ON THE NOTION OF INDISCERNIBILITY IN THE LIGHT OF GALOIS-GROTHENDIECK THEORY

GABRIEL CATREN[1,2] AND JULIEN PAGE[1]

1- SPHERE - UMR 7219, Université Paris Diderot - CNRS, Paris, France.

2- Facultad de Filosofía y Letras, Universidad de Buenos Aires - CONICET, Buenos Aires, Argentina.

Abstract. We analyze the notion of *indiscernibility* in the light of the Galois theory of field extensions and the generalization to K-algebras proposed by Grothendieck. Grothendieck's reformulation of Galois theory permits to recast the Galois correspondence between symmetry groups and invariants as a duality between G-*spaces* and the minimal *observable algebras* that separate theirs points. In order to address the Galoisian notion of indiscernibility, we propose what we call an *epistemic reading* of the Galois-Grothendieck theory. According to this viewpoint, the Galoisian notion of indiscernibility results from the limitations of the 'resolving power' of the observable algebras used to discern the corresponding 'coarse-grained' states. The resulting Galois-Grothendieck duality is rephrased in the form of what we call a *Galois indiscernibility principle*. According to this principle, there exists an inverse correlation between the coarsegrainedness of the states and the size of the minimal observable algebra that discern these states.

1. Introduction

> "If you pursue this analogy too closely, everything coincides identically; if you avoid it, all is scattered into infinity."
>
> J.W. von Goethe
> *Maxims And Reflections*, §554 [17]

The notion of *indiscernibility* is a fundamental notion in philosophy, mathematics and physics. This notion is intimately related to the notion of *symmetry* and, therefore, to the mathematical concept of *group* and its different generalizations (groupoids, pregroups, quantum groups, etc.). Now, the notion of group was introduced for the first time by the French mathematician Evariste Galois (1811-1832) in order to demonstrate that a general formula for the roots of a fifth (or higher) degree polynomial equation does not exist (by using only the usual algebraic operations–addition, subtraction, multiplication, division– and application of radicals–i.e. n^{th} roots–). The notion of group permitted Galois to keep track of the permutations of the roots of a polynomial $p(x) \in K[x]$ that are *indiscernible* from the viewpoint of the field K. More precisely, the so-called *Galois group* of the polynomial encodes the permutations of the roots that are K-*symmetry transformations*, i.e. transformations that do not produce any 'observable' effect from the viewpoint of K. In this way, the very birth of the notion of group was motivated by the need to formalize notions such as *symmetry transformation*, *indiscernibility*, and *invariance*.

In the aftermath of Galois, the main ideas of Galois theory were transferred and generalized to other fields of modern mathematics, mainly to the theories of K-algebras, rings, covering spaces, and differential equations [5, 14, 32]. In particular, Grothendieck's generalization of Galois theory to the topological theory of covering spaces led to a general reformulation of Galois ideas in terms of the so-called *Galois categories* ([18]; [19], Exposé V, Section 4; see also Robalo, Galois Theory towards Dessins d'Enfants (unpublished)[1]). Moreover, Janelidze proposed a general Galois theorem in the framework of category theory that reduces to the Galois theories of fields, K-algebras, rings and covering spaces under suitable specifications [5].[2] In this way, the Galois theory of field extensions appears as a concrete realization of an abstract scheme in which the Galoisian notion of indiscernibility is addressed in full generality. This multiplicity of concrete realizations and vast generalizations is a symptom of the richness and deepness of Galois' ideas, richness that goes far beyond the theory of polynomial equations and field extensions. Moreover, and besides its importance in pure mathematics, Galois theory has started to find its way in the realm of mathematical-physics, notably in the framework of renormalization theory in quantum field theory (see Ref.[9, 10]).[3]

In what follows we propose a conceptual analysis of the Galoisian notion of indiscernibility. To do so, we shall focus on the algebraic Galois theory of field extensions and the generalization of this theory to K-algebras proposed by Grothendieck (the main references that we shall follow are Ref.[5], chap. 2 and Ref.[14], chap. 5; see also Ref.[33][4]). In Section N°2, we start the analysis of Galois theory by unpacking the idea according to which the Galoisian notion of (in)discernibility is a relative notion. This means that this notion depends on the *resolving power* of the *domain of rationality* from which the individuals in question are being '*observed*'. In Section N°3, we show that the relativity of the notion of indiscernibility entails one of the fundamental features of Galois theory, namely that the corresponding symmetry group, far from being fixed once and for all, can vary. Indeed, instead of only considering the invariants under the symmetry transformations generated by a fixed symmetry group, Galois theory considers the variations of the algebraic structures of invariants under different *symmetry breakings* of the symmetry groups. In this way, a variation of the domain of rationality entails a concomitant variation of both the symmetry groups and the corresponding algebraic structures of invariants. Under certain conditions, the variability of the symmetry group entails the existence of a *Galois correspondence* between a partial order of symmetry groups on the one hand and a partial order of algebraic structures of invariants on the other. Roughly speaking, the larger the symmetry group, the fewer the corresponding invariants.

In the rest of the article we shall use the generalization of Galois theory proposed by Grothendieck to analyze the notion of Galoisian indiscernibility in the framework of the duality between *geometry* and *algebra*. More precisely, Grothendieck's reformulation will permit us to revisit the duality between an *abstract algebraic structure* and the different *dual spaces* on which the former can be *represented* as *concrete observable algebras*. To do so, we shall introduce in Section N°4 Grothendieck's notion of *functor of points*. Instead of considering the roots of a polynomial $p(x) \in K[x]$ in a fixed 'domain of rationality', the functor of points encodes the sets of A-roots of $p(x)$ for every possible K-algebra A. The set of A-roots of $p(x)$ defines what we shall call *A-dual space*. Following Lavwere's terminology, the K-algebra A will be called *dualizing object* (see Ref.[29], p. 121). The notion of functor of points will allow us to establish a distinction between the different *restricted representation theories* of a K-algebra defined by the different dualizing K-algebras A and the *general representation theory* encoded in the functor of points. Then in Section N°5 we introduce the *Gelfand transform* between an algebraic structure defined by $p(x)$–namely, the K-algebra that *represents* the functor of points defined by $p(x)$–and the algebras of A-valued observables on the different A-dual spaces. In this way, a polynomial $p(x) \in K$ defines different A-dual spaces on the one hand and the corresponding algebras of A-valued observables on these spaces on the other. We shall then analyze the conditions under which the Gelfand transform is an isomorphism between the initial abstract algebra and a concrete observable algebra on a dual space. In Section N°6, we show that the Galois duality between symmetry groups and invariants on the one hand and the duality between algebras and spaces on the other can be unified as a duality between dual G-spaces and the minimal observable algebras that separate theirs points. We then rephrase the resulting Galois-Grothendieck duality in terms of what we call a *Galois indiscernibility principle*. According to this principle, there is an inverse correlation between the coarsegrainedness of the states in a dual G-space and the size of the minimal observable algebra that discerns these coarse-grained states. In the final section, we conclude by briefly discussing the relationship between Galois-Grothendieck theory and Leibniz's *principle of the identity of indiscernibles*.

2. The Relativity of (In)discernibility

In what follows, certain algebraic structures (notably commutative fields and K-algebras) will play the role of what we shall call, by borrowing an expression introduced by Kronecker, a *domain of rationality* (*Rationalitäts-Bereich*, see Ref.[24], Vol.2, pp. 251-256; see also Ref.[35]). By this term, we shall understand an algebraic language wherein we can formulate certain kind of propositions. In particular, a field K is a domain of rationality in which one can formulate propositions given by polynomial equations of the form $p(x) = 0$ with $p(x) \in K[x]$. In a first approximation, we could say that the roots of $p(x)$ are the truthmakers of such a proposition. However, this definition is meaningless if we do not specify the domain of rationality in which we shall look for its roots. In order to guarantee that a polynomial equation $p(x) = 0$ with $p(x) \in K[x]$ makes sense, the domain of rationality for the possible values of x has to be a K-algebra.[5] The first evident possibility is to look for the solutions of such a polynomial equation in the field K itself. However, it is a remarkable fact that there might be roots of $p(x)$ that do not belong to K. Hence, the fact that a proposition is formulated in a domain of rationality K does not mean that we have to restrict the search of its truthmakers to K. The distinction between the domain of rationality to which belong the coefficients of a polynomial equation and the different possible domains of rationality in which we can look for its solutions is one of the essential underpinnings of Galois theory. Given a polynomial $p(x) \in K[x]$ of degree n, it can be shown that there exist a minimal extension of K, called a *splitting field* K^p of $p(x)$, in which we can find n roots of $p(x)$ (counted with multiplicity).[6] Hence, if we restrict the search of the roots of $p(x)$ to K-algebras that are fields, we can state that the truthmakers of a polynomial proposition $p(x) = 0$ are the n roots $\{\alpha_1, ..., \alpha_n\}$ of $p(x)$ in a splitting field K^p (where n is the degree of $p(x)$). Let's consider for instance the archetypical example of the polynomial $p(x) = x^2 + 1$ considered as a polynomial in $\mathbb{R}[x]$. The two complex roots $\{i, -i\}$ of this polynomial do not belong to the field $\mathbb{R}$ in which the polynomial is defined. The best that we can do from the viewpoint of $\mathbb{R}$ is to assign arbitrary names to these unknown roots, such as α_1 and α_2. We can thus say that the individuals named α_1 and α_2 are truthmakers of the proposition $x^2 + 1 = 0$, i.e. that the saturated propositions $\alpha_1^2 + 1 = 0$ and $\alpha_2^2 + 1 = 0$ are both true. We shall now argue that the individuals denoted by these names are $\mathbb{R}$-*indiscernible*, i.e. indiscernible from the viewpoint of $\mathbb{R}$.

