THE MYSTERIOUS STRENGTH OF THE GALOIS THEORY

Jean-Jacques Szczeciniarz

Paris Diderot University

Contents

1 Introduction

1-1- Philosophical and historical Introduction

My aim is to present some issues concerning the situation of the Galois theory in the contemporary mathematical corpus. I want to restrict myself to a preliminary treatment of

certain questions questions and I would like to propose a few possible approach rather than some results. Let us consider this scheme. It will help to orient our thinking. I will focus on the left center column that leads up from Galois to Grothendieck. The main feature of my paper is to explain the main elements of the mathematical theory but in such a way that the explanation will be interfaced with a philosophical comment.

At first glance I would say, as Borceux and Janelidze do in their book *Galois Theories* (Cambrige University Press 2001)[BJ] : "Evariste Galois would certainly be surprised to see how often his name is mentioned in the mathematical books and articles of the twentieth century in topics which are so far from his original works". I suffices to consider the scheme.

We generally consider Galois theory as the classical polynomial theory we know and only during the nineteenth century did the problem of equations of higher degree reached a final answer: the impossibility of solving by radicals a general equation of degree at least 5, and some method for finding some solutions by radicals when these exist. [BJ]. The work by Lagrange, Ruffini, Van der Monde were very important contributions to this problem. I cannot deal directly with the "resolvant" of Galois and I will not treat directly the work by Camille Jordan, *Traité des substitutions*[CJ]. But we could say that the authentic Galois theory lies in these topics.

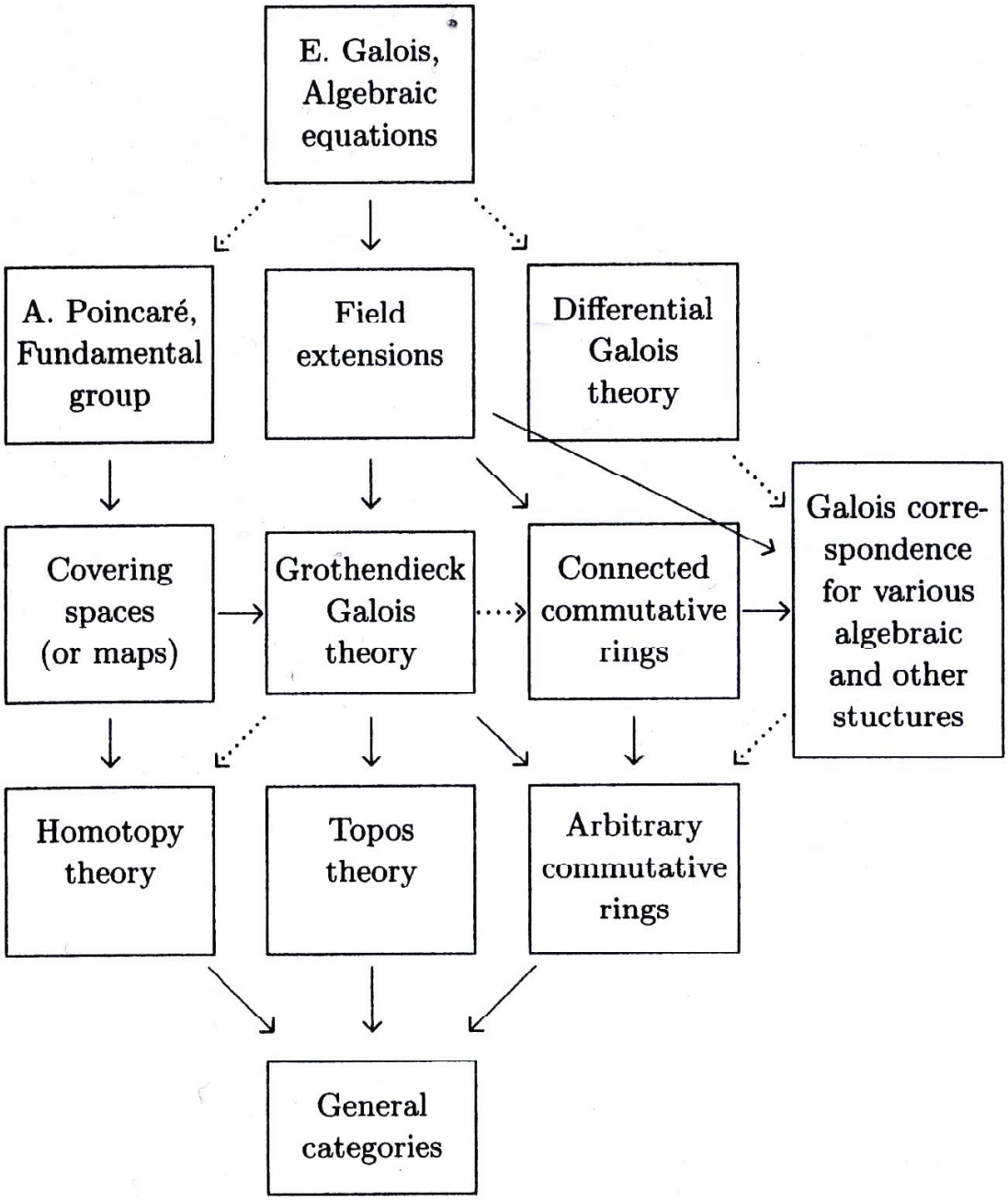
I would like to try to present and to measure the distance between this nineteenth century theory and Grothendieck theory.

I want to explore what Galois theory's or Galois theories' power or strength consists in. My philosophical thesis would be that Grothendieck is rebuilding Galois theory in his frame of Category theory and Algebraic Geometry. But this new framework is itself present in the classical Galois theory. How is it possible? Mathematical concepts or structures have two essential faces: the face through which they lie inside their own discipline (geometry, algebra, arithmetic, etc.) the face through which they are linked to other disciplines and this at different levels. Taking into account this double face is the main feature of the Galois theory, The concept which is essential in this view is the concept of Galois correspondence. It constitues a correspondence (functor) between two algebraic structures (categories) groups and fields and is the basis of all Galois theories. I will present some considerations to help us to understand this mathematical fact.

1-2 Remark on method

A strong peculiarity of those developments about solving equations is that the methods used to reach the final goal proved to be more interesting than the problem to be solved. Nobody uses the formulae for solving cubic or quartic equations. .. but their considerations forced the discovery of complex numbers. And the impossibility proof for equation of higher degree led to specifying the notion of group...[BJ vii]

The *phenomenon* of the superiority of the methods on the objectives to be reached is a



Scheme 1: The contexts of Galois theories

very important one. I can give at least two reasons for that.

First the analysis of the target leads to much more deep and complex concepts. It is the case of a polynomial and, much more striking, the case of the link with symmetric functions.

Secondly, such an analysis leads to the establishing of more and more links within the whole mathematical corpus. What is important in such theories (like Galois) is their ability to mobilize many other mathematical concepts or even other intramathematical theories. The spirit of the Galois theory is and this at the starting point, to be a not solely intra - but also intermathematical theory. Even if we remain focussed on the polynomial theory it is open on the theory of the relations between the roots and on the links between polynomials and symmetric functions. [Edwards p 9][Stewart , GT p. 87]

Nevertheless, for this reason I am not at second glance convinced that Galois would be so surprised by the constant mention of this theory. What I will try to remain the reader is that Galois theory encountered extraordinary, unexpected (or even unexpectable) developments, and these developments have been proved necessary. From the point of view of the History of Mathematics the developments are unforeseeable. [Jean Cavaillès]. But after the new construction has been successful we have to deal with the necessity of this contingency, which also constitutes the features of Galois theories and their links. The necessity lies at the level of the conceptual links, obviously not at the level of the empirical emergence of the new theory. But I would like to suggest that Galois theory involves through its main theorems the most important so called "degree of virtuality".

1-3- Quotation by Grothendieck

Before my analysis, I have to recall some extracts from *Récoltes et Semailles*:

> "$\cdots$ Désolé d'avoir l'air de vouloir me singulariser plus qu'il ne paraît permis! A mon propre soulagement je crois pourtant discerner une sorte de frère potentiel (et providentiel!) J'ai déjà eu tantôt l'occasion de l'évoquer, comme le premier dans la lignée de mes frères de tempérament, c'est Evariste Galois, dans sa courte et fulgurante vie, je crois discerner l'amorce d'une grande vision, celle justement des épousailles du nombre et de la grandeur dans une vision géométrique nouvelle. J'évoque ailleurs dans *Récoltes et Semailles* comment il y a deux ans est apparue en moi cette intuition nouvelle que le travail mathématique qui à ce moment exerçait sur moi la fascination la plus puissante j'étais en train de reprendre l'héritage de Galois". Cette intuition rarement évoquée depuis, a pourtant eu le temps de mûrir en silence.$\cdots$ La filiation la plus directe que je crois reconnaître à présent avec un mathématicien du passé, est bien celle qui me relie à Evariste Galois. A tort ou à raison, il me semble que cette vision que j'ai développée pendant quinze années de ma

> vie, et qui a continué de mûrir en moi et à s'enrichir pendant les seize années écoulées depuis mon départ de la scène mathématique- que cette vision est aussi celle que Galois n'aurait pu s'empêcher de développer s'il s'était trouvé dans les parages à ma place, et sans qu'une mort précoce ne vienne brutalement couper court un magnifique élan"
>
> [**Alexandre Grothendieck**]*Récoltes et semailles***p. 70**

After the new theories are elaborated and proved, it becomes necessary to admit that they are the theories Galois would have from himself developed. And the mathematical thought has to convince us that this is the case.

2 Classical Galois theory and some Generalizations

In the first part I recall what the classical Galois theory consists in. The elementary concepts of normality and separability are displayed. I will try to give an epistemological and philosophical comment on the Galois correspondence and explain why its abstract development was pertinent.

