\sqcup_i Y) = (\oplus_{\sqcup Y} K)^G = (\oplus_i(\oplus_{Y_i} K))^G = \oplus_i(R(Y_i))$. ■

Lemma 2.4.9. *Let $H \leq G$ be a subgroup. The k-algebra $R(G/H)$ is isomorphic to K^H.*

Proof. Take the k-algebra morphism

$$\phi : K^H \to \bigoplus_{G/H} K$$
$$\lambda \longmapsto (g\lambda)_{g \in G/H}$$

Since λ is invariant under the action of H, ϕ is well defined because it does not depend on the chosen representant of the equivalence class $\overline{g}$. This map is injective because in one of the entries of the tuple we can take the unity as a representant of the equivalence class and we will have an equality. Since $P(K^H) = G/H$ we apply 2.4.5 and the First Isomorphism Theorem and the result follows. ■

Theorem 2.4.10 (Galois Theorem)**.** *Let G be the Galois group of a Galois extension $k \to K$. Then the finite k-algebras which are trivial over K are in canonical correspondence with the finite G-sets. More precisely:*
If A is a finite k-algebra which is trivial over K, the canononical morphism

$$A \to R(P(A))$$

is a k-algebra isomorphism. And if X is a finite G-set, the canonical morphism

$$X \to P(R(X))$$

is a G-set morphism.
Moreover, if A and B are in $\mathscr{C}$, P verifies a bijection

$$Hom_{k-alg}(A,B) = Hom_G(P(B),P(A))$$

whose inverse is induced by R.

Proof. Let A be a finite k-algebra trivial over K. In 2.4.5 it has been proven that $A \to R(P(A))$ is an isomorphism.
On the other hand, remember than P turns direct sums into disjoint unions and R do the opposite. Therefore, it is enough to consider a connected G-set X to prove that $X \to P(R(X))$ is a G-set isomorphism. Indeed, if X is not connected it is isomorphic to the disjoint union of its orbits and R takes them to its direct sum but P takes them back to its disjoint union. Therefore, take a connected G-set X. By 2.1.8 X is isomorphic to G/H for some $H \leq G$. Then, by 2.4.9, $K^H \simeq R(G/H) = R(X)$. Now, since K^H is a finite extension, by the Prolongation Theorem, G acts transitively on $Hom_{k-alg}(K^H,K) = P(K^H)$ which means that $P(K^H)$ is connected. But we can consider the mapping $G = Hom_k(K,K) \to Hom_k(K^H,K)$ which attaches to any $f \in Hom_k(K,K)$ its restriction $f_{K^H} \in Hom_k(K^H,K)$ which is an epimorphism so it can be factorize through $G \to G/\sim \xrightarrow{\varphi} Hom_k(K^H,K)$ where the equivalence relation $\sim$ is given by $g \sim g'$ if and only if $\varphi(g) = \varphi(g')$ which happens if and only if the restriction of both g, g' to K^H is the same function, that is, if $g(x) = g'(x)$ for any $x \in K^H$ if and only if $(g')^{-1}g(x) = x$ for any $x \in K^H$ if and only if $(g')^{-1}g \in H$. Therefore, we get that $G/\sim$ is actually G/H and we get that $G/H \simeq Hom_k(K^H,K) = P(K^H)$. It follows that $X \to P(R(X))$ is an isomorphism.

Now take $A, B \in \mathscr{C}$. We can suppose that B is a finite extension $k \to L$ trivial over K. Then, applying what we have seen above and 2.1.9:

$$Hom_{k-alg}(A,L) = \{\textit{components of } A \otimes_k L \textit{ isomorphic to } L\} =$$

$$= \{\textit{orbits of } P(A \otimes_k L) \textit{ isomorphic to } P(L)\} = \{\textit{orbits of } P(A) \times P(L) \textit{ isomorphic to } P(L)\} =$$

$$= Hom_G(P(L),P(A)).$$

■

Remark. The fact that we can factorize the mapping $G \to Hom_k(K^H,K)$ as we do in the proof above comes from the commutativity of the diagram below, where the equivalence relation is the one given in the proof.

$$\begin{tikzcd}
G \arrow[r, "\varphi"] \arrow[d, "supr."'] & Hom_k(K^H,K) \\
G/\sim \arrow[r, "bij."'] & Hom_k(K^H,K) \arrow[u, "inject."']
\end{tikzcd}$$

Remark (The Galois Theorem in classical Galois Theory). Given a Galois extension K of k, the classical Galois Theorem establishes a 1-1 correspondence between the intermediate fields $k \subset L \subset K$ and the subgroups of the Galois group G of K such that L is related to $Gal(K/L)$. Let L be such an intermediate extension, then it is of course a k-algebra which also splits on K because K is Galois and K_K is K-trivial. Now, P$(L) = Hom_k(L,K)$ which is actually a connected G-set, but any connected G-set X is isomorphic to G/H where H is the stabilizer of an element $x \in X$. Then $P(L)$ is isomorphic to G/H where $H = Gal(K/L)$. Thus, we are attaching L to $Gal(K/L)$. Therefore, the classical Galois Theorem is contained in our new Galois Theorem.

2.5 Galois envelope

Definition 2.5.1. Let $k \to L$ a finite extension. We call *Galois envelope of* L over k to any extension $k \to K$ verifying the following:

i) K is a composite of L.

ii) L is trivial over K.

Remark. Definition 1.2.3 gives us a definition of the composite of two k-algebras K, L given the morphisms of algebras $K \to E$ and $L \to E$. This one is slightly different: given two k-algebras K and L, we say that K is the composite of L if K is the image of some tensor product of L. That is, if K is a quotient of some tensor product of L.