In order to provide a formal definition of the notion of (in)discernibility, let's introduce the notion of *K-algebraic relations* for a given domain of rationality K. Let $X = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ be a set of n distinct elements of a field extension of K, for example the n distinct roots of a polynomial $p(x) \in K[x]$.[7] The ordering of the set X implies that the group of permutations of the elements of X can be identified with the group of permutations of n elements S_n. The *K-algebraic relations* in the α_i's are polynomial propositions of the form $q(\overrightarrow{\alpha}) = q(\alpha_1, \alpha_2, ..., \alpha_n) = 0$, where $q \in K[x_1, x_2, ..., x_n]$. The set X is said to be a set of K-indiscernible elements if the validity of any K-algebraic relation in its elements is not changed by any permutation of these elements. This means that for every permutation $\sigma \in S_n$ and every $q \in K[x_1, x_2, ..., x_n]$ such that $q(\overrightarrow{\alpha}) = 0$, we have that $\sigma \cdot q(\overrightarrow{\alpha}) = 0$ where $\sigma \cdot q(x_1, x_2, ..., x_n) \doteq q(x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, ..., x_{\sigma^{-1}(n)})$.[8] This K-indiscernibility is maximal, in the sense that the K-algebraic relations satisfied by $\overrightarrow{\alpha}$ remain invariant under *all* the permutations of the α_i's in S_n. But we can define weaker notions of K-indiscernibility such that the valid permutations belong to a subgroup H of S_n. We shall say that the α_i's are *(H, K)-indiscernible* if and only if $\sigma \cdot q(\overrightarrow{\alpha}) = 0$ for every $\sigma \in H$ and every $q \in K[x_1, x_2, ..., x_n]$ such that $q(\overrightarrow{\alpha}) = 0$. Reciprocally, given a set $X = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ of n elements of an extension of K, we can define the set $S_K(X)$ of all the permutations of the n elements α_i that leave invariant the K-algebraic relations satisfied by $\overrightarrow{\alpha}$. More precisely, $S_K(X) \doteq \{\sigma \in S_n : \forall q \in K[x_1, x_2, ..., x_n]/q(\overrightarrow{\alpha}) = 0, \sigma \cdot q(\overrightarrow{\alpha}) = 0\}$. It can be shown that $S_K(X)$ is a subgroup of S_n.[9] The group $S_K(X)$ encodes the K-indiscernibilities of the α_i's. The bigger $S_K(X)$ is, the more the α_i's 'look alike' from the viewpoint of K. It's worth noting that the notion of (H, K)-indiscernibility and the group $S_K(X)$ only depend on the set $\{\alpha_1, \alpha_2, ..., \alpha_n\}$, but not on the order of the α_i's.

In particular, we shall say that two individuals α_1 and α_2 are K-indiscernible if every K-algebraic relation in $K[x_1, x_2]$ satisfied by these individuals is invariant under a permutation of α_1 and α_2. In the previous example, the fact that i and $-i$ are $\mathbb{R}$-indiscernible means that there is no $q \in \mathbb{R}[x_1, x_2]$ such that $q(\alpha_1, \alpha_2) = 0$ and $q(\alpha_2, \alpha_1) \neq 0$. In particular, there is no $r(x) \in \mathbb{R}[x]$ such that $r(\alpha_1) = 0$ and $r(\alpha_2) \neq 0$. On the contrary, two individuals will be called K-*discernable* with respect to a given domain of rationality K if the algebraic relations in $K[x_1, x_2]$ can *resolve* them, i.e. if there is at least one K-algebraic relation satisfied by α_1 and α_2 that is not invariant under their permutation. For instance, i and $2i$ are $\mathbb{R}$-discernible, since whereas i is a root of x^2+1, $2i$ is not. This example also shows that α_1 and α_2 can be K-discernable even if they do not belong to K. The important point is that in the framework of Galois theory the (in)discernibility of two individuals, far from being an absolute notion, depends on the domain of rationality K from which one is trying to resolve them. The relative K-indiscernibility of two individuals, far from entailing their identity, means that the ‘sufficient reason’ that explains their qualitative (or predicable) difference lies beyond the domain of rationality K. In particular, a qualitative multiplicity of L-discernible elements can appear, from the restricted viewpoint of a domain of rationality K endowed with a lower resolving power, as a purely numerical multiplicity of K-indiscernible elements. We could say that every domain of rationality K is endowed with a particular *resolving power*, i.e. with a capacity to *resolve* or *separate* different individuals. We shall say that two K-indiscernible individuals lack, from the viewpoint of K, *predicable discernibility.* This means that in K their difference is purely numerical, which means that it cannot be ‘predicated’ by means of the algebraic resources of the domain of rationality K. We could say that the difference between two K-indiscernible individuals is beyond the *cut-off* defined by the resolving power of K. The best that we can do from the viewpoint of K is to arbitrarily assign different names to K-indiscernible individuals. However, this nominal covering of a numerical difference is not grounded on a K-predicable difference. All in all, the limitations of the resolving power of a domain of rationality K implies that, *from the standpoint of* K, there is a numerical multiplicity of K-indiscernible individuals.[10]

It is worth noting that any element in K can be discerned from any other element by means of the K-algebraic relations. Indeed, any $\alpha \in K$ is the unique root of the polynomial $p(x) = x - \alpha \in K[x]$. In other terms, $x = \alpha$ is the only truthmaker in K of the proposition $p(x) = x - \alpha = 0$. We could say that the proposition $p(x) = x - \alpha = 0$ is the *individuating* K*-predicate* of α [31]. Every element of K is thus endowed with an individuating K-predicate. Since the resolving power of a domain of rationality K allows us to discern the elements of K itself, indiscernible elements necessarily belong to an *extension* of K.

3. Galois correspondence

Let’s consider a polynomial $p(x)$ of degree n over a field K and the set $X = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ of its n different roots (assumed to be simple) in a splitting field K^p. We define the so-called *Galois group* $Gal_K(p)$ of $p(x)$ over K as follows:

$$Gal_K(p) = S_K(X) = \{\sigma \in S_n : \forall q \in K[x_1, x_2, ..., x_n]/q(\overrightarrow{\alpha}) = 0 \Rightarrow \sigma \cdot q(\overrightarrow{\alpha}) = 0\}.$$

The permutations in $Gal_K(p)$ will be called *Galois permutations.*[11] According to the definition of $Gal_K(p)$, a permutation of the roots of $p(x)$ is a Galois permutation if and only if it does not modify the K-algebraic relations between the roots. The Galois group of p over K is then the subgroup of S_n such that any algebraic relation in $K[x_1, x_2, ..., x_n]$ satisfied by the n roots is still satisfied when a Galois permutation of the roots is performed. Since there is no algebraic relation in $K[x_1, ..., x_1]$ capable of making the difference between the roots permuted by an element in $Gal_K(p)$, the Galois permutations are ‘invisible’ from the viewpoint of K. In this way, the Galois group of $p(x) \in K[x]$ encodes the limitations of the resolving power of K to discern the roots of p. It is worth stressing that the K-indiscernibility encoded by a Galois group is not always maximal, in the sense that the Galois group is not always equal to the whole S_n. In order to stress this fact we shall substitute the notion of *K-indiscernibility* by the more precise notion of *(G, K)-indiscernibility* (where $G \doteq Gal_K(p)$).

In order to discern (G, K)-indiscernible individuals, we have to *extend* the domain of rationality K. By extending K, it is possible to discern individuals that were K-indiscernible. For example, the individuals i and $-i$, that are $\mathbb{R}$-indiscernible, can be discerned by extending $\mathbb{R}$ to $\mathbb{C}$. In fact, the propositions $x \mp i = 0$ are the individuating $\mathbb{C}$-predicates of the individuals i and $-i$. We could say that the existence of a purely numerical difference that puts the discernibility resources of K into question naturally induces the necessity of *extending* K. If K is not a splitting field of a polynomial $p(x) \in K[x]$, then we can extend the field K to a new field L such that $K \subset L \subseteq K^p$, where K^p is a splitting field of p. By increasing the 'resolving power' of the field by means of which we try to discern the roots of p it might be possible to discern more roots. It can be shown that such a field extension is given by an *injective* field homomorphism $K \hookrightarrow L$, i.e. that K can be viewed as a subfield of L.[12] Each element $\alpha \in L$ defines the following evaluation homomorphism (which is a morphism of K-algebras):

$$\begin{aligned} \varepsilon_\alpha : K[x] &\rightarrow L \\ f(x) &\mapsto f(\alpha). \end{aligned}$$