Let $K \subseteq L$ be an algebraic field extension. An element $I \in L$ is called *algebraic* over K when there exists a non-zero polynomial $p(X) \in K[X]$ such that $p(I) = 0$ The extension $K \subseteq L$ is called *algebraic* when all elements of L are algebraic over K

2.1 The main question and its significance

The essential question was to find the roots of a polynomial; but we should also ask what is the meaning of the search for the roots. This implies the setting up of all possible links between the indeterminates and the coefficients of the polynomial. There exists in the "substance" of a polynomial some power of exploration which is localized in the relation between the coefficients (that are known) and some symmetrical links between the roots (or unknown). This trend is originated in the original Galois work and goes from Newton, Gauss, Lagrange, and Galois' work on symmetric fonctions and polynomials until Lagrange's and Galois 's resolvent.

I will focus on the field extension. What does exactly this extension mean? It is an extension of a set of elements provided with the field structure in a greater set, so that one can dispose roots of a polynomial, roots which were not in the basic field (the field where the coefficients take their values). I will explain what the extension consists in, but the theory of extensions represents a second way the Galois theory is developed, namely as a theory of the extensions of algebraic structures. These structures are so to say a way

of getting the conditions to make possible some operations. Theory has to postulate the existence of such a structure where splitting a polynomial is effective, the splitting field.

2.2 The abstract turn of the Galois theory

In this new trend the attention of the work on the polynomial symmetries becomes secondary, it even remains a remote background. I remain the reader of the basic theorem that is a transition from the polynomial Galois theory to the structuralist, abstract Galois theory. The Dedekindian tradition, which has dominated for the last century formulates Galois theory in the following way. A group is associated not to an equation $f(x) = 0$ with coefficients in K but to a normal extension $K \subseteq L$, noticed $L : K$. The group, denoted $Gal[L : K]$associated to the normal extension $K \subseteq L$ is all automorphisms of L which leaves elements of K fixed. Focussing on this idea I can summarize in the following manner. With any polynomial Galois associated a group of permutations of its zeros (group concept existed only in rudimentary form). But the group that becomes the main concept is the group of all automorphisms of L for an extension $K \subseteq L$ which fixes the elements of K. Namely the group we named group of K-automorphisms of L. The concept of group has been transferred to the set of all K-automorphisms of L. And then if $L : K$ is an extension $K \subseteq L$ what is important is that to any intermediate extension $L : M$ such that $K \subseteq M \subseteq L$ one associates the group $Gal[M : K]$ of all M-automorphisms of L. This is in this direction that I am going to develop my paper.

Theorem [Simple Algebraic Extensions]. Let K be a given field and let $G(X)$ be an irreducible polynomial with coefficients in K. Then one can construct a field $K(t)$ such that: (1) $K(t)$ contains K

(2) $K(t)$ contains an element t which is a root of G, that is which satisfies $G(t) = 0$, and

(3) every element of $K(t)$ can be expressed as a polynomial in t with coefficients in K, that is, given any $x \in K(t)$ there is an integer ν and an element $b_0, b_1, \cdots b_\nu$ of K such that $x = b_0 + b_1 t + \cdots + b_\nu t^\nu$.

Comment. This theorem explains what the algebricity consists in. Algebraic means to contain the zeros of a polynomial.

2.3 Galois extension

. We need the extension of a field K on a field L possesses two main features in order to make possible the concept of the Galois group: separability and normality.

2-3-1 Separable extension Let us recall that the derivative of a polynomial

$$p(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_2 X^2 + a_1 X^1 + a_0$$

in $K[X]$ is the polynomial

$$p'(X) = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + 2a_2X + a_1$$

$p'(X)$ has degree $n-1$ if and only if the characteristic of K does not divide n.

Proposition Let K be a field and an element $a \in K$ and a polynomial $p(X)$ in $K[X]$. The following conditions are equivalent

i) a is a multiple root of $p(X)$

ii) $p(a) = 0$ and $p'(a) = 0$

Definition

A field extension $K \subseteq L$ is separable when

(i) the extension is algebraic

(ii) the roots of the minimal polynomial of every $l \in L$ are all simple.

Comment. The simplicity is a condition of splitting for the polynomial. And correlatively it corresponds to the algebraic construction of the extension. I recall, like [BJ p. 5]

Proposition Let $K \subseteq L$ be a field extension in characteristic zero. If $L \in L$ is algebraic over K, all roots of the minimal polynomial of l over K are simple.

Corollary In characteristic zero all algebraic extensions are separable

Proposition Let $K \subseteq M \subseteq L$ be field extensions. If $K \subseteq L$ is separable then $M \subseteq L$ is separable as well.

[**comment**] What is remarkable is the fact that the property of separability carries over intermediate fields. It prepares the game for the Galois correspondence.

2-3-2 Normal extension

Definition

A field extension $K \subseteq L$ is normal when

(i) the extension is algebraic

(ii) for every element $l \in L$ the minimal polynomial of l over K factors entirely in $L[X]$ in polynomial of degree 1.

An algebraic field extension $K \subseteq L$ with L algebraically closed is necessarily normal.

3 Abstract field extension

Remark. Inseparability

Let K be a field of characteristic $p > 0$, the map $\phi K \to K$ defined by $\phi(k) = k^p$ with $(k \in K)$ is the Frobenius monomorphism or *Frobenius map* of K.

When K is finite, ϕ is called *the Frobenius automorphism* of K. We use the Frobenius map to give an example of an inseparable polynomial. Let $K_0 = Z_p$, for prime p. Let $K = K_0(u)$ where $u$is transcendental over K_0 and let

$$f(t) = t^p - u \in K[t]$$

Let Σ be a splitting field for f over K, and let τ be a zero of f in Σ.Then $\tau^p = u$. according to the Frobenius map we get

$$(t - \tau)^p = t^p - \tau^p = t^p - u = f(t)$$

Thus if $\sigma^p - u = 0$ then $(\sigma - u)^p = 0$, so that $\sigma = \tau$.

All the zeros of f in Σ are *equal*. (According Jan Stewart [GT p. 184]).

Let us show that f is irreducible over K. Suppose that $f = gh, g, h, \in K[t]$ and g has lower degree than f. We must have $g(t) = (t - \tau)^s, 0 < s < p$ by uniqueness of factorization. Hence the constant coefficient τ^s of g lies in K.This [J Stewart] GT ibid.] implies that $\tau \in K$ for there is integer a and b such that $as + bp = 1$ and $\tau^{as+bp} \in K$ it follows that $\tau \in K$. Then $\tau = v(u)/w(u), v, w \in K[u]$. Then

$$v(u)^p - u(w(u))^p = 0$$

The terms of highest degree cannot cancel. Hence f is irreducible.

Comment on the irreducibility. Considering this case it becomes clear why we need to specify the separability. Why such a case can exist in the case of finite characteristic? There exists a condition on f for inseparability over fields of characteristic p. Only powers of t that are multiples of p occur.

I would claim that the simplicity of roots makes possible the construction of the Galois group, as permutation group of the roots.

4 Classical Galois theory the point of view of morphisms

Definition Let $K \subseteq L$ be an algebraic field extension. A field homomorphism $f : L \to L$ is called a K-homomorphism when it fixes all elements of K, that is, $f(k) = k$ for every element $k \in K$.

Comment . The starting point of the theory consists in considering automorphism of field modulo points in the basic field that are fixed by this morphism. The fixed point of the start are points lying in a basic field so that we get automorphisms of L modulo fixed points that are elements of a subfield of the field L. When one has in mind the polynomial, the coefficients that are in the basic field are fixed, and the roots are moved.

I would like to develop this remark. The difference between the fixed elements and the moved ones is important. The permutations allow us to distinguish the block of roots. It is another kind of invariance, they are identified modulo this permutation group.

Consider any quartic with the roots $\alpha, \beta, \gamma, \delta$. consider three subfields of C related to $\alpha, \beta, \gamma, \delta$, namely

$$K \subseteq K(\gamma, \delta) \subseteq K(\alpha, \beta, \gamma, \delta)$$

Let $H = \{I, R\} \subseteq G$. Stewart asks to assume that we also know :

1- The numbers fixed by H are precisely those in $K(\gamma, \delta)$.

2- The numbers fixed by G are precisely those belonging to K.

In this way we can work out how to solve the quartic equation $g(t) = 0$. We know (it is presupposed) that the numbers $\alpha + \beta, \alpha \cdot \beta$ are fixed by H.These numbers are coefficients of the quadratic equation:

$$(t - \alpha)(t - \beta) = t^2 - (\alpha + \beta)t + \alpha \cdot \beta,$$

and according 1 they lie in $K(\gamma, \delta)$. Then α, β satisfy this quadratic equation whose coefficients are in $K(\gamma, \delta)$. It becomes possible to express α, β in terms of rational functions of γ, δ, and to obtain α, β as radical expressions in γ and δ. It is matter to be noticed that H fixes the elements of the subfield in which the coefficients of the polynomial lie and that these coefficients are rational functions of the roots that are to be found. If we are repeating the same analysis to find γ and δ, the numbers $\gamma + \delta$ and $\gamma \cdot \delta$ are fixed by the whole G. I recall that R interchanges α and β, and I notice S the subgroup that interchanges γ and δ. Then $\gamma + \delta$ and $\gamma \cdot \delta$ are fixed by the whole G and then are fixed by R and by S. And these numbers belong to K, Stewart takes Q as basic field. The Galois subgroup fixed the field which contains the coefficients of the polynomial $g(t)$ and interchanges the roots lying in the immediate extension. Here γ and δ satisfyng a quadratic equation over $K = Q$ so they are given by radical expressions in rational numbers.

Comment The subgroup structure of the Galois group is related to the possibility of solving the equation $g(t) = 0$. This specific structure, group fixing the coefficients of the polynomial and a then a rational function of the roots and at the same time interchanging these roots was discovered by Galois. He understood the link between rational function of the roots and group fixing or not the roots on which it acts.