Proposition 2.5.2. *Let K be the Galois envelope of a finite k-algebra L. Then K is a Galois extension. Moreover, $|Hom_{k-alg}(L,K)| = dim_k(L)$.*

Proof. Since K is a quotient of some tensor product of L, let us say $L^{\otimes n}$ for some $n \in \mathbb{N}$, then $K \otimes_k K$ is a quotient of $L^{\otimes n} \otimes_k K$. But, by *ii)* $L \otimes_k K$ is a trivial K-algebra. If we assume that $L^{\otimes n-1} \otimes_k K$ is trivial, then so is $L^{\otimes n} \otimes_k K = L \otimes_k L^{\otimes n-1} \otimes_k K$. Then $K \otimes_k K$ as a quotient of $L^{\otimes n} \otimes_k K$ is also a trivial K-algebra and we conclude that $k \to K$ is Galois.
Now, $|Hom_{k-alg}(L,K)| = |\{components\ of\ L \otimes_k K\ isomorphic\ to\ K\}| = dim_k(L)$ because $L \otimes_k K$ is K-trivial. ■

Theorem 2.5.3. *Any separable finite extension has a Galois envelope which is unique up to isomorphism.*

Proof. *Existence*. Let $k \to L$ be a separable finite extension. If L is trivial over itself, that is, if $L \otimes_k L = \oplus L$ then L is Galois and it is its own envelope. Let us assume now that L is not that way. Then there would exist L' such that $L \otimes_k L = L \oplus \ldots \oplus L \oplus L' \oplus L \oplus \ldots \oplus L$. Therefore: $L \otimes_k L' = L \otimes_k (L \otimes_L L') = (L \otimes_k L) \otimes_L L' = (L \otimes_L L') \oplus \ldots \oplus (L \otimes_L L') \oplus (L' \otimes_L L') \oplus (L \otimes_L L') \oplus \ldots (L \otimes_L L') = L' \oplus \ldots \oplus L' \oplus (L' \otimes_L L') \oplus L' \ldots \oplus L'$. This implies that there are more components of $L \otimes_k L'$ which are isomorphic to L' than components of $L \otimes_k L$ which are isomorphic to L because there is a component of $L' \otimes_L L'$ which is isomorphic to L'. Now, we apply a descent argument: if L is not trivial over L' and L'' is a component of $L \otimes_k L'$ which is not isomorphic to L' there are more components of $L \otimes_k L''$ which are isomorphic to L'' than components of $L \otimes_k L'$ isomorphic to L'. This process is finite because the number of components of $L \otimes_k L^i$ is bounded by $deg_k(L)$. We do this until we find a composite K of L such that L is trivial over K.
Uniqueness. Let K and K' be two Galois envelopes of the extension $k \to L$. Then K' is a quotient of some tensor product of L, $L^{\otimes n}$ $n \in \mathbb{N}$, so $K \otimes_k K'$ is a quotient of $K \otimes_k L^{\otimes n}$ which is a trivial K-algebra so it follows that K' is trivial over K. Therefore, there exist morphisms $K' \to K$ and $deg_k(K') \leq deg_k(K)$. We proceed analogously for K and get $deg_k(K) \leq deg_k(K')$. Then any morphism $K' \to K$ is an isomorphism. ■

Lemma 2.5.4. *Let K, L be Galois extensions of a field k. Then, all their composites are Galois extensions of k isomorphic to one another.*

Proof. Let KL be a composite of K and L. K is Galois so it is trivial over K. Note now that through the morphism $K \to K \otimes_k L \to KL$ we get that KL is a quotient of K so $K \otimes_k KL$ is a quotient of $K \otimes_k K$ so K is trivial over KL. Analogously we get that L is trivial over KL. Therefore $K \otimes_k L$ is trivial over KL. Hence all the composites of K and L are trivial over KL because all of them are quotients of $K \otimes_k L$. In particular KL is trivial over itself so it is Galois. Since any composite of K and L admits morphisms in KL and KL is an arbitrary composite, all of them have the same degree over k and any of such morphisms is an isomorphism. ■

Definition 2.5.5. Let A be a separable finite algebra. We call the *Galois envelope of A* to the composite of all the Galois envelopes of its components.

Remark. Note that since A is a separable finite algebra it decomposes into its components by the *Decomposition Theorem*.

Remark. By the previous lemma, the Galois envelope of A is actually a Galois extension K such that A is trivial over K and it is the smallest extension with this property. Now, if A is a separable extension of k, by 2.5.3 the Galois envelope is unique up to isomorphism. In terms of the classical Galois Theory, the Galois envelope of a separable extension is the normal closure.

Bibliography

[1] J.A. NAVARRO GONZALEZ, *Teoría de Galois*, Universidad de Extremadura, 1984.

[2] M.F. ATIYAH, I.G. MACDONALD, *Introduction to Commutative Algebra*, Perseus Books, Cambridge, Massachussetts, 1969.

[3] S. LANG, *Algebra*. Third Edition, Springer, 2002.

[4] P.J. MCCARTHY, *Algebraic Extensions of Fields*, Blaisdell Publishin Company, 1966.

[5] F. MONTANER, *course notes Galois Theory*, Universidad de Zaragoza.

[6] A. ELDUQUE, *course notes Algebra (Groups and Galois Theory)*, Universidad de Zaragoza. `http://www.unizar.es/matematicas/algebra/elduque/files/AlgebraElduque2010.pdf`

[7] F. BORCEUX, G. JANELDIZE, *Galois Theories*, Cambridge University Press, 2001.

[8] I. STEWART, *Galois Theory*, Third Edition, Chapman & Hall, 2004.

Index