If ε_α is not injective, then its kernel is an ideal generated by an irreducible polynomial $p_{\alpha,K} \in K[x]$ (that can be assumed to be monic), called the *minimal polynomial* of α over K. In such a case, α is said to be *algebraic* over K.[13] The image $K[\alpha]$ of ε_α is isomorphic to $K[x]/\langle p_{\alpha,K}\rangle$. Since $p_{\alpha,K}$ is irreducible, $\langle p_{\alpha,K}\rangle$ is a maximal ideal, and then $K[x]/\langle p_{\alpha,K}\rangle$ is the smallest field (that we shall denote $K(\alpha)$) containing both K and α. The extension $K(\alpha)$ is a vector space over K of dimension $[K(\alpha)] : K] = deg(p_{\alpha,K})$ with basis $\{1, \alpha, ..., \alpha^{n-1}\}$.[14] To every algebraic element α_i over K, we can associate the Galois group $Gal_K(p_{\alpha_i,K})$ that encodes the (G, K)-indiscernibilities of the K^p-roots of $p_{\alpha_i,K}$ for K^p a splitting field. A field extension $(L : K)$ is called *algebraic* if every $l \in L$ is algebraic over K, *i.e.* if $p(l) = 0$ for some $p(x) \in K[x]$. A field K is *algebraically closed* if it has no algebraic extensions other than itself, i.e. if the splitting field K^p of every polynomial $p(x) \in K[x]$ is K itself. An *algebraic closure* $\overline{K}$ of K is an algebraic extension that is algebraically closed. On the contrary, if ε_α is injective, *i.e.* if it does not exist a nonzero polynomial $p \in K[x]$ such that $p(\alpha) = 0$, we say that α is *transcendental* over K. In this case, $[K[\alpha] : K] = \infty$ and $K[\alpha] \cong K[X]$.

In what follows we shall only consider algebraic extensions. The notion of field extension allows us to provide an alternative definition of the notion of Galois group. Instead of considering the Galois group $Gal_K(p)$ of a polynomial $p(x)$ over K, we can consider the group $Aut(L : K)$ of K-automorphisms of a field extension $i : K \hookrightarrow L$, i.e. the group of automorphisms of L that leave the elements of K invariant. Since by definition these automorphisms must leave K invariant, an automorphism $\sigma \in Aut(L : K)$ must satisfy $i = \sigma \circ i$. Now, let's consider the extension $K \hookrightarrow K^p$ where K^p is a splitting field of a polynomial $p(x) \in K[x]$ that is separable (i.e. that has only distinct roots in K^p). Then the Galois group of $Gal_K(p)$ of $p(x)$ over K and the group $Aut(K^p : K)$ are isomorphic:

$$Gal_K(p) \cong Aut(K^p : K) \tag{1}$$

Each K-automorphism $\tilde{\sigma} \in Aut(K^p : K)$ of K^p canonically induces a Galois permutation $\sigma \in Gal_K(p)$ of the roots by restriction: $\sigma(\alpha_i) \doteq \tilde{\sigma}(\alpha_i)$. Since $\tilde{\sigma}$ fixes the coefficients of $p(x)$, the element $\sigma(\alpha_i)$ is again a root of $p(x)$ (indeed, $p(\tilde{\sigma}(\alpha_i)) = \tilde{\sigma}(p(\alpha_i)) = \tilde{\sigma}(0) = 0$). By using the same argument, one can check that σ is a Galois permutation.[15] Reciprocally, each σ in $Gal_K(p)$ defines an automorphism $\tilde{\sigma} \in Aut(K^p : K)$ given by $y = q(\vec{\alpha}) \mapsto \tilde{\sigma}(y) = \sigma \cdot q(\vec{\alpha})$ (where we have used that any $y \in K^p = K(\alpha_1, ..., \alpha_1)$ can be written as a polynomial q in the variables $(\alpha_1, ..., \alpha_1)$).[16] One can check that these two process are inverse from one another. The group $Aut(K^p : K)$ is called *Galois group of the extension* $(K^p : K)$ and is denoted $Gal(K^p : K)$. While the Galois $Gal_K(p)$ of $p(x)$ over K encodes the limitations of the resolving power of

K to discern the roots of $p(x)$, the Galois group $Gal(K^p : K)$ encodes that automorphisms of K^p that leave invariant K.

If the field extension $(L : K)$ satisfies the condition of being a *Galois extension*, then it induces a correspondence (called *Galois correspondence*) between *intermediate extensions* $K \hookrightarrow M \hookrightarrow L$ and subgroups of $Gal(L : K)$. A finite algebraic extension $(L : K)$ is a *Galois extension* if and only if the only elements of the extension $(L : K)$ that are invariant under the action of $G \doteq Aut(L : K)$ are the elements in K, *i.e.* if and only if $L^G = K$ ([32], p. 12). Since by definition $K \subseteq L^G$, the extension$(L : K)$ is Galois if and only if G acts non-trivially on every l in $L - K$. This means that a Galois extension is an extension for which the number of invariants is minimal (*i.e.* only those of K) and the number of K-symmetries is maximal. Now, it can be shown that an extension $(L : K)$ is a Galois extension if and only if it is *normal* and *separable*. *Normality* means that if one root of an irreducible polynomial $p(x) \in K[X]$ belongs to L, then every roots does, *i.e.* $p(x)$ splits into linear factors in L (possibly identical). If not all the roots of $p(x)$ were in L, then we would have Galois permutations between the roots of $p(x)$ that would not be in the group $Aut(L : K)$ of K-automorphisms of L. In other terms, the group $Aut(L : K)$ would not encode all the K-indicernibilities.[17] Another possibility for spoiling the maximality in the number of K-symmetries is the presence of multiple roots for some irreducible polynomial $p(x)$ in $K[x]$. A polynomial $p \in K[x]$ of degree n is said to be *separable* if its roots in a splitting field K^p are *simple*, i.e. if it has n *different* roots in K^p. An algebraic extension $(L : K)$ is said to be separable if every irreducible polynomial in $K[x]$ that has a root in L is separable. In characteristic 0 (*i.e.* in the usual cases of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ and their extensions), every irreducible polynomial p is separable. Hence, the problem of inseparability can only appear in characteristic $c > 0$. Whereas in characteristic 0 we can distinguish between 0 and c, in characteristic c the numbers 0 and c are identified. Hence, it might happen that roots that are distinct in characteristic 0 become identified in characteristic $c > 0$. All in all, an algebraic field extension $(L : K)$ is *Galois* if and only if for every irreducible polynomial $p \in K[x]$ such that $l \in L$ is one of its roots all the other roots of $p(x)$ are in L (normality) and all the roots are simple (separability). If these two conditions are satisfied, then we can guarantee that $Gal(L : K)$ acts non-trivially on every element in $L - K$.

Let's consider now intermediate extensions $K \hookrightarrow M \hookrightarrow L$ of a finite Galois extension $K \hookrightarrow L$. By passing from the extension $(L : K)$ over K to the extension $(L : M)$ over a field M endowed with a 'higher' resolving power, *i.e.* by *extending* the domain of rationality from K to M, we can break some of the K-indiscernibilities. In other terms, elements of L that were K-indiscernible might be M-discernible. In this way, the extension of the domain of rationality from K to M induces a 'symmetry breaking mechanism' that amplifies the resolving power and reduces the corresponding indiscernibility. This means that $Gal(L : M)$ must be a subgroup of $Gal(L : K)$. It can be shown that Galois extensions induce a *Galois correspondence* between the lattice of subgroups H of $G \doteq Gal(L : K)$ and the lattice of intermediate extensions M. This correspondence is given by the following inverse applications. To a subgroup H of G, we shall associate the set of H-invariant elements of L, *i.e.* the set $Fix(H) = \{x \in L : \forall h \in H, h \cdot x = x\}$. Conversely, to an intermediate extension $K \hookrightarrow M \hookrightarrow L$, we shall associate the subgroup G_M of G that leaves invariant the elements in M, i.e. the group $G_M = \{g \in G : \forall x \in M, g \cdot x = x\} = Gal(L : M)$. The maps $H \mapsto Fix(H)$ and $M \mapsto Gal(L : M)$ define a contravariant bijection between the subgroups H of the Galois group $Gal(L : K)$ and the intermediate extensions M. In this way, intermediate domains of rationality endowed with a resolving power higher than that of K define subgroups of $Gal(L : K)$ and larger sets of invariant elements. If we extend the domain of rationality from K to L itself, the corresponding subgroup of G will be $Gal(L : L) = \{id_L\}$. This simply means that every element of L is L-discernible, i.e. that we have completely broken the indiscernibilities encoded by the Galois group $Gal(L : K)$.

4. Grothendieck's functor of points

We have thus far associated to an irreducible and separable polynomial $p(x) \in K[x]$ a splitting extension K^p and the symmetry group $G = Gal(K^p : K)$. This group encodes the limitations of the propositional resources of K to discern the roots of $p(x)$. By successively extending K to intermediate extensions $K \subset M \subset K^p$, we can progressively break these K-indiscernibilities and, in the limit (i.e. when the intermediate field M is K^p itself), reduce the symmetry group to the identity. In this way, we could think that the limitations of a domain of rationality K to discern the roots of a polynomial p can be definitively sublated by passing to a splitting extension K^p.[18] However, this is the case only if we restrict the search for the roots of polynomial equations to fields. As we said before, a more general algebraic structure in which we can search for the roots of a polynomial $p(x) \in K[x]$ is a K-algebra. Now, there is a remarkable differences between K-algebras and fields. The minimal polynomial over K of some algebraic element of a K-algebra A is irreducible only if A is an *integral domain* (i.e. if $ab = 0$ implies $a = 0$ or $b = 0$ with $a, b \in A$) (see Ref.[5], p. 18). Therefore, whereas a polynomial $p(x) \in K[x]$ of degree n cannot have more than n roots (counted with multiplicity) in any field, $p(x)$ can have more than n roots in a K-algebra.[19] In this way, the idea according to which it is always possible to find an 'absolute' field extension that contains 'all' the roots of a polynomial equation $p(x) \in K[x]$ is misleading.