4.1 The abstract setting (J Stewart)[GT . 90]

The abstract modern approach follows Galois in principle (the symmetries of the polynomial are in the background) it differs in practice, says Stewart, [Stewart] in theory also.

The permutations of $\alpha, \beta, \gamma, \delta$ that preserve the algebraic relations between them are actually the symmetry group of the subfield $K(\alpha, \beta, \gamma, \delta)$ of C generated by the zeros of g, or more precisely its automorphism group.

Comment. There is a change of point of view: we consider the polynomials not just with integer or rational coefficients, but coefficients that lie in a subfield K of C (or Stewart says, any field). The zeros of a polynomial $f(t)$ with coefficients that lie in K determines another field L which contains K but may well be larger.

Thus the primary object of consideration is a pair of fields $K \subset L$ or in a slight generalization, a field extension of L. When Galois talks of polynomial, the modern approach talks of field extension. And the Galois group of the polynomial becomes the group of K-automorphisms of L. Thus, John says, the bulk of the theory is described in terms of fields extensions and their groups of K-automorphisms. This point of view was introduced by Dedekind in 1894, when presented subring and subfield of C in an axiomatic way. And then the roots of a polynomial are viewed as the support of morphisms that permute them. A field extension is also viewed as a monomorphism.

4.2 The point of view of morphisms to be continued

Let us introduce some notations and constructions.

Let $K \subseteq L$ be a Galois field extension.

Given an intermediate field extension $K \subseteq M \subseteq L$ we consider the Galois group $Gal[L : M] = Aut_M L$ of those automorphisms of L which fix M.

Given a subgroup $G \subseteq Gal[L : K]$, we write

$$Fix(G) = \{l \in L | \forall g \in G \; g(l) = l\}$$

$Fix(G)$ is a subfield of L since each $g \in G$ is a field automorphism, and it contains K since each $g \in G$ is a K-automorphism $K \subseteq Fix(G) \subseteq L$.

Remark I will present some features of the concept of functor.

1- Category. I recall: a category has objects, $A, B, C, \cdots$, and arrows, $f, g, h, \cdots$, To say that g goes from A to B we write $g : A \to B$, or say that A is the*domain* of g, and B the *codomain*. We may write $Dom(g) = A$ and $Cod(g) = B$. Two arrows f and g with $Dom(f) = Cod(g)$ are called $composable$ then we must have a *composite*, and an arrow called $f \circ g$

2- Functor. A functor $\mathbf{F}$ from a category $\mathbf{A}$ to a category $\mathbf{B}$, written $\mathbf{F} : A \to B$ assigns to each object A of $\mathbf{A}$ an object $\mathbf{F}A$ of $\mathbf{B}$ and to each arrow f of $\mathbf{A}$ an arrow $\mathbf{F}f$ of $\mathbf{B}$ meeting the following conditions.

It preserves domains and codomains: given $f : A \to B$ we have $\mathbf{F}f : \mathbf{F}A \to \mathbf{F}B$.

It preserves identities: for any A of $\mathbf{A}$, $\mathbf{F}(1_A) = 1_{\mathbf{F}A}$

It preserves composition : if f and g are composable in $\mathbf{A}$ then $\mathbf{F}(g \circ f) = \mathbf{F}g \circ \mathbf{F}f$ where the second composite is formed in $\mathbf{B}$.

3- Adjoint functor. Let C, D be two categories and $\mathbf{F} : C \to D$ and $\mathbf{G} : D \to C$ be two functors. The functor $\mathbf{F}$ is left adjoint of $\mathbf{G}$ that is right adjoint of $\mathbf{F}$, if for all object X of C and for all object Y of D, we have a functorial bijection

$$Hom_{\mathcal{D}}(\mathbf{F}X, Y) \to Hom_{\mathcal{C}}(X, \mathbf{G}Y)$$

Let $(X, \leq_X)(Y, \leq_Y)$be two preordered sets, C_X, C_Y the canonically associated categories and $\mathbf{F} : C_X \to C_Y$ and $\mathbf{G} : C_Y \to C_X$ be two functors. Suppose that $\mathbf{F}$ is left adjoint of $\mathbf{G}$. Since each set of morphisms in C_X or C_Y is reduced to an element or is empty the bijection of adjunction is given by :

$(F(x) \leq y) \leftrightarrow (x \leq G(y))$. Let us consider successively $x = G(y)$ and $y = F(x)$, we get

$(G(y) \leq G(y)) \Longrightarrow (F(G(y) \leq y)$

$(F(x) \leq F(x)) \Longrightarrow (x \leq G(F(x))$

Comment. The Galois connection (correspondence) on the pre orders is "naturally" extended in an adjunction. Viewing groups and fields as categories and f and g resp. as functors $\mathbf{F}$ and $\mathbf{G}$, we get the usual definition of two adjoint functors. Indeed viewing f and g as covariant functors between X and the dual of Y we get for Galois connexion f as left adjoint to g. The Galois connection is functorial. What it means? Galois could not use category terminology and even connexion (correspondence). Nevertheless this terminology respects the main feature of the theory: connexion between Galois subgroups and field Galois extension, reversion of order of inclusion between groups and fields.

This double relation, namely connexion and reversion of inclusions is the main expression of the Galois theory from the point of view of its form. The greater a first extension of the algebraic structure (field), the smaller the second extension of the algebraic structure (group) that controls the first extension. And it turns out that the structure that expresses this situation is a contravariant functor.

In this sense we have the following theorem.

Proposition Let $K \subseteq L$ be a Galois field extension . The map

$K \subseteq M \subseteq L \overset{\overset{Gal}{\curvearrowright}}{\underset{Fix}{\curvearrowleft}} \{G | G \subseteq Gal[L : M]\}$ constitute a Galois connection. Indeed Gal and Fix are contravariant functors between posets so the announced adjunction property reduces to the trivial relations [BJ]

$$Fix(Gal(M)) = M \subseteq Fix(Gal[L : M]),\ G \subseteq Gal(Fix(G))$$

Comment. We should notice the way to get fixed fields from Galois groups and Galois groups from fixed field. That means that all field extension is related to a control by a

subgroup. The extension implies the group action, i.e. automorphisms of the elements of the extension and the fixation of the elements of the basic field by the same subgroup. This double action of this Galois group (identity on the basic field, permutation on the extended elements) expresses the form of the extension. The reverse of the inclusions, extension towers in one side, subgroups inclusion in the other side is another meaning of the theory: the more you extend the (field) structure to get the roots of the polynomial the less you need a (group) control structure because the roots are more and more distinct. In order to complete the significance of these extensions let us consider the following theorem.

Galois theorem. Let $K \subseteq L$ be a finite dimensional Galois extension of fields. In this case, the adjunction is a contravariant isomorphism. Moreover, for every intermediate field extension $K \subseteq M \subseteq L$

$$dim[L : M] = \#Gal[L : M]$$

The equality of the cardinalities is a way to complete the significance of the correspondence. Let us consider the dimension of the field extension (or of the vector space of the extended field over the basic field) that is a passive dimension and on the other hand the dimension (order) of the Galois group is active, it yields the automorphisms.

5 Galois theory of Grothendieck

[BJ p. 15] presents Grothendieck theory in its spirit not in its generality, which figures in the context of schemes. The generalization comes through steps : it needs the concept of algebra, split algebra and is able to explain a general form of Galois equivalence.

5.1 Algebra on a field

An algebra A on a field K is a vector space on K provided with a multiplication that makes it into a ring that satisfies $k(aa') = (ka)a'$, for all a, a' in A. The idea is to exploit this new structure of algebra in order to extend the results of the field frame to this new frame. Particularly one uses this supplementary ring structure on A. It is necessary to set the relations between the structures of algebra and of field. I recall some propositions, [BJ] found. The interesting example of K- algebra for us is the ring $K[X]$ of polynomials with coefficients in K.

Comment. Algebra gives a better vision of the decomposed polynomial, it gives a way to enlarge a polynomial structure independently of unknowns. To replace field extensions over fields by the commutative algebra over fields is an important generalization. It makes possible a supplementary operation of multiplication. After a "vertical" extension it yields

in a certain sense a "horizontal" extension. When one reach a high plateau one has to extend it farther.

Proposition

Let K be a field and A a K- algebra. The following conditions are equivalent:

(i)A is a field

(ii) A has only trivial ideals

Proposition

Let K be a field. Every ideal of the K- algebra $K[X]$ is principal.

Proposition

Let K be a field and $p(X)$ be a polynomial. Then the following conditions are equivalent.

(i)the polynomial $p(X)$ is irreducible

(ii) the ideal $p(X)$ generated by $p(X)$ is maximal

(iii) the K- algebra $K[X]/p(X)$ is a field

Comment. It is important to get all operations that were possible by means of the concept of field, by means of algebra. Particularly when the relations between irreducible polynomial and maximal ideal and quotient that is in this case a field. The concept of irreducible polynomial makes possible the passage from the "polynomial point of view" to "the structural view" of the Galois theory" because the quotient by the irreducible polynomial is a field isomorphic to the extended basic field.

In order to emphasize the relation between the irreducible polynomial and the quotient by this polynomial from one side and the K-algebra $K[X]/\langle p(X)\rangle$ from the other side let us consider the implication from (iii) to (i). Let $p(X) = s(X).r(X)$ be a factorization of $p(X)$. It follows that $\langle p(X)\rangle \subseteq \langle s(X)\rangle$ from which $\langle s(X)\rangle/\langle p(X)\rangle$ is an ideal of $K[X]/\langle s(X)\rangle$.