According to what we have just said, the 'imperfection' of a domain of rationality K with respect to a polynomial $p \in K[x]$ (*i.e.* the fact that it does not include all the roots of p) cannot be completely overcome by passing to a splitting field K^p. Nevertheless, there is an alternative strategy for handling the limitations *of any possible domain of rationality.* This strategy was proposed by Alexander Grothendieck in the framework of his refoundation of algebraic geometry and consists in claiming that a polynomial $p(x) \in K[x]$ does not have a unique set of roots, *but rather a set of A-roots for each possible K-algebra.* According to this idea, the 'solution' of a polynomial equation is not the set of its roots in an 'absolute' domain of rationality, but rather the 'application' that defines a set of A-roots for each possible K-algebra A. We shall formalize this idea by associating to a polynomial $p(x) \in K[x]$ a mathematical entity $V_p(-)$ that sends each K-algebra A to the set of A-roots of $p(x)$ (i.e. to the set of roots of $p(x)$ in A). In other terms, to each polynomial $p(x)$ we can associate an 'application' $V_p(-)$ that sends each K-algebra A to the set $V_p(A)$ of its A-roots:

$$\begin{array}{rcl} V_p(-) : K\text{-}alg & \rightarrow & Sets \\ A & \mapsto & V_p(A) = \{roots\ of\ p(x)\ in\ A\}\,. \end{array}$$

In this way, instead of considering the roots of p in a single K-algebra, the 'application' $V_p(-)$ encodes the different sets of A-roots of $p(x)$ for any possible K-algebra A. It is possible to show that this 'application' assigns to every morphism $f : A \rightarrow B$ of K-algebras a morphism $V_p(f) : V_p(A) \rightarrow V_p(B)$ of sets and that this application between morphisms respects the identity morphism of K-algebras and the composition of morphisms. All this can be summarized by stating that $V_p(-)$ defines a covariant functor from the category of K-algebras to the category of sets. By following the standard terminology used in algebraic geometry, this functor will be called *functor of points* (see for instance Ref.[15]). To sum up we can say that Grothendieck substituted the notion of an 'absolute' domain of rationality supposed to contain all the roots of a polynomial $p(x)$ by the functor $V_p(-)$ that encodes the different sets of A-roots of p defined by all possible K-algebras A. We could say that Grothendieck bypassed the lack of an 'absolute' domain of rationality by considering all the K-domains of rationality at once.

We have thus far associated to a polynomial $p(x)$ over K a functor $V_p(-)$ that assigns to each K-algebra A the set $V_p(A)$ of A-roots of p. We shall now interpret the set $V_p(A)$ as a *A-dual space* over which $p(x)$ induces an *algebra of A-valued functions.* In other terms, we shall not consider the A-roots of p as elements of an amorphous set, but rather as 'points' of a geometric space.[20] To do so, we must firstly define a K-algebra canonically associated to $p(x)$, namely the quotient algebra $K[x]/\langle p(x)\rangle$. Now, it is easy to see that we have the following bijective correspondence between the set $V_p(A)$ and the

K-morphisms $Hom_{K\text{-}alg}(\frac{K[x]}{\langle p(x)\rangle}, A)$[21]:

$$\begin{array}{rcl} V_p(A) = \{roots\ of\ p(x)\ in\ A\} & \xrightarrow{\simeq} & Hom_{K\text{-}alg}\left(\dfrac{K[x]}{\langle p(x)\rangle}, A\right) \\ \alpha & \mapsto & \varepsilon_\alpha : \dfrac{K[x]}{\langle p(x)\rangle} \to A, \end{array}$$

where

$$\varepsilon_\alpha(\bar{f}) = f(\alpha).$$

This means that the object $K[x]/\langle p(x)\rangle$ *represents* the functor of points $V_p(-)$ in the category of K-algebras, i.e. that:

$$V_p(-) \cong Hom_{K\text{-}alg}\left(\frac{K[x]}{\langle p(x)\rangle}, -\right),$$

where the symbol "$\cong$" means that there is a natural transformation between both functors that is an isomorphism ([20], p. 8).

In the rest of the article, we shall use the following terminology (partially coming from physics). The set $V_p(A)$ will be called *A-dual space* of the K-algebra $\frac{K[x]}{\langle p(x)\rangle}$. The A-roots α of $p(x)$ in $V_p(A)$, i.e. the K-morphisms $\varepsilon_\alpha : \frac{K[x]}{\langle p(x)\rangle} \to A$, will be called *$A$-states* (or *$A$-points*) of the K-algebra $\frac{K[x]}{\langle p(x)\rangle}$. Each A-valued function on the A-dual space will be called an *A-valued observable*. As we shall see in the following section, the representability of the functor of points $V_p(-)$ allows us to represent *abstract* elements in the K-algebra $\frac{K[x]}{\langle p(x)\rangle}$ as *concrete* A-valued observables on each A-dual space.

5. The Gelfand transform

We shall now introduce the so-called *Gelfand transform* between $\frac{K[x]}{\langle p(x)\rangle}$ and a K-algebra of A-valued observables over the A-dual space $V_p(A)$. In what follows we shall only consider K-algebras A of finite dimension. The corresponding A-dual spaces are finite and discrete. This assumption allows us to avoid technical topological problems that are not relevant for the present discussion. In our case, the Gelfand transform defined by a K-algebra A sends each element $\bar{f} \in \frac{K[x]}{\langle p(x)\rangle}$ to an A-valued observable $\hat{f}$ over the A-dual space $V_p(A)$[22]:

$$\begin{array}{rcl} Gel_A : \dfrac{K[x]}{\langle p(x)\rangle} & \to & \mathcal{C}(V_p(A), A) \\ \bar{f} & \mapsto & \hat{f} : V_p(A) \to A \end{array} \tag{2}$$

where

$$\hat{f}(\alpha) = \varepsilon_\alpha(\bar{f}).$$

This construction is analogue to the Gelfand transform that identifies a commutative C^*-algebra $\mathcal{U}$ with the algebra of $\mathbb{C}$-valued continuous functions that vanish at infinity on the spectrum of $\mathcal{U}$ (see for instance Ref.[13], p. 11).[23] The Gelfand transform (2) permits to represent the K-algebra $\frac{K[x]}{\langle p(x)\rangle}$ in the algebra $\mathcal{C}(V_p(A), A)$ of A-valued observables on the A-dual space $V_p(A)$.[24] In turn, each A-point $\alpha \in V_p(A)$ permits to represent the algebra $\mathcal{C}(V_p(A), A)$ in A by means of the evaluation map $\hat{f} \mapsto \hat{f}(\alpha)$. In both cases, a 'geometric' entity (i.e. the space $V_p(A)$ and each A-point α respectively) defines a representation of an algebra (i.e. $\frac{K[x]}{\langle p(x)\rangle}$ and $\mathcal{C}(V_p(A), A)$ respectively) in another algebra (i.e. $\mathcal{C}(V_p(A), A)$ and A respectively).[25] In other terms, geometric entities define morphisms between algebraic structures.[26] In turn, the composition of both representations

$$\frac{K[x]}{\langle p(x)\rangle} \xrightarrow{Gel_A} \mathcal{C}(V_p(A), A) \xrightarrow{\varepsilon_\alpha} A$$

where

$$\overline{f(x)} \mapsto \widehat{f} \mapsto \widehat{f}(\alpha),$$

permits to characterize each A-point α as a state that defines a K-linear representation of the abstract algebra $\frac{K[x]}{\langle p(x)\rangle}$ in A. In order to clarify the relationship between the notion of representation as a morphism of K-algebras and the linear representations of K-algebras on a vector space, let's note that we can interpret the value $\widehat{f}(\alpha)$ as a multiplicative operator acting in A. In other terms, every A-point $\alpha : \frac{K[x]}{\langle p(x)\rangle} \to A$ defines a K-linear representation $\frac{K[x]}{\langle p(x)\rangle} \to End_K(A)$ of $\frac{K[x]}{\langle p(x)\rangle}$ in the underlying vector space of A, where the 'operator' $\alpha(\overline{f(x)}) = \widehat{f}(\alpha) \in A$ acts in A by multiplication.[27] In this way, each A-dual space $V_p(A)$ parameterizes the different A-representations of $\frac{K[x]}{\langle p(x)\rangle}$. *The evaluation of an observable $\hat{f} \in \mathcal{C}(V_p(A), A)$ on a A-state $\alpha \in V_p(A)$ yields the multiplicative operator $\widehat{f}(\alpha) \in A$ that represents the abstract algebra element $\bar{f} \in \frac{K[x]}{\langle p(x)\rangle}$ in the representation labeled by α.* It is worth remarking that we do not have a single duality[28] between the abstract K-algebra $\frac{K[x]}{\langle p(x)\rangle}$ and the observable algebra on a single dual space, but rather one duality for each possible dualizing object A. Each dualizing object A defines the A-dual space of $\frac{K[x]}{\langle p(x)\rangle}$ and each A-dual space parameterizes the different representations of $\frac{K[x]}{\langle p(x)\rangle}$ as multiplicative operators acting in A. The functor of points $V_p(-)$ encodes the different representations of $\frac{K[x]}{\langle p(x)\rangle}$ as observable algebras that one can obtain by varying the dualizing object A. We could then say that the functor of points $V_p(-)$ of a K-algebra $\frac{K[x]}{\langle p(x)\rangle}$ encodes the *general representation theory* of the algebra. Differently from the *restricted representation theory* encoded in a single A-dual space $V_p(A)$, the general representation theory defined by the functor of points $V_p(-)$ encompasses all the restricted representations theories at once.

The fact that an abstract K-algebra can be represented as observable algebras on different dual spaces does not mean that the former is necessarily isomorphic to the corresponding observable algebras. In general, the Gelfand transform $Gel_A : f \mapsto \hat{f}$ defined by a K-algebra A is neither injective nor surjective. The obstruction to the injectivity of the Gelfand transform stems from the fact that the dual space $V_p(A)$ might lack enough points. In such a case, the space $V_p(A)$ cannot 'support' a faithful representation of $\frac{K[x]}{\langle p(x)\rangle}$.[29] This obstruction can be bypassed by choosing a suitable dualizing object, namely a splitting field K^p of $p(x)$ (which is assumed to be separable). Indeed, the fact that the K^p-dual space $V_p(K^p)$ contains all the roots of $p(x)$ belonging to a field implies that $V_p(K^p)$ supports a faithful representation of $\frac{K[x]}{\langle p(x)\rangle}$.[30] Now, it can happen that the K-algebra $\frac{K[x]}{\langle p(x)\rangle}$ does not induce, via Gel_{K^p}, all the K^p-valued observables over $V_p(K^p)$.[31] However, we can solve this problem by extending the scalars of the K-algebra $\frac{K[x]}{\langle p(x)\rangle}$ from K to K^p, i.e. by passing from the K-algebra $\frac{K[x]}{\langle p(x)\rangle}$ to the K^p-algebra $K^p \otimes_K \frac{K[x]}{\langle p(x)\rangle} \cong \frac{K^p[x]}{\langle p(x)\rangle}$ (see Ref.[5], p. 21). Indeed, it can be shown that the Gelfand transform

$$\begin{aligned} Gel_{K^p} : \frac{K^p[x]}{\langle p(x)\rangle} \quad &\to \quad Hom_{K\text{-alg}}(V_p(K^p), K^p) \\ \bar{f} \quad &\mapsto \quad \hat{f} : \alpha \mapsto \hat{f}(\alpha) = \alpha(\bar{f}) \end{aligned}$$

is an isomorphism ([5], p. 24). This means that the abstract $K^p[x]$-algebra $\frac{K^p[x]}{\langle p(x)\rangle}$ is isomorphic to the concrete algebra $\mathcal{C}(V_p(K^p), K^p)$ of K^p-valued observables on the K^p-dual space $V_p(K^p)$ defined by the K^p-roots of $p(x)$.

6. Galois-Grothendieck duality

In Section N°3, we have introduced the Galois correspondence between the lattice of intermediate field extensions $K \hookrightarrow M \hookrightarrow K^p$ of a finite Galois extension $(K^p : K)$ and the lattice of subgroups of the Galois group $Gal_K(p)$. In turn, in Sections N°4 and N°5 we have analyzed the relations between the abstract K-algebra $\frac{K[x]}{\langle p(x)\rangle}$ defined by $p(x)$ and the different dual spaces on which $\frac{K[x]}{\langle p(x)\rangle}$ can be represented, by means of the Gelfand transform, as concrete observable algebras. We shall now show that Grothendieck's reformulation of Galois' main theorem for K-algebras synthesizes the Galois correspondence on the one hand and the Gelfand duality between algebraic structures and geometric entities on the other. By doing so, we shall obtain a duality between algebraic and geometric structures *endowed with an action of a symmetry group.*

According to what we said in Section N°4, a polynomial $p(x)$ over K defines a functor $V_p(-)$ that encodes the different A-dual spaces associated to each each K-algebra A. In order to introduce a Galois group action we shall now fix a finite Galois extension $(L : K)$ of K. Instead of considering the different A-dual spaces of a fixed K-algebra B by means of the functor of points $V_B(-) = Hom_K(B, -)$, we shall consider the L-dual spaces (for L fixed) associated to different K-algebras by means of the functor $Hom_K(-, L)$. In other terms, we shall now fix the dualizing object L and vary the abstract K-algebra that we want to represent as a concrete observable algebra on the corresponding L-dual space. Now, by fixing the dualizing object to L, the L-dual space $V_B(L) = Hom_K(B, L)$ of B is naturally endowed with an action of the Galois group $G \doteq Gal(L : K)$. This action is defined by the following composition:

$$\begin{array}{rcl} G \times Hom_K(B, L) & \rightarrow & Hom_K(B, L) \\ (g, \phi) & \mapsto & g \circ \phi, \end{array}$$

and can be schematized by means of the following diagram:

$$\begin{tikzcd} & L \arrow[loop right, "g \in G"] \\ B \arrow[ur, "\phi"] & \\ & K \arrow[ul] \arrow[uu] \end{tikzcd} .$$

The Galois-Grothendieck theorem states that there is an anti-equivalence of categories between the category $Split_K(L)_f$ of finite K-algebras split by L and the category of finite G-sets ([5], p. 28).[32] In one direction, this equivalence of categories is given by the functor $Hom_K(-, L)$:

$$\begin{array}{rcl} Split_K(L)_f & \rightarrow & G\text{-}FSet, \\ B & \Rightarrow & Hom_K(B, L). \end{array} \tag{3}$$

By following the terminology used in Ref.[5], this functor will be called *spectrum functor* and denoted $Spec_L(-)$. Whereas the functor of points $V_B(-)$ defines the different A-dual spaces of a fixed K-algebra B, the spectrum functor $Spec_L(-) = Hom_K(-, L)$ defines the L-dual spaces (with L fixed) of the different K-algebras. By means of the Gelfand transform

$$Gel_L : B \mapsto \mathcal{C}(Spec_L(B), L),$$

each finite dimensional K-algebra B split by L induces an algebra of L-valued observables on the L-dual space $Spec_L(B)$ of B. Since the extension $(L : K)$ is a finite Galois extension, the Gelfand transform Gel_L is an injection.[33]

If the K-algebra B is an intermediate field $K \subset B \subset L$, then it can be shown that the G-action on $Spec_L(B)$ is transitive, i.e. that $Spec_L(B) \cong G/H_B$ for some subgroup $H_B \subset G$. In the general case, we must use the fact that a finite dimensional K-algebra split by L is a product $\prod_i B_i$ of intermediate fields $K \subset B_i \subset L$. Since the Galois-Grothendieck duality is defined in terms of an anti-equivalence of categories, the spectrum functor transform the (Cartesian) products in the category $Split_K(L)_f$ into coproducts in the category $G\text{-}FSet$[34]:

$$Spec_L(-) : \prod_i B_i \Rightarrow \coprod_i Spec_L(B_i).$$

Conceptually, this means that the product of the observable algebras (induced by) B_i on the different spaces $Spec_L(B_i)$ defines an observable algebra on the disjoint union of the spaces. For instance, the L-dual space associated to the (Cartesian) product $B_1 \times B_2$ is the coproduct (i.e. the disjoint union) of $Spec_L(B_1)$ and $Spec_L(B_2)$. This means that the Gelfand transform applied to an abstract element $f = (f_1, f_2) \in B_1 \times B_2$ defines an observable $\hat{f} = (\hat{f}_1, \hat{f}_2)$ on $Spec_L(B_1) \coprod Spec_L(B_2)$. The observable $\hat{f}$

is given by $\hat{f}(x) = \hat{f}_1(x)$ if $x \in Spec_L(B_1)$ and $\hat{f}(x) = \hat{f}_2(x)$ if $x \in Spec_L(B_1)$. In turn, the coproduct in $Split_K(L)_f$ is given by the tensor product over K.[35] The anti-equivalence of categories between $Split_K(L)_f$ and G-$FSet$ implies that the tensor products in $Split_K(L)_f$ induce, by means of the Gelfand transform, observables on the Cartesian product of the corresponding L-dual spaces. For instance, $B_1 \otimes_K B_2$ induces an algebra of observable on the Cartesian product $Spec_L(B_1) \times Spec_L(B_1)$.[36]