By the properties of a field this ideal is zero or the whole field. If it is (0) then $\langle s(X)\rangle/ = \langle p(X)\rangle$ and $p(X)$ divides $s(X)$ thus $r(X)$ is a constant. If this ideal is $K[X]/p(X)$ then the constant polynomial 1 is in $s(X)$ up to a polynomial in $\langle p(X)\rangle$, that is (BJ)

$$1 = u(X) \cdot s(X) + v(X) \cdot (X) = s(X) \cdot (u(X) + v(X) \cdot r(X))$$

Thus $s(X)$ is a constant.

Comment. The quotient by the irreducible polynomial is a field and in this way we focus on the structure of field.It is interesting to notice that the irreducibility is translated in the fact that this quotient has only two ideals, the trivial one and the whole field.

5.2 An algebra on a field and the generalization of algebricity properties on a field

Let K be a field and A a K-algebra. An element $a \in A$ is algebraic when there exists a polynomial $p(X) \in K[X]$ with $p(a) = 0$. The K algebra A itself is called "algebraic" when all its elements are algebraic. **Comment.** It is worth stressing that the polynomial structure becomes an element of a field structure.

Proposition

Let K be a field, A a K-algebra and $0 \neq a \in A$ an algebraic element with minimal polynomial $p(X)$ of degree n. The K -subalgebra $K(a) \subseteq A$ generated by a is isomorphic to

$$K(a) \cong \frac{K[X]}{\langle p(X) \rangle} \cong \{k_0 + k_1 X + \cdots + k_{n-1} X^{n-1} | k_i \in K\},$$

where in the last expression the operations are defined modulo $p(X)$.

Comment. I would like to comment on this isomorphism. When one write the expression of the quotient we can observe the structure of the polynomial expression as such. This structure is worked to become a form that concentrates other kinds of structure: vector space, ideal (maximal and prime), field and algebra. In this last proposition we have to deal with the algebra structure. The sub-algebra $K(a)$ is worked in such a way that it will be considered a set of polynomials modulo the minimal polynomial $p(X)$. This polynomial controls the set of polynomials that constitutes the sub-algebra.

I have to add that the introduction of the structure of algebra allows to dispose of larger structure. I called it a "horizontal" extension. We get the multiplicative structure of the algebra. The initial vector space gained by means of this concept a new frame for the Galois theory: particularly the ring $K[X]$ with coefficient in K is a K- algebra, from which we get the set of polynomial functions. It is easy to remark that we have here a kind of abstraction: in a larger frame introducing the possibility of an elementary operation : the multiplication as we said above and this operation has many outcomes .

6-2-1-Properties of K-algebra in relation with a field extension k $\subseteq$ L

Proposition

Let $K \subseteq L$ be a field extension. Every L-algebra B is trivially a K-algebra, by restriction of the scalar multiplication to the elements of K. On the other hand every K -algebra A yields an L - algebra $L \bigotimes_K A$ where the multiplication of this algebra is determined by

$$(l \otimes a)(l' \otimes a') = (ll')(aa')$$

and the scalar multiplication by

$$l(l' \otimes a) = (ll') \otimes a)$$

$l, l' \in L, a, a' \in A$

Comment. In the spirit of Grothendieck, [BJ] introduces the tensor product in order to extend the K- algebra to the L -algebra. By means of the tensor product one yield an specific extension: the extension of the algebra and of scalars of the algebra. Let us consider the role played by the tensor product. It allows us to extend the structure of algebra because it yields the multiplication and the multiplication of scalars. Both multiplications are given by the properties of the relation between the product and the tensor product. We have got the extension by the algebra ad the extension of algebra.

Remark. It is possible to iterate these different extensions like in the case of the field extensions. Algebra structure captures a part of field structure and field extension and for this reason it can be extended in the same manner.

By this theorem it is possible to cross another step in the road to categorical generalization of the theory. Indeed these constructions extend to functors,

$$L - Alg \longrightarrow K - Alg, \quad B \mapsto B, \quad K - Alg \longrightarrow L - Alg,$$

$$A \mapsto L \bigotimes_K A$$

the second functor is left adjoint to the first one. For the proof we need simply to exhibit a natural isomorphism

$$Hom_L(L \bigotimes_K A, B) \cong Hom_K(A, B)$$

Comment. It is worth noticing that the restriction of scalars and the extension of this one can extend to functors. It is the specific Grothendieck's Abstraction. First the extension of scalars by the tensor product and secondly in a quasi natural way, the functorial translation. It supposes that the algebras are viewed as categories. What is the benefit of this translation? It makes possible the presentation of the extension "as such". It is the particularity of the functorial (categorical) translation: we get a level of abstraction where the extension can be worked as the basic element. That means that the structuralist view of the extension is a goal of Grothendieck's theory. But inversely the extension seems to be a deep way to consider a motor of the Galois theory. The step of generalization that replaces the field extension by the commutative algebra over fields is very effective. I recall the equivalences [BJ p. 305] gives: For a finite dimensional commutative algebra A over a field the following conditions are equivalent:

(i)A is a finite product of separable field extensions

(ii) $L \bigotimes_K A$ has no nilpotent elements for any field extension L of K

(iii) The L-algebra $L \bigotimes_K$ is of the form $L \times \cdots L$ for any extension L of K

(iv) A is projective as an $(A \bigotimes_K A)$-module

Two propositions [BJ] p.21

Proposition 1:

Let $K \subseteq L$ be a field extension and A be a K-algebra. Then the following isomorphism holds:

$$Hom_K(A, L) \cong Hom_L(L \bigotimes_K A, L)$$

Proposition 2:

Let $K \subseteq L$ be a field extension and $p(X) \in K[X]$ a polynomial. Then the following isomorphism holds

$$L \bigotimes_K \frac{K[X]}{\langle p(X) \rangle} \cong \frac{L[X]}{\langle p(X) \rangle}$$

On the right side the polynomial is viewed as a polynomial with coefficients in L.

Comment. The first proposition is a corollary of the previous one. It means that in the case of an field extension and any algebra A we get the above isomorphism. The comment has to be about the change from the extended object to the morphisms. It is the spirit of the Galois theory that is translated in the Grothendieck's view. This view results from the concept of abstraction that Grothendieck promotes. The extension is developed through a conception in terms of *morphisms.*

The second proposition presents a kind of contraction of the "tensored" field extension, in order to give another analysis of the quotient by the minimal polynomial.

I would like to give a last theorem before the passage to the concept of split algebra. This theorem is a synthesis of the previous results in terms of morphisms.

Proposition

Let $K \subseteq L$ be a field extension and $p(X) \in K[X]$ a polynomial. Then there exists a bijection between

(i) The roots of $p(X)$ in L

(ii) the homomorphisms of K-algebras $\frac{K[X]}{\langle p(X) \rangle} \longrightarrow L$

Comment. This bijection represents the passage from the roots of the minimal polynomial to the set of the elements of the quotient of the K - algebra $K[X]$ by the minimal polynomial to the field L. In this way the roots of a polynomial are viewed as morphisms into the field which contains these roots. And the domain of these morphisms is given through the quotient by the polynomial. It is easy to underline the role played by the polynomial. *It structures the extensions that are considered as morphims.* It is well known that this concept lies at the center of Grothendieck's thought. But Grothendieck is working in such a way that morphisms appear in all objects or structures he treats.

6-2-2- Split algebras

A Galois extension of fields is an algebraic field extension such that the minimal polynomial $p(X) \in K[X]$ of each element $l \in L$ factors in $L[X]$ into factors of degree 1 with

distinct roots. The notion of $Split\ algebra$ is constructed to capture these properties of Galois extension, through the concept of algebra.

Let us posit the following **definition** :

Let $K \subseteq L$ be a field extension and A a K-algebra. The extension L splits the K-algebra A when (i) the algebra A is algebraic over K

(ii) the minimal polynomial $p(X) \in K[X]$ of every element of A factors in $L[X]$ into factors of degree 1 with distinct roots.

The K-algebra A is an étale algebra when it is split by the algebraic closure of K.

Comment. The $Split\ algebra$ is a new structure (and a category) corresponding to the structure of splitting field, transferred to the case of algebras. This reformulation proposes a new theoretic extension of the Galois situation. We can pose the same question : what advantage does the concept of algebra procure? A split algebra extends the factoring of the polynomial to the structure of algebra : the concept of algebra yields a more precise visibility on the factoring of the polynomial. The Galois theory is formulated through a specific issue : yielding the largest structure for the linear factoring of the minimal polynomial. The target of Grothendieck in this construction was to give the polynomial factoring an algebraic structural status.

I want to explain the theorem I consider the most important in this step of the theory [BJ] p. 24. **Theorem**

Let $K \subseteq L$ be a field extension of finite dimension m and A a K-algebra of finite dimension n. Then the following conditions are equivalent:

(i) the extension L splits the L-algebra A

(ii) the following map called the *Gelfand transformation* is an isomorphism of K-algebra

$$Gel : L \bigotimes_K A \to L^{Hom_L(L \bigotimes_K A, L)};$$

$l \bigotimes a \to (f(l \bigotimes a))$ where $f \in Hom_L(L \bigotimes_K A, L)$

(iii) the following map is an isomorphism of L-algebras:

$$L \bigotimes_K A \to L^{Hom_K(A,L)}$$

$l \bigotimes a \to (l(g(a))$; where $g \in Hom_K(A, L)$

(iv)$\sharp Hom_L(L \bigotimes_K A, L) = n$

(v) $\sharp Hom_K(A, L) = n$

(vi) $L \bigotimes_K A$ is isomorphic to L^n as an L-algebra

(vii)$\forall x \in L \bigotimes_K A, x \neq 0, \exists f \in Hom_L(L \bigotimes_K A, L)$ such that $f(x) \neq 0$

There are simple proofs of these different equivalences. I would like to begin with a comment on (iv) and then explain the idea of Gelfand transformation.

Comment. This proposition provides a sort of translation reformulation of the structural situation of Galois theory into the terms of Grothendieck's interpretation of this theory. The starting point is the tensor product ; it makes an A- algebra K into a L-algebra. It is a way to preserve the algebra structure through its extension.

This tensor product is related to the set of maps (morphisms) from the tensor product in the basic field into this basic field. We deal here with a kind of a twofold duality.

I will comment the following lemma that concerns (i) and (ii).

lemma

L splits the K -algebra A if and only if its Gelfand transformation is an isomorphism. That is condition (i) and (ii) of the theorem are equivalent.

Comment This lemma means that the isomorphism of Gelfand transformation is related specially to the fact that the extension L splits the K-algebra A. From the point of view of the Gelfand transformation the isomorphism means that the tensor product $L \bigotimes_K A$ corresponds to a "decomposition" in maps from morphisms $Hom_L(L \bigotimes_K A, L)$ to L. We can use the correspondence between the roots of polynomial $p(X)$ and $Hom_K(\frac{K[X]}{\langle p(X)\rangle}, L)$. The Gelfand transformation yields a larger frame to interpret the splitting in terms of maps. The spirit of this analyzis consists in the explication of the goal Grothendieck aims at. Reformulate the objects, here roots of polynomial, in terms of morphisms the field extension becomes in this way, first of all, the development of possible morphisms.

Remark on the proof of the lemma. It uses all previous equivalences. Particularly the fact that n distinct roots for the minimal polynomia of $a \in A$ K-algebra, $p(X) \in K[X]$ of degree n means that $\sharp Hom_K(K(a), L) = n$.

III - The Galois equivalence. This theorem (Galois theorem according [BJ] p. 28) concludes the translation of the Galois theory inside the frame of Grothendieck theory. It is important to emphasize that it is expressed in the category language and in the structure of the algebra and G -set. I recall that given a group G whose composition law is writtent multiplicatively, a left G-set is a set X provided with a left action of G, : $G \times X \to X, \qquad (g, x) \to gx$

$1x = x, \qquad g(g'x) = (gg')x$

A morphism $f : X \to Y$ of left G-sets respects the action of G, that is,

$$f(gx) = g(fx).$$

Galois theorem. Let $K \subseteq L$ be a finite dimensional Galois extension of fields. Let us write $Gal[L : K]$ for the group of K-automorphims of L and $Gal[L : K] - Set_f$ for the category of finite $Gal[L : K] - sets$. Let us also write $Split_K(L)_f$ for the category

of those finite dimensional K-algebras which are split by L. The functor on $Split_K(L)_f$ represented by L factors through the category $Gal[L:K]-Set_f$:

$$Hom_K(-,L) : Split_K(L)_f \longrightarrow Gal[L:K]-Set_f$$

$$A \longrightarrow Hom_K(A,L)$$

with $Gal[L:K]$ acting by composition on $Hom_K(-,L)$. This factorization functor is a contravariant equivalence of categories.

Comment I shall explain the meaning of this theorem. First, it is a reformulation of Galois theorem. Let us consider the factorization functor. It relates the category $Split_K(L)$ to the category $Gal[L:K]-Set_f$. It is a meaning of the Galois theorem. The link between the category where there exists a factorization into linear factors and the category where the Galois group acting by composition on the functor that represents $Split_K(L)$ is an extension reformulation of the Galois theorem: from one side (like a memory of the field extension) the category $Split_K(L)$ from the other side, the acting Galois group. But this link is enriched. Second, I would say that this reformulation is a dynamical one: Split -Algebra focusses on the splitting and Galois -group on the acting of the group. And both dynamics are related to each other. Let us look back to the equivalence of categories. By the comment of the lemmas [BJ] uses I will explain what this means. First the proof expresses what the action of $Gal[L:K]$ consists in. It is given by

$$Gal[L:K] \times Hom_K(A,L) \longrightarrow Hom_K(A,L), \qquad (g,f) \mapsto g \circ f$$

The Galois group contributes in this way to give the representation of $Split$ a meaning. And it is the primary significance of the Galois group. The proof splits in five lemmas. Both first prepare the proof of the equivalence of categories.

Lemma 1 For every algebra $A \in Split_K(L)_f$ we get a structure of a $Gal[L:K]-set$ on $L \bigotimes_K A$ by putting

$$Gal[L:K] \times (L \bigotimes_K A) \longrightarrow L \bigotimes_K A, \qquad (g, l \otimes a) \to g(l) \otimes a$$

Via the Gelfand isomorphism this action becomes :

$$Gal[L:K] \times L^{Hom_K(A,L)} \to L^{Hom_K(A,L)},$$

$$(g,\phi) \to [f \to g(\phi(g^{-1} \circ f))]$$

where $\phi : Hom_K(A,L) \to L$ and $f \in Hom_K(A,L)$ I give the whole proof from [BJ].

Let us fix an element $g \in Gal[L:K]$ and consider the morphism

$$\gamma : L^{Hom_K(A,L)} \longrightarrow L^{Hom_K(A,L)}, \quad (\gamma(\phi))(f) = g(\phi(g^{-1} \circ f))$$

$$\begin{aligned}((\gamma \circ Gel)(l \otimes a))(f) &= (\gamma(Gel(l \otimes a)))(f) \\ &= (g(Gel(l \otimes a)g^{-1} \circ f)) \\ &= g(l(g^{-1} \circ f)(a))) \\ &= g(l(g^{-1}(f(a))) \\ &= g(l)gg^{-1}(f(a)) \\ &= g(l)(f(a)) \\ &= Gel(g \otimes id)(l \otimes a)(f) \\ &= ((Gel \circ (g \otimes id))(l \otimes a)(f).\end{aligned}$$

Let us consider the role played by the Gelfand isomorphism. It makes possible the resort to set of morphisms and then the action of the Galois group, that is the apparition of the composition. We also need the commutativity of the diagram.

$$\begin{array}{ccc} L \bigotimes_K A & \xrightarrow[\cong]{Gel} & L^{Hom_K(A,L)} \\ {\scriptstyle g \otimes id}\downarrow & \circlearrowleft & \downarrow{\scriptstyle \gamma} \\ L \bigotimes_K A & \xrightarrow[Gel]{\cong} & L^{Hom_K(A,L)} \end{array}$$

This expresses the equivalence between both formulations of the statement. We have got the structure of $Gal[L:K] - set$ on $L \bigotimes_K A$, and the isomorphism of Gelfand transformation expresses the "extension" of this structure.

Lemma 2

For every algebra $A \in Split_K(L)_f$ one has

$$A \cong Fix_{Gal[L:K]}(L \bigotimes_K A) =$$

$$= \{x \in L \bigotimes_K A | \forall g \in Gal[L:K](g \otimes id)(x) = x\}$$

In this lemma we come back to the classical Galois theorem. All object (algebra) of the category $Split_K(L)$ corresponds to objects of $L \bigotimes_K A$ fixed by the group $Gal[L:K]$.

And then it is possible to prove the Galois equivalence.

Lemma 3. The functor described above is full.

The proof [BJ p. 31] proposes is a little technical. He fixes two K -algebras A and B in $Split_K(L)$ and a morphism of $Gal[L:K]$-sets

$$\phi : Hom_K(B, L) \to Hom_K(B, L)$$

that becomes via Gelfand

$$L^\phi : L^{Hom_{A,L}} \to L^{Hom_K(B,L)}$$

and using the previous lemma and the Gelfand isomorphism he constructs the following situation:

$$\begin{array}{ccccc} A & \xrightarrow{\cong} & Fix_{Gal[L:K]}(L \otimes_K A) & \xrightarrow{\cong} & Fix_{Gal[L:K]}(L^{Hom_K(A,L)}) \\ & & & & L^\phi \downarrow \\ B & \xleftarrow{\cong} & Fix_{Gal[L:K]}(L \otimes_K B) & \xleftarrow{\cong} & Fix_{Gal[L:K]}(L^{Hom_K(B,L)}) \end{array}$$

Let $\psi : A \to B$ be this composite. The fullness of the functor amounts to $\phi = Hom_K(\psi, L)$

$$\begin{array}{ccc} L \bigotimes_K B & \xrightarrow[\cong]{Gel_B} & L^{Hom_K(B,L)} \\ {\scriptstyle p_B}\downarrow & & \downarrow{\scriptstyle p_h} \\ B & \xrightarrow[h]{} & L \end{array}$$

p_h is the projection of index h. Let i_B where $i_B(b) = 1 \otimes b$ be the inverse image of p_B. One get, [BJ] a second commutative diagram, indeed :

$$(p_h \circ Gel_B \circ i_B)(b) = (p_h \circ Gel_B)(1 \otimes b) = p_h(h'(b)_{h' \in Hom_K(B,L)}) = h(b)$$

We need the following commutative diagram:

$$\begin{array}{ccccc} A & \xrightarrow{i_A} & L \bigotimes_K A & \xrightarrow[\cong]{Gel_A} & L^{Hom_K(A,L)} \\ {\scriptstyle \psi}\downarrow & & {\scriptstyle \bar{\phi}}\downarrow & \circlearrowleft & \downarrow{\scriptstyle L^\phi} \\ B & \xrightarrow[i_B]{} & L \bigotimes_K A & \xrightarrow[Gel_B]{\cong} & L^{Hom_K(A,L)} \end{array}$$

$\bar{\phi}$ is the morphism corresponding to L^ϕ by the Gelfand isomorphim and it ensures the commutativity of the diagram. In this way we get the end of the proof.

$$Hom_K(\psi, L)(h) = h \circ \psi$$

$$= p_h \circ Gel_B \circ i_B \circ \psi$$
$$= p_h \circ Gel_B \circ \bar{\phi} \circ i_A$$
$$= p_h \circ L\phi \circ Gel_A \circ i_A$$
$$= p_{\phi(h)} \circ Gel_A \circ i_A$$
$$= \phi(h)$$

Comment The fullness describes a property of the functor $Hom_K(-L)$, thus expresses the fact that the Galois equivalence, in terms of categories, allows us to find for all morphisms of $Gal[L : K] - sets$, namely all morphisms between the images of the functor of objects of the category $Split_K(L)$ the corresponding morphism of the images by this functor. This property of the equivalence of categories (fullness) ensures that as soon as one get a morphism between G-sets and thus group actions it comes from morphism between objects of K-algebras that split. It is an element of a reformulation of the Galois correspondence.