In order to define an anti-equivalence of categories between $Split_K(L)_f$ and G-$FSet$, we shall define a quasi-inverse functor to the spectrum functor. Such a functor will be called *functor of (L-valued) G-invariant observables* and denoted $\mathcal{C}^G(-, L)$. The functor $\mathcal{C}^G(-, L)$ has to assign a K-algebra split by L to each G-$FSet$. Let's begin by considering the case of a homogeneous finite G-set, i.e. of a G-set $\mathcal{O}$ endowed with a transitive G-action. The transitivity of the action implies that $\mathcal{O} \cong G/H$, where H is a subgroup of G that leaves fixed an element in $\mathcal{O}$. Now, it can be shown that

$$Spec_L(Fix(H)) \cong \frac{G}{H}, \tag{4}$$

as G-sets for every subgroup H of G, where $Fix(H) = \{l \in L / \forall h \in H, h(l) = l\}$ is the field of H-invariant elements of L and $H = Gal(L : Fix(H))$.[37] In this way we recover the original Galois correspondence between intermediate fields $K \subseteq Fix(H) \subseteq L$ and subgroups H of the Galois group G in the form of a correspondence between intermediate fields $Fix(H)$ and homogeneous G-sets isomorphic to G/H. The L-dual space (4) associated to the K-algebra $Fix(H)$ is a homogeneous G-set such that the isotropy group of its points is $H \subseteq G$. Hence, the functor of G-invariant observables $\mathcal{C}^G(-, L)$ must send each homogeneous finite G-set $\mathcal{O} \cong \frac{G}{H}$ to the K-algebra $Fix(H)$ of H-invariant elements in L:

$$\begin{array}{ccc} Split_K(L)_f & \longleftarrow & G\text{-}FSet : \mathcal{C}^G(-, L) \\ Fix(H) & \Leftarrow & \dfrac{G}{H}. \end{array}$$

If the finite G-set $\mathcal{O}$ is not homogeneous, then $\mathcal{O}$ is the disjoint union of its G-orbits $\mathcal{O}_i$, where each orbit $\mathcal{O}_i$ is a homogeneous G-space isomorphic to G/H_i for some subgroup $H_i \subseteq G$. Since the functor of observables $\mathcal{C}^G(-, L)$ changes coproducts into products, we have that:

$$\prod_i Fix(H_i) \Leftarrow \coprod_i (\mathcal{O}_i \simeq \frac{G}{H_i}) : \mathcal{C}^G(-, L).$$

In other terms, the observable algebra on a disjoint union of G-homogeneous spaces $\mathcal{O}_i \simeq \frac{G}{H_i}$ can be obtained from the Cartesian product of the intermediate extensions B_i composed of the H_i-invariant elements of L.

It can be shown that $\mathcal{C}^G(-, L) = Hom_G(-, L)$, i.e. that $\mathcal{C}^G(\mathcal{O}, L)$ is the K-algebra of G-morphisms between $\mathcal{O}$ and L (see Ref.[27]).[38] This means that $\mathcal{C}^G(\mathcal{O}, L)$, far from yielding all the L-valued observables on a G-set $\mathcal{O}$, only gives the observables that are G-morphisms, i.e. the observables $\hat{f} \in \mathcal{C}(\mathcal{O}, L)$ such that $g\hat{f}(x) = \hat{f}(gx)$ for $x \in \mathcal{O}$. This last expression can be rewritten as $g^{-1}\hat{f}(gx) = \hat{f}(x)$. Hence we can say that the observables in $\mathcal{C}^G(\mathcal{O}, L)$ are the fixed points of $L^{\mathcal{O}}$ under the *descent action* given by $(g \cdot f)(x) = g(\hat{f}(g^{-1} \cdot x))$ (see Ref. [5], p. 29). This explains why we have called the functor $\mathcal{C}^G(-, L)$ *functor of G-invariant observables*. All in all, the spectrum functor $Spec_L(-)$ and the functor of G-invariant observables $\mathcal{C}^G(-, L)$ define an anti-equivalence of categories

$$Split_K(L)_f \underset{Spec_L(-) = Hom_K(-, L)}{\overset{\mathcal{C}^G(-, L) = Hom_G(-, L)}{\rightleftarrows}} G\text{-}FSet$$

between the category $Split_K(L)_f$ of finite K-algebras split by L and the category G-$FSet$ of finite G-sets. The use of products and coproducts allows us to generate the most general objects of both categories (i.e. K-algebras that are not necessarily fields and G-sets that are not necessarily homogeneous) from the simplest cases (treated by the original Galois correspondence) provided by intermediate fields and homogeneous G-sets. The following diagram schematizes the Galois-Grothendieck duality for two K-algebras B_1 and B_2 split by L:

K-algebras *G-Sets*

$$\begin{tikzcd}
& B_1 \otimes_K B_2 & \\
& B_1 \times B_2 \arrow[dl, two heads] \arrow[dr, two heads] & \\
B_1 \arrow[uur, hook] & & B_2 \arrow[uul, hook'] \\
& K \arrow[ul, hook] \arrow[ur, hook'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
& Spec_L(B_1) \times Spec_L(B_2) \arrow[ddl, two heads] \arrow[ddr, two heads] & \\
& Spec_L(B_1) \sqcup Spec_L(B_2) & \\
Spec_L(B_1) \arrow[ur, hook] \arrow[dr, two heads] & & Spec_L(B_2) \arrow[ul, hook'] \arrow[dl, two heads] \\
& Spec_L(K) &
\end{tikzcd}$$

The generalization of the Galois correspondence as a duality between K-algebras and G-sets permits us to reinterpret the former in the following terms. Each K-algebra $B \in Split_K(L)_f$ defines a L-dual space $Spec_L(B)$ such that each abstract element $f \in B$ defines, by means of the Gelfand transform, a concrete L-valued observable on $Spec_L(B)$. Now, in the previous section we argued that the observable algebra induced by B on $Spec_L(B)$ cannot be isomorphic to the whole algebra of L-valued observables on this space.[39] As we have just explained, a K-algebra B only induces the L-valued observables on $Spec_L(B)$ *that are G-invariant* with respect to the descent action. In other terms, $Gel_L(B)$ is the subalgebra of $\mathcal{C}(Spec_L(B), L) \cong B \otimes_K L$ composed of the G-invariant observables. Now, it can be shown that the G-observables on $Spec_L(B)$ induced by B by means of the Gelfand transform are enough for discerning (or separating) the states in $Spec_L(B)$. This means that if $\widehat{f}(\alpha) = \widehat{f}(\beta)$ for every $f \in B$ (with $\alpha, \beta \in Spec_L(B)$), then necessarily $\alpha = \beta$. Conversely, if $\alpha \neq \beta$, then necessarily there exists at least one element f in B such that $\alpha(f) \neq \beta(f)$, i.e. such that $\widehat{f}(\alpha) \neq \widehat{f}(\beta)$.[40] In this way, the Galois-Grothendieck duality is a duality between finite G-sets $\mathcal{O}$ and the *minimal* K-algebras $\mathcal{C}^G(\mathcal{O}, L)$ that separate states in $\mathcal{O}$.

Let's consider for instance the extreme cases of K-algebras split by L, namely the K-algebras K and L. Firstly, $Spec_L(L) = Hom_K(L, L) = G$. This means that the G-set associated to L is G itself with respect to the left action given by the product in G. Since $Spec_L(L) = G \simeq G/H_L$, the isotropy group H_L of the states in $Spec_L(L)$ is just the trivial group $\{id_G\}$. We could say that the 'resolving power' of L completely breaks all the indiscernibilities encoded in the Galois group $Gal(L : K)$. On the other extreme, $Spec_L(K) = Hom_K(K, L) = \{id_K\}$, i.e. the only K-morphism from K to L is just the identity on K. Hence, $Spec_L(K)$ is composed of a single state $\{id_K\} \doteq \{*\}$. Since $Spec_L(K) \simeq G/H_K$, the isotropy group H_K of the unique state $\{*\}$ in $Spec_L(K)$ must be the whole Galois group G. We can thus say that the whole space $Spec_L(L)$ collapses, from the 'viewpoint' of K, to a single maximally 'coarse-grained' state $\{*\}$. We can interpret this fact by taking into account that the only observables induced by K are the constant functions. Since constant functions assign the same numerical value to every possible state, no state can be discerned from any other.

Let's consider now the L-dual space $Spec_L(Fix(H))$ associated to the K-algebra $Fix(H)$ for some $H \subseteq G$. The observables induced by $Fix(H)$ separate the states in $Spec_L(Fix(H))$. This means that, from the viewpoint of the algebra $Fix(H)$, the space $Spec_L(Fix(H))$, far from being a purely numerical multiplicity of indiscernible states, is a qualitative multiplicity of discernible states that differ in some predicative respect. Now, each discernible state α in $Spec_L(Fix(H))$ is endowed with an isotropy group H that encodes the limitations of the resolving power of $Fix(H)$. In other terms, a state $\alpha \in Spec_L(Fix(H))$

is a 'H-coarse-grained' state composed of different 'micro-states' that cannot be discerned by means of the resolving power of $Fix(H)$. The 'internal symmetries' of α encoded by the isotropy group H, far from resulting from the *absolute* indiscernibility between the micro-states in the H-orbit α, are just a symptom of the limitations of the 'resolving power' of $Fix(H)$. By passing to a domain of rationality $Fix(H')$ endowed with a higher 'resolving power' (i.e. with $H' \subseteq H$), the indiscernibilities between the micro-states in a H-orbit can be partially broken. This means that the micro-states in a H-orbit can be partially discerned by $Fix(H')$. By 'observing' the states in $Spec_L(Fix(H))$ by means of the algebra $Fix(H')$, we obtain a space of states composed of a higher number of discernible states endowed with a smaller isotropy group H'. In other terms, the symmetry breaking process associated to an increasing of the 'resolving power' of the observable algebra separates each H-coarse-grained state into distinct H'-coarse-grained states that can be qualitatively discerned.