Lemma 4

The functor is faithful. Let us consider a second morphism $\psi' : A \to B$ such that $Hom_K(\psi', L) = \phi$. One should prove that it implies that $\psi' = \psi$ It is clear that, (BJ), for every $h \in Hom_K(B, L)$

$$p_h \circ Gel_B \circ i_B \circ \psi' = h \circ \psi'$$
$$= \phi(h)$$
$$= p_{\phi(h)} \circ Gel_A \circ i_A$$
$$= p_h \circ L^{\phi} \circ Gel_A \circ i_A$$
$$= p_h \circ Gel_B \circ i_B \circ \psi$$

by using the previous diagram. Since this relation holds for all projection p_h and since both Gel_B and i_B are injective we get $\psi' = \psi$. This injectivity, as element of the equivalence makes more precise the categorical Galois equivalence.

Comment Fulness and faithfulness are a specific reformulation of Galois correspondence. It expresses the conceptual virtualities of the Galois extensions. By means of the categorical reformulation we get a dynamical unity of the elements of the correspondence that are also dynamical elements .

The last property we have to show is the essential surjectivity on the objects.

Lemma 5

The functor is essentially surjective on the objects.

That means that every quotient of the $Gal[L:K]$-set $Gal[L:K]$ has to be isomorphic to an object of the form $Hom_K(A,L)$ for some $A \in Split_K(L)_f$. All object of the image category has to be isomorphic to an object of the form $Hom_K(A,L)$. This property completes the dynamics of the correspondence. The image category $Gal[L:K]-Set_f$ is covered by the image of the functor. Let us consider the proof.

Let H be a subgroup $H \subseteq Gal[L:K]$ and the corresponding $Gal[L:K]$-quotient-set $Gal[L:K]/H$ A previous proposition showed that there exists a bijection between the subgroups of G and the quotient of the G-set G. It has to be proved that

$$\frac{Gal[L:K]}{H} \cong Hom_K(Fix(H),L).$$

By the inclusion $Fix(H) \subseteq L$ we get by functoriality a morphism (BJ) ρ

$$Gal[L:K] \cong Hom_K(L,L) \to Hom_K(Fix(H),L),$$

sending $f : L \to L$ to its restriction $f_| : (Fix(H) \to L$

$$\begin{array}{ccccc} K & \rightarrowtail & Fix(H) & \rightarrowtail & L \\ \| & & \downarrow & & \vdots \\ K & \rightarrowtail & L & = & L \end{array}$$

We know that it is possible to extend $f_|$ to f. Every morphism of K-algebra $Fix(H) \to L$ is the restriction of a morphism $L \to L$. The main argument consist in the explicit construction of the extension in such a way to obtain the extension of the initial morphism. Thus the map ρ is a quotient map.

It remains to prove that $Hom_K(Fix(H),L)$ is the quotient $\frac{Gal[L:K]}{H}$. To this goal it suffices to show that $f, g \quad L \rightrightarrows L$ have the same restrictions to $Fix(H)$ if and only if $f^{-1} \circ g \in H$. $f_|Fix(H) = g_|Fix(H)$ means that $f \circ g^{-1}$ fixes the points of $Fix(H)$. That means that

$$f^{-1} \circ g \in Gal[L : Fix(H)] = H$$

It is (BJ) the classical Galois theorem that yields this equality. The sub group of the Galois group of $Fix(H)$ -automorphims of L, i. e. that fix the elements of $Fix(H)$ fixed by H is H.

On the other hand every finite $Gal[L:K]$-set is a finite disjoint union of quotient of of $Gal[L:K]$. To conclude, (BJ) appeals to arguments of category theory. I recall the lemma that [BJ p. 25.] uses.

Lemma

The class of those K-algebra satisfying the equivalent conditions (ii) to (vii) is stable under subobjects, quotients, finite products, and tensor products.

And since L splits the K - algebra A if and only if its Gelfand transformation is an isomorphism, the category $Split_K L_f$ has finite products. It suffices to prove that the contravariant functor $Hom_K(-L)$ transforms finite products into finite sums. That is what [BJ] proves using the sequel

$A \longleftarrow A \times B \longrightarrow B$

This concludes the proof of the lemma and then of the theorem of the Galois equivalence.

6 Some analysis about the (classical) Grothendieck Galois theory

There exists other way to generalize Galois theory. One of these consists in treating arbitrary extensions.

First, to what (BJ) calls a "finite dimensional Galois subextension", namely the intermediate field extensions $K \subseteq M \subseteq L$, with $K \subseteq M$ a finite dimensional Galois extension of fields.

In this generalization we will have to deal with topology intervention.

Particularly we have the proposition

Proposition

Let $K \subseteq L$ be a Galois extension of fields. The field L is the set-theoretical filtered union of the subextensions $K \subseteq M \subseteq L$ where $K \subseteq M$ is a finite dimensional Galois extension.

Comment In this generalization we have to deal with the subextension as such, that means with the relation between the subextensions. And when the subextensions are arbitrary the Galois group will be a topological group. This group will turn out to be discrete when the extension is finite dimensional.

I would like set out two propositions without proof in order to describe the topological point of view.

[BJ p.39]

Let $K \subseteq L$ be a Galois extension of fields. in the category of groups:

$$Gal[L : K] = lim_M Gal[L : K]$$

when M runs through the poset of finite dimensional Galois extensions $K \subseteq M \subseteq L$ and for $M \subseteq M'$, the corresponding morphism

$$Gal[M' : K] \to Gal[M : K], f \to f_|$$

is the restriction.

It suffices to prove that the projections $p_M : Gal[L : K] \to Gal[M : K]$ form a cone, and that this cone is a limit one.

It yields the topological group.

[BJ p. 40] can give the following definition.

Definition

Let $K \subseteq L$ be a Galois field extension. The topological Galois group of this extension is the group $Gal[L : K]$ provided with the initial topology for all the projections

$$Gal[L : K] \cong lim_M Gal[M : K] \to Gal[M : K], f \to f_|M$$

where M runs through the finite dimensional Galois subextensions $K \subseteq M \subseteq L$ and each $Gal[L : M]$ is provided with the discrete topology. All the groups $Gal[M : K]$ are finite. The diagram constituted by these $Gal[M : K]$ is cofiltred. The topological Galois group is thus (BJ) a cofiltred projective limit, in the category of topological groups, of a diagram constituted of discrete finite groups: such a group is called a *profinite group*.

Before going to a commentary on this topological generalization I would like to explain some properties of this topology.

Lemma 1

Let $K \subseteq L$ be a Galois field extension. The subgroups $Gal[L : M] \subset Gal[L : K]$ for $K \subseteq M \subseteq L$ a finite dimensional Galois subextension, constitute a fundamental system of open and closed neighbourhoods of id_L.

Lemma 2

Let $K \subseteq L$ be a Galois extension of fields. The topology of the Galois group $Gal[L : K]$ is the initial topology for all the maps

$$ev_l : Gal[L : K] \to L, f \mapsto f(l)$$

where l runs through L and the codomain L of ev_l is provided with the discrete topology. This topology is also called the topology of pointwise convergence on $Gal[L : K]$

And then we have the corollary

Corollary Let $K \subseteq L$ be a Galois extension of fields. For every $f \in Gal[L : K]$, the subsets

$$V_M(f) = \{g \in Gal[L : K] | g_|M = f_|M\} \subseteq Gal[L : M]$$

for $K \subseteq M \subseteq L$ running through the arbitrary finite dimensional subextensions constitute a fundamental system of neighbourhoods of f.

Comment The most important feature of these topologies is that they give a way to control the continue distance of the subextensions through the topological group corresponding to these extensions. It it worth noticing that a fundamental open subset of this

group contains a fundamental neighbourhood of the identity i.e. id_L that is the subgroup $Gal[L : M]$. The topological generalization of the Galois correspondence provides the extensions with the advantages of the topology. From two points of view. Firstly, it establishes a link with another domain of mathematics and its resources. Secondly and most importantly, the topological view completes the correspondence by the dynamics of topology. I will develop this feature below.

It is interesting to notice what the closure of a subset of $Gal[Gal[L : K]$ consists in. [BJ p. 43] Let $K \subseteq L$ be a Galois extension of fields. Given a subset $U \subseteq Gal[L : K]$ its closure is given by

$$\overline{U} = \Big\{ f \in Gal[L : K] \Big| \forall MK \subseteq M \subseteq L \, with \, K \subseteq M \text{ finite dimensional Galois extension}$$

$$\exists g \in Ug | M = f|M \Big\}$$

6.1 Classical infinitary Galois theory

The issue is to generalize the Galois theorem to the case of an arbitrary Galois extension $K \subset L$, namely to the contravariant isomorphism of the Galois correspondence. By using two propositions we can prove Galois theorem for arbitrary extension.

Proposition 1[BJ] p. 40

Let $K \subseteq M \subseteq L$ be a finite dimensional intermediate Galois extension. The canonical restriction morphism

$$p_M : Gal[L : K] \to Gal[M : K]; \quad f \mapsto f_{|M}$$

is a topological quotient for the equivalence relation determined by the subgroup $Gal[L : M] \subseteq Gal[L : K]$

Proposition 2

Let $K \subseteq L$ be an arbitrary Galois extension of fields. For every finite dimensional intermediate extension $K \subseteq M \subseteq L$

$$Gal[L : M] = \{ f \in Gal[L : K] | \forall m \in M f(m) = m \}$$

is an open and closed subgroup of $Gal[L : K]$.

In the proof of this proposition [BJ] uses elementary properties of topological groups namely: every subgroup of a topological group containing an open subgroup is itself open, and every open subgroup is closed.

And then the **corollary**

Let $K \subseteq L$ be an arbitrary Galois extension of fields. For every arbitrary intermediate extension $K \subseteq M \subseteq L$

We also need (BJ) the following **lemma**:

Let $K \subseteq L$ an arbitrary Galois extension of fields and $G \subseteq Gal[L : K]$ a closed subgroup. Moreover let us suppose that

$$K = Fix(G) = \{l \in L | \forall g \in Gg(l) = l\}$$

$G = Gal[L : K]$. Two features emerge from these topological properties of the subgroups. The fact that the subgroup is closed allows to characterize the intermediate subextensions. It brings out another feature of the Galois correspondence. Particularly the feature of $Fix(G)$ for $G \subseteq Gal[L : K]$.

And we get the topological Galois theorem. **Galois theorem** Let $K \subseteq L$ be an arbitrary Galois extension of fields. The correspondences

$$K \subseteq M \subseteq L \mapsto Gal[L : M],$$
$$G \subseteq Gal[L : K] \mapsto Fix(G)$$

induce a contravariant isomorphism between the lattice of arbitrary extensions $K \subseteq M \subseteq L$ and the lattice of closed subgroups $G \subseteq Gal[L : K]$

Comment We have here the third Galois theorem : it is established in the frame of topological groups. The subgroups are closed subgroups and extensions are arbitrary extensions. We gain a topological meaning of $Fix(G)$. Finally the topological contravariance means that we are interested in the form of the distance of the inclusions and their reverse. This form yields a supplementary unification frame. But this unification consists in coming out of the algebraic properties. This point of view completes the classical initial Galois theorem. And this classical infinitary Galois theorem can be seen as the element of the main theory: Grothendieck infinitary Galois theory.

6.2 Infinitary Grothendieck Galois theory : the main element

An important element necessary to understand and to explain the Grothendieck theory is the profinite topological spaces. I will give only some notions before coming to the main theory. I recall the definitions given by [BJ].

7-2-1 Profinite topological spaces

Definition 1[BJ p. 47]

A topological space is profinite when it is the projective limit, indexed by a cofiltered poset, of finite discrete topological spaces.

Definition 2

A topological space is totally disconnected when two distinct points admit disjoint neighborhoods which are both open and closed.

I give now three lemmas of [BJ] p. 48

Lemma 1

In the category of topological spaces and continuous mappings, a projective limit of totally disconnected spaces is again totally disconnected.

I recall [BJ] that given a diagram$\mathcal{D}$ of topological spaces, its projective limit L is the space

$$L = \{(x_X)_{X\in\mathcal{D}} \in \prod_{X\in\mathcal{D}} X | \forall f \in \mathcal{D}, f : X \to Y, f(x_X) = x_Y\}$$

Lemma 2

A projective limit of compact and totally disconnected spaces is again compact and totally disconnected.

And we have this property:

Theorem

A topological space is profinite if and only if it is compact and totally disconnected. with two corollaries

Corollary 1

A topological space is profinite when it homeomorphic to a projective limit of finite discrete spaces.

Corollary

For a compact Hausdorff space X the following conditions are equivalent

(i) X is profinite

(ii) the topology of X has a basis constituted of clopens (simultaneously open and closed subsets)

(iii) X is totally disconnected

Comment Some remarks about the definitions of a profinite space. This space and its properties are constructed and introduced in order to compose the algebraic control and the topology. Particularly through the property of compactness. The total disconnectedness allows us to dispose as for classical topology the property of separation. The concept of projective limit as subgroup of direct product contributes to this algebraic control. We have to take into account the fact that one construct this limit by means of the projective system associated. $\ldots G_2 \xrightarrow{\alpha_2} G_1 \xrightarrow{\alpha_1} G_0$ where G_i are topological groups.

6.3 Infinitary Galois theory of Grothendieck : the fourth theorem

We can consider that this theory represents the synthesis of the previous Galois theories. The first generalization by the concept of K- algebra, and the second by extension to arbitrary Galois extension will be concentrated and "potentialized" in this third theory.

Definition

Let G be a topological group. A topological G-space is topological space provided with a continuous action of G. A morphism of topological $G-$ spaces is a continuous morphism of G-sets. A topological G-space is profinite when it is a projective limit, indexed by a cofiltered poset, of finite discrete topological spaces. Before going to the last theorem, I will explain six lemmas [BJ P. 57 sq] gives.

Lemma 1

Let K be a field. Every algebraic K-algebra A is the set-theorical filtered union of its finite subalgebras.

Lemma 2

Let $K \subseteq L$ be a an arbitrary Galois extension of fields. For every K-algebra A which is split by L there is a bijection

$$Hom_K(A, L) \cong \lim_B Hom_K(B, L)$$

where the limit is cofiltered and indexed by the finite dimensional subalgebra $B \subseteq L$ Moreover, each $Hom_K(B, L)$ is finite. In particular, the above limit formula provides $Hom_K(A, L)$ with the structure of a profinite space.

Comment Let us consider these lemmas.The first one interprets the concept of algebras as a filtered union of its subalgebras: in this way it introduces the topology in the structure of algebra. The second one provides $Hom_K(A, L)$ with a structure of a profinite space. This "topologization" of all the Galois structure brings out a new structural frame: the image by the functor $Hom_K(-, L)$ is provided with a topological structure. The construction added to the categorical meaning and in terms of algebra the topological meaning.

Lemma 3

Let $K \subseteq L$ be an arbitrary Galois extension of fields. For every K-algebra A which is split by L, the map

$$\mu : Gal[L : K] \times Hom_K(A, L) \to Hom_K(A, L), \quad (g, f) \mapsto g \circ f$$

is a continuous action of the topological group $Gal[L : K]$ on the topological space $Hom_K(A, L)$, where these are provided with the profinite topologies we got.

The proof of lemma 2 uses the fact that the projection

$$p_B : Hom_K(A, L) \cong lim_B Hom_K(B, L) \to Hom_K(B, L)$$

is continuous and a diagram that uses this projection. Indeed proving the continuity of the group action reduces to proving that for every finite dimensional subalgebra $B \subseteq B$ the composite $p_B \circ \mu$ where μ is the action. The left vertical composite is continuous.

$$\begin{array}{ccc} Gal[L:K] \times Hom_K(A,L) & \overset{\mu}{\longrightarrow} & Hom_K(A,L) \\ \downarrow & & \\ Gal[M:K] \times Hom_K(A,L) & & \\ \downarrow & & \\ Gal[M:K] \times Hom_K(B,M) & & \end{array}$$

It is important to set up the topology for the group action. At this step the action of the topological Galois group is seen as continuous and is the way to give the Galois framework topological meaning. This meaning is general because the topology is the discrete topology.

For the lemme 3, we have to prove that for every finite subdimensional subalgebra $C \subseteq A$ the composite

$$Hom_K(B,L) \overset{\Gamma(f)}{\longrightarrow} Hom_K(A,L) = lim_C Hom_K(C,L) \overset{p_C}{\longrightarrow} Hom_K(A,L)$$

is continuous. $f(C) \subseteq B$ is a finite dimensional K-algebra.

Considering the following commutative diagram:

$$\begin{array}{ccc} Hom_K(B,L) & \overset{\Gamma(f)}{\longrightarrow} & L^{Hom_K(A,L)} \\ \downarrow{\scriptstyle p_C} & & \downarrow{\scriptstyle p_C} \\ Hom_K(f(C),L) & \overset{}{\underset{\gamma(f)}{\longrightarrow}} & Hom_K(C,L) \end{array}$$

where $(\gamma(f))(h)(c) = h(f(c))$ for all $c \in C$. We get the result since all arrows are continuous.

After this "topologization"of the situation [BJ] shows how to achieve its reformulation in terms of categories.

lemma 4

Let K be a field and A an algebraic K-algebra. Let us write $A = colim B$ where B runs through the finite dimensional subalgebras of A. For every finite dimensional K-algebra C, the canonical morphism

$$\rho : colim_B Hom_K(C,B) \overset{\cong}{\longrightarrow} Hom_K(C,A)$$

is bijective. The commutativity of the colim with $Hom_K(C,B)$ is an element of this new situation.

The last lemma before the theorem is categorical.

Lemma 5

Let $G = lim_{i \in G_i}$ be a profinite group, expressed as a cofiltered projective limit of finite discrete groups. Let us assume that the projections $p_i : G \to G_i$ are surjective. We write $G_i - Set_f$ for the category of finite G_i-sets and $G - Top_f$ for the category of discrete finite topological G-spaces. For every index $i \in I$, there is a functor

$$\gamma_i : G_i - Set_f \to G - Top_f, \quad X \mapsto X$$

where the G action on X is given by $g.x = p_i(g).x$. This functor γ_i identifies $G_i Set_f$ with a full subcategory of $G - Top_f$. Moreover the category $G - Top_f$ is the set theoretical filtered union of the full subcategories $G_i - Set_f$.

This functor is full and faithful. This lemma through the functor it describes says that we get a dynamical unity between categories $G - Set_f$ and $G - Top_f$. This unity has been constructed on the basis of the action of profinite group.

Finally I can set out the last theorem that is according to [BJ] he Grothendieck Galois theorem

Galois theorem

Let $K \subseteq L$ be an arbitrary Galois extension of fields. We write $Split_K(L)$ for the category of K-algebras split by L and $Gal[L : K]-$ Prof for the category of profinite $Gal[L : K]$-spaces. The functor

$$\Gamma : \text{Split}_K(L) \longrightarrow \text{Gal}[L : K] - \text{Prof}\,, \quad A \mapsto Hom_K(A, L)$$

is a contravariant equivalence of category.