Conversely, let's see what happens when we try to discern states in $Spec_L(Fix(H))$ by means of a K-algebra endowed with a lower 'resolving power'. To do so, let's consider the observable algebra induced by $Fix(H'')$ with $H \subseteq H''$. Since H'' is bigger than H, the set $Fix(H'')$ of H''-invariant elements in L is smaller that $Fix(H)$. Hence, we can expect the observables induce by $Fix(H'')$ not to completely discern the states in $Spec_L(Fix(H))$. Let's consider for instance two states j and k in $Spec_L(Fix(H))$ such that $k = h'' \cdot j$ with $h'' \in H'' - H$. Since h'' is not in the isotropy group H of the states in $Spec_L(Fix(H))$, the states j and k are different states in this space. Now, any element f in the algebra $Fix(H'')$ satisfies $\hat{f}(h'' \cdot j) = \hat{f}(j)$ for $h'' \in H''$.[41] Then, all the observables induced by $Fix(H'')$ assign the same value to j and k even if they are different states in $Spec_L(Fix(H))$. This means that the 'resolving power' of the observables induced by $Fix(H'')$ are too weak to discern states in $Spec_L(Fix(H))$ connected by transformations in $H'' - H$. The observable algebra induced by $Fix(H)$ is the minimal observable algebra that discerns the H-coarse-grained states in $Spec_L(Fix(H)) \simeq G/H$. The space $Spec_L(Fix(H'')) \simeq G/H''$ of states that can be discerned by means of $Fix(H'')$ is smaller than $Spec_L(Fix(H)) \simeq G/H$ (since $H \subseteq H''$). In fact, a state in $Spec_L(Fix(H''))$ can be obtained by identifying the states in $Spec_L(Fix(H))$ connected by transformations in $H'' - H$. From the 'viewpoint' of $Fix(H)$, the states in $Spec_L(Fix(H''))$ are $(H'' - H)$-coarse-grained states.

We can thus conclude that the higher the resolving power of a K-algebra B, the higher the number of states in $Spec_L(B)$ that can be discerned by means of the observables induced by B and the smaller the isotropy group H_B that encodes the coarsegrainedness of these states. Reciprocally, the 'bigger' the isotropy group of each 'coarse-grained' state in a G-set, the 'smaller' the number of states in the G-set and the 'smaller' the observable algebra that separates these states. In this way, the different levels of the Galois-Grothendieck duality realize different combinations between the 'size' of the isotropy group of the 'coarse-grained' states and the 'size' of the observable algebra that discern these states. We could then rephrase the Galois-Grothendieck duality in the form of a *Galois indiscernibility principle*: the 'size' of the isotropy group of the 'coarse-grained' states in a G-set is inversely correlated to the 'size' of the minimal observable algebra that discern these states.

7. Conclusion

In order to address the notion of indiscernibility, we have proposed an *epistemic* reading of Galois-Grothendieck theory. According to this particular way of understanding Galois-Grothendieck theory, the *resolving power* of an *abstract algebra B* fixes the *coarsegrainedness* of the *states* in $Spec_L(B)$ that can be discerned by means of the *observable algebra* on $Spec_L(B)$ induced by B. In this geometric framework, the original Galois correspondence appears as an inverse correlation between the coarsegrainedness of the states and the size of the minimal observable algebra that discern these states (result that we have called *Galois indiscernibility principle*).

In order to conclude, we shall say some words about the relation between Galois-Grothendieck theory and Leibniz's *principle of the identity of indiscernibles*. According to Leibniz's principle, distinct individuals, i.e. individuals that differ numerically, must also differ in some predicative respect. In other terms, Leibniz claims that numerically distinct and indiscernible individuals cannot exist. According to this stance, we should be able to reduce every indexical "*thisness*" to a conceptually determined "*suchness*" [1, 36]. Now, in the framework of Galois-Grothendieck theory, the notion of indiscernibility, far from being an absolute notion, is indexed by the domain of rationality from which one is trying to discern the corresponding individuals. For instance, the (G, K)-indiscernibilities encoded in a Galois group $G_K(p)$, far from resulting from the *ontic* (or *absolute*) indiscernibility between the roots of $p \in K[x]$, result from the limitations of the domain of rationality K. In the framework of Galois-Grothendieck theory, the indiscernibility between two individuals always has (what we could call) an 'epistemic' cause. In this way, whereas Leibniz proposed to simply *identify* indiscernible individuals, Galois theory summons to *resolve*, *separate* or *discern* them by extending the original domain of rationality. The relative (G, K)-indiscernibility between two individuals, far from entailing their identity, means that the 'sufficient reason' that explains their qualitative (or predicable) difference lies beyond the domain of rationality K. In this way, a 'qualitative' multiplicity of L-discernible individuals can appear, from the restricted viewpoint of a domain of rationality K endowed with a lower resolving power, as a purely numerical multiplicity of (G, K)-indiscernible individuals.[42]

Taking into account what we have just said, we could be tempted to argue that in the last instance Galois-Grothendieck theory validates Leibniz's principle. Indeed, we could reformulate Leibniz's principle in a Galoisian manner by saying that the indiscernibility between two individuals necessarily results from the limits of the 'resolving power' of the algebraic 'devices' that allow us to 'observe' (or to 'speak about') the individuals in question. We could indeed maintain that in the last instance individuals that are absolutely indiscernible (i.e. irrespective of the indexation by any domain of rationality), cannot exist. However, it is worth stressing that Galois-Grothendieck theory is neutral with respect to such a possibility. Indeed, Galois-Grothendieck theory leaves open the question concerning the possible existence of entities that are *ontically* indiscernible, i.e. of entities that differ *solo numero* in any possible domain of rationality. Far from showing that 'individuals' that are absolutely indiscernible cannot exist, Galois-Grothendieck theory just shows how a relative 'epistemic' indiscernibility can result from the limited resolving power of the corresponding observable algebra.[43]

Acknowledgments

The research leading to these results has received funding from the European Research Council under the European Community's Seventh Framework Programme (FP7/2007-2013 Grant Agreement n° 263523). We also thank Daniel Bennequin for helpful discussions concerning the relationship between Galois theory and physics. The reading of his article *Questions de physique galoisienne* [4] was one of the original motivations for writing this work.

Notes

[1]This reference can be found in https://dspace.ist.utl.pt/bitstream/2295/575330/1/dissertacao.pdf.

[2]It is also worth mentioning that Da Costa, Rodriguez and Bueno developed, in the wake of the works of Jose Sebastiao e Silva and Mark Krasner, a "generalized or abstract Galois theory" (see Refs.[11, 12] and references therein). This theory relates the invariance under symmetry transformations on the one hand and the notion of definability with respect to a given language on the other.

[3]It is also worth noting that the formal analogy between Grothendieck-Galois theory and the Tannaka-Krein reconstruction theorem for compact topological groups points towards the possible relevance of the former in algebraic quantum field theory (see Refs.[7, 22, 34]). Indeed, the Tannaka-Krein formalism is at the heart of the analysis of superselection sectors in algebraic quantum field proposed by Doplicher, Haag, and Roberts (DHR) (see Ref.[21] and references therein).

[4]For an account of some recent developments of Galois' ideas, see Refs.[2, 3]. Different philosophical treatments of Galois theory can be found in Refs.[8, 28, 35, 37].

[5]A K-algebra A is a ring endowed with a scalar multiplication by elements of the field K such that $k(aa') = (ka)a'$ with $k \in K$ and $a, a' \in A$. Equivalently, a K-algebra is a K-vector space endowed with a multiplication. A typical example of a K-algebra is the power K^n where the addition and the multiplications are defined componentwise. The K-algebra K^n for $n > 1$ is not a field. For instance, the element $(1, 0) \in K^2$ does not have a multiplicative inverse (where the unit of K^2 is $(1, 1)$).

[6]It can be shown that a splitting field always exist and that two such fields are necessarily isomorphic (see Ref.[26], p. 236).

[7]Let's note that by writing the set X as $X = \{\alpha_1, \alpha_2, ..., \alpha_n\}$, we have ordered the set, i.e. we have chosen a bijection $Ord : \{1, 2, ..., n\} \to X$. The following discussion does not depend on this election.

[8]One can prove that this definition of K-indiscernibility is equivalent to that of Model Theory: for every first-order K-formula ϕ (not only the atomic ones) and every permutation σ, $K(\overrightarrow{\alpha}) \models (\phi(\overrightarrow{\alpha}) \Leftrightarrow \sigma \cdot \phi(\overrightarrow{\alpha}))$. See Ref.[30] (p. 178) for details.

[9]Indeed, $id_X \in S_K(X)$. If $\sigma_1, \sigma_2 \in S_K(X)$, then $\forall q$, $q(\overrightarrow{\alpha}) = 0 \Rightarrow \sigma_1 \cdot q(\overrightarrow{\alpha}) = 0$ and thus $\sigma_1 \cdot q$ annuls $\overrightarrow{\alpha}$ so that $\sigma_2 \cdot (\sigma_1 \cdot q) = (\sigma_2 \cdot \sigma_1) \cdot q$ annuls $\overrightarrow{\alpha}$. Finally, every σ in S_X is of finite order so that $\sigma^{-1} = \sigma^p$ for some $p \in \mathbb{N}$.