It is a synthesis of all previous theorem. I will comment on this synthesis.

The proof that Γ is full and faithful uses the results of previous lemmas. Let us consider $A, B \in Split_K(L)$. We know that

$$A = colim C, C \subseteq A; \qquad B = colim D, D \subseteq B$$

where the colimits are filtered and C, D run respectively through finite dimensional subalgebras of A and B. For each pair A, B we can choose finite dimensional extensions, M_C, M_D which split respectively C and D. We can even choose a finite dimensional Galois extension M_{CD} which splits both C and D and we get

$$K \subseteq M_C \subseteq M_{CD} \subseteq L, \quad K \subseteq M_D \subseteq M_{CD} \subseteq L,$$

We also get

$$Hom_K(C, L) \cong Hom_K(C, M_{CD}), Hom_K(D, L) \cong Hom_K(D, M_{CD})$$

We have then, (BJ)

$$Hom(\Gamma(A),\Gamma(B)) \cong Hom(Hom_K(A,L)Hom_K(B,L))$$
$$\cong Hom(Hom_K(colim_C C,L)Hom_K(colim_D D,L))$$
$$\cong Hom(lim_C Hom_K(C,L), lim_D Hom_K(D,L))$$
$$\cong lim_D Hom(lim_C Hom_K(C,L), lim_D Hom_K(D,L))$$
$$\cong lim_D colim_C Hom(Hom_K(C,L), Hom_K(D,L))$$
$$\cong lim_D colim_C Hom_K(Hom_K(C,M_{CD}), Hom_K(D,M_{CD}))$$
$$\cong lim_D colim_C Hom(D,C) \cong lim_D Hom(D, colim_C)$$
$$\cong Hom(colim D, colim C) \cong Hom(B,A)$$

Let us remark that the Galois correspondence and the second Galois theorem (Grothendieck generalization to algebras)is integrated in the proof through the role played by $Split_K(L)$. This isomorphism proves the full- and faithfulness of Γ.

The previous lemma applies in such a way that determines the functor Γ and allows us to prove that it is essentially surjective. A profinite $Gal[L:K]$-space is a cofiltered projective limit $X \cong lim_{i\in I} X_i$ of finite discrete topological $Gal[L:K]$- spaces. Each X_i is a finite $Gal[M_i:K]$-set for some finite dimensional Galois extension $K \subseteq M_i \subseteq L$. BJ uses here the functor γ_i.

$$\gamma_i : G_i - Set_f \to G - Top_f, \quad X \mapsto X$$

And then he uses the Galois Grothendieck previous theorem (what is no topological). $X_i = Hom_K(C_i, M_i)$ for some finite dimensional K-algebra C_i which is split by M_i. Moreover we observed that

$$X_i = Hom_K(C_i, M_i) \cong Hom_K(C, L)$$

As noticed it is important to emphasize that the topology is introduced by means of cofiltered limit, which is suited to Galois extensions.

Given $f_{ij} : X_i \to X_j$ in the diagram of X, the space X_i is a finite discrete $Gal[M_i:K]$-space and the space X_j is a finite discrete $Gal[M_j:K]$-space. We can choose a finite dimensional Galois extension $K \subseteq M \subset L$ such that $M_i \subseteq M$ and $M_j \subseteq M$ and this yelds $X_i = Hom_K(C_i, M)$ and $X_j = Hom_K(C_j, M)$, where C_i and C_j are finite dimensional K-algebras split by L. The morphism : $h_{ij} : C_j \to C_i$ induces the morphism

$$X_i = Hom_K(C_i, M) \to Hom_K(C_j, M) = X_j$$

by applying the previous Galois Grothendieck. [BJ] constructed in this way a diagram constituted by the C_i from the diagram constituted by the X_i. It suffices to put $A = colim_{i\in I}C_i$, filtered colimit of algebras. One prove that L splits A.

And finally one has:

$$Hom_K(A, L) \cong Hom_K(colim_{i\in I}C_i, L) \cong lim_{i\in I}Hom_K(C_i, L) \cong lim_{i\in I}X_i \cong X$$

7 Generalization in four steps

I recall the steps of generalization of the Galois theory. Let us take into account that we have only a partial generalization. The next generalization is to replace the commutative algebra over fields by the commutative algebras over connected commutative rings. I don't deal with this. But the generalizations I presented give us some precious philosophical indications.

Ist step. Proposition Let $K \subseteq L$ be a Galois field extension . The map

$K \subseteq M \subseteq L \overset{\overset{Gal}{\curvearrowright}}{\underset{Fix}{\curvearrowleft}} \{G|G \subseteq Gal[L : M]\}$ constitute a Galois connection. Indeed Gal and Fix are contravariant functors between posets so the announced adjunction property reduces to the trivial relations [BJ]

$$Fix(Gal(M)) = M \subseteq Fix(Gal[L : M]),\ G \subseteq Gal(Fix(G))$$

IId step. Galois theorem Let $K \subseteq L$ be a finite dimensional Galois extension of fields. Let us write $Gal[L : K]$ for the group of K-automorphims of L and $Gal[L : K] - Set_f$ for the category of finite $Gal[L : K] - sets$. Let us also write $Split_K(L)_f$ for the category of those finite dimensional K-algebras which are split by L. The functor on $Split_K(L)_f$ represented by L factors through the category $Gal[L : K] - Set_f$:

$$Hom_K(-, L) : Split_K(L)_f \longrightarrow Gal[L : K] - Set_f$$

$$A \longrightarrow Hom_K(A, L)$$

with $Gal[L : K]$ acting by composition on $Hom_K(-, L)$. This factorization functor is a contravariant equivalence of categories.

IIId step. Galois theorem Let $K \subseteq L$ be an arbitrary Galois extension of fields. The correspondences

$$K \subseteq M \subseteq L \mapsto Gal[L : M],$$
$$G \subseteq Gal[L : K] \mapsto Fix(G)$$

induce a contravariant isomorphism between the lattice of arbitrary extensions $K \subseteq M \subseteq L$ and the lattice of closed subgroups $G \subseteq Gal[L : K]$

IVth step. Galois theorem

Let $K \subseteq L$ be an arbitrary Galois extension of fields. We write $Split_K(L)$ for the category of K-algebras split by L and $Gal[L : K]-$ Prof for the category of profinite $Gal[L : K]$-spaces. The functor

$$\Gamma : \text{Split}_K(L) \longrightarrow \text{Gal}[L : K] - \text{Prof}\,, \quad A \mapsto Hom_K(A, L)$$

is a contravariant equivalence of category. I have to add one remark regarding the generalization: when one need to prove the validity of generalization one have necessarily to be able to return to the starting point by means of a restriction. I give only one example.

The Grothendieck Galois theorem contains the classical Galois theorem. The contravariant equivalence of categories implies the existence of an isomorphism between the lattice of subobjects

$$K \rightarrowtail M \rightarrowtail L$$

in $Split_K(L)_f$ and the lattice of quotients $Hom_K(M, L)$.

$$Gal[L : K] \cong Hom_K(L, L) \twoheadrightarrow Hom_K(M, L) \twoheadrightarrow Hom_K(K, L) \cong \{*\}$$

in $GalL : K] - Set_f$. You have the Galois isomorphism.

This is not the end of the history. I have focused on generalization on algebraic-topological Grothendieck Galois theory. There exists many other generalizations. (See the schema). Particularly there is the extension of the Galois theory to Poincaré theory, or to differential Galois theory. Grothendieck constructed the synthesis of these different generalizations. The theory of Galois categories concerns characterizing those categories equivalent to the category of finite sets on which a finite (or profinite) group acts. In this theory lies the deepest meaning of the generalization. But I put forward a significant movement of this generalization.

As for the new geometrical vision Grothendieck speaks about, it concerns through the Galois correspondence the links, at different categorical levels, between Algebra and Geometry or Topology Grothendieck invented. What is important is the fact that Galois correspondence contains a geometrical significance. Galois group - even purely algebraic- is full of geometry.

I would conclude in four points. Firstly, the generalization of Galois theory is based on the concept of correspondence. This correspondence is an bijection (morphism functorial) between different structures (categories) and reversed inclusion. This only pure form supports the schema of the generalization. Secondly, the generalization proceeds from ons side by deepening both sides of the correspondence, from the other side by rebuilding and

enriching the morphism. Thirdly, the strengths of the generalization results from its functorial nature: as relation between structures considered as such this nature was since the Galois formulation functorial. Fourthly, as for the nature of the mathematical structures concerned, the ontology consists in a extension power (synthetic) of the structures we have to deal with. And the the theory is strong, the more it brings out explicitly this feature. For this reason Galois theory is first of all - through the category theory- a theory of the extension of mathematics.

Références

[BJ] **Francis Borceux and George Janelidze** *Galois theories* Cambridge University Press 2001

Régine Douady, Adrien Douady *Algèbre et théories galoisiennes*, II, Cedic 1979

[JS] **Jan Stewart** *Galois theory* Chapman and Hall, First ed 1973, second ed. 1983, Third ed. 2004

Bourbaki *Algèbre* chapitre IV , Masson Paris 1981

Gillles Châtelet*La physique mathématique comme projet* Presses de l'ENS 2010

Harold M. Edwards *Galois theory* Springer Verlag 1984

Alexandre Grothendieck *Récoltes et semailles*

Alexandre Grothendieck *Revêtements étales et groupe fondamental*, SGA1, exposé V, Springer Lect. Notes in Math. **224**, 1971

Colin MacLarty *Elementary Categories, Elementary Toposes*Oxford Logic Guides 21. Clarendon Press Oxford 1995

Alain Prouté *Introduction à la logique catégorique* Prépublications de l'Université Paris VII Version remaniée 2010

Marius Van der Put, Michael F. Singer *Galois Theory of Linear Differential Equations* Springer 2003