[10]With respect to the relations between the notions of *individuality* and *discernibility* (or *distinguishability*), we report the reader to Ref.[16]. It is worth noting that in Ref.[16], hypothetical elements that are *absolutely* indiscernible, i.e. elements that can be distinguished *solo numero* in any possible domain of rationality, are called *non-individuals*. Now, the notion of indiscernibility formalized by Galois theory is a weaker notion, since it is relative to the different possible domains of rationality. Therefore, we have decided to call the corresponding elements *K-indiscernible individuals*.

[11]Note that this definition of $Gal_K(p)$ depends on the choice of a splitting field K^p. Hence, the Galois group of $p(x)$ is actually defined up to isomorphisms.

[12]The kernel of a ring homomorphism $\sigma : K \to L$ is an ideal of K. But a field K has only one proper ideal, namely $\{0\}$. Hence, a field homomorphism $\sigma : K \to L$ is necessarily injective.

[13]It is worth stressing that the minimal polynomial $p_{\alpha,K}$ depends of the base field K. For instance, the minimal polynomial of $\sqrt[4]{3}$ is $X^4 - 3$ in $\mathbb{Q}$ and $X^2 - \sqrt{3}$ in $\mathbb{Q}(\sqrt{3})$.

[14]From the equation $p_{\alpha,K}(\alpha) = 0$, we can express α^n as a linear combination of $\{1, \alpha, ..., \alpha^{n-1}\}$ with coefficients in K. We can then express every $g(\alpha)$ in $K(\alpha)$ as a linear expression in $\{1, \alpha, ..., \alpha^{n-1}\}$. The minimality of $p_{\alpha,K}$ implies that these elements are linearly independent.

[15]Indeed, $q(\vec{\alpha}) = 0$ implies that $\sigma \cdot q(\vec{\alpha}) = q(\tilde{\sigma}^{-1}(\vec{\alpha})) = \tilde{\sigma}^{-1}(q(\vec{\alpha})) = \tilde{\sigma}^{-1}(0) = 0$.

[16]This definition does not depend on the choice of q. Indeed, $y = q(\vec{\alpha}) = q'(\vec{\alpha}) \Rightarrow (q - q')(\vec{\alpha}) = 0 \Rightarrow \sigma \cdot (q - q')(\vec{\alpha}) = 0$ since $\sigma \in Gal_K(p)$ and finally $\sigma \cdot q(\vec{\alpha}) = \sigma \cdot q'(\vec{\alpha})$.

[17] Consider for instance the polynomial $p(x) = x^3 - 2 \in \mathbb{Q}$. The unique $\mathbb{R}$-root of p is $\alpha = \sqrt[3]{2}$. If $\sigma \in Aut(\mathbb{Q}(\alpha) : \mathbb{Q})$, then $\sigma(\alpha)$ must also be a root of p in $\mathbb{Q}(\alpha)$. Since the other two roots of p are the complex numbers $j\alpha$ and $j^2\alpha$ with $j = e^{2i\pi/3}$ (which are not in $\mathbb{Q}(\alpha)$), necessarily $\sigma(\alpha) = \alpha$. Hence, $G = Aut(\mathbb{Q}(\alpha) : \mathbb{Q}) = \{id_{\mathbb{Q}(\alpha)}\}$ and $\mathbb{Q}(\alpha)^G = \mathbb{Q}(\alpha) \neq \mathbb{Q}$. Since not all the roots of $p(x)$ are in $\mathbb{Q}(\alpha)$, the transformation that permutes α and $j\alpha$ is not in G, but rather in $Aut(\mathbb{Q}(j, \alpha) : \mathbb{Q})$. One can prove that actually $(\mathbb{Q}(j, \alpha) : \mathbb{Q})$ is a Galois extension and that $Gal(\mathbb{Q}(j, \alpha) : \mathbb{Q}) \cong S_3$.

[18]The French philosopher Albert Lautman has described this succession of extensions from K to K^p as an "as ascent towards the absolute" by means of which the "the imperfection of a base field K with respect to a given polynomial" progressively decreases (see Ref.[**?**], pp. 126-128).

[19]For instance, the *diagonal* K-algebra K^m is not an integral domain, since $(1, 0, ..., 0)(0, 1, ..., 0) = (0, 0, ..., 0)$. Now, the roots in K^m of a polynomial $p(x) = (x - \alpha_1)...(x - \alpha_n)$ with $\alpha_i \in K$, are vectors $\overrightarrow{\alpha}$ whose components are given by the K-roots of $p(x)$. Each K-root α_i can be identified with the K^m-root $(\alpha_i, ..., \alpha_i)$ of m identical components. However, in addition to the K^m-roots induced by the n K-roots, one has all the K^m-roots given by vectors in K^m whose components are not all equal. These extra K^m-roots of $p(x)$ do not cancel any of the n linear factors of $p(x)$. Hence, the *reducible* minimal polynomial of each extra K^m-roots $\overrightarrow{\alpha}$ is the product of the factors $(x - \alpha_i)$ where the α_i's are the components of $\overrightarrow{\alpha}$.

[20]In the context of infinitary Galois theory, the corresponding dual spaces are indeed profinite *topological* G-spaces (see Ref.[5], p. 62). In what follows, we shall only consider the case of finite K-algebras and finite dual spaces. In this restricted framework, the topology of the dual spaces is the discrete topology. Hence, in the finite case the profinite topological G-spaces of the general theory will be simply replaced by G-sets.

[21]A K-homomorphism $\varepsilon \in Hom_K(\frac{K[x]}{\langle p(x) \rangle}, A)$ is completely specified by fixing the element $\alpha \in A$ to which $\overline{x}$ (i.e. the class of the polynomial $x \in K[x]$) is sent. In other terms, $\varepsilon(\bar{f}(x)) = f(\alpha)$, where $\bar{f}(x)$ denotes the class of $f(x)$ in $K[x]/\langle p(x) \rangle$. Now, in order to guarantee that such a morphism is a homomorphism of K-algebras, the zero in the quotient algebra $\frac{K[x]}{\langle p(x) \rangle}$ has to be sent to the zero in A. In particular, the polynomial $\bar{p}(x)$, being zero in $\frac{K[x]}{\langle p(x) \rangle}$, has to be sent to the zero in A. This means that $\varepsilon(\bar{p}(x)) = p(\alpha) = 0$. Hence, $\overline{x}$ has to be sent to a root α of $p(x)$ in A. In this way, a morphism in $Hom_K(\frac{K[x]}{\langle p(x) \rangle}, A)$ is completely specified by choosing a root α of $p(x)$ in A ([5], p. 22).

[22]Since we shall only consider the finite case, where $V_p(A)$ is discrete, the algebra $\mathcal{C}(V_p(A), A)$ of *continuous* functions coincides with the algebra $A^{V_p(A)}$ of all functions.

[23]The spectrum $Spec(\mathcal{U})$ of a C^*-algebra $\mathcal{U}$ is the (locally compact) space of its characters. A *character* is a non-null morphism of $\mathbb{C}$-algebras $\chi : \mathcal{U} \to \mathbb{C}$. If $\mathcal{U}$ is unital, $Spec(\mathcal{U})$ is a compact space. In functional analysis and modern mathematical physics, a *state* of a C^*-algebra $\mathcal{U}$ is defined as a morphism of $\mathbb{C}$-vector spaces $\phi : \mathcal{U} \to \mathbb{C}$ satisfying certain conditions (see for instance Ref. [25]). This explains why we have decided to call the points of $V_p(A)$ (i.e. the K-algebra morphisms $\alpha : \frac{K[x]}{\langle p(x) \rangle} \to A$) *$A$-states*.

[24]By *representation*, we understand here a K-algebra homomorphism. Equivalently, we can say that $\frac{K[x]}{\langle p(x)\rangle}$ is represented in $\mathcal{C}(V_p(A), A)$ as a multiplicative operator.

[25]For the characterization of *points* as representations of algebraic structures, see Ref.[6], §5.

[26]The fact that the functor of points is representable allows us to generalize the previous construction to any K-algebra, i.e. to K-algebras that are not necessarily of the form $\frac{K[x]}{\langle p(x)\rangle}$. Given any K-algebra B, we can define its functor of points as $V_B(-) = Hom_K(B, -)$. The set $V_B(A)$ can be considered as the set of A-points of B. We can now define a kind of Gelfand transform as $Gel_A : B \to A^{V_B(A)}$ given by $f \mapsto \hat{f}$ where $\hat{f}(\alpha) = \alpha(f) \in A$. Given a morphism $\phi : A \to C$ of K-algebras, the composition of morphisms of sets guarantees that ϕ induces a map $Hom_{K\text{-alg}}(B, A) \to Hom_{K\text{-alg}}(B, C)$ given by $f \mapsto \phi \circ f$. This means that the representable functor $V_B(-)$ is a covariant functor.

[27]This way of interpreting $\widehat{f}(\alpha)$ is justified by considering an analogous situation in the framework of the GNS (Gelfand-Naimark-Segal) construction for C^*-algebras applied to the commutative case. In this context, each $\mathbb{C}$-valued state $\chi : \mathfrak{U} \to \mathbb{C}$ on an abstract commutative C^*-algebra $\mathfrak{U}$ defines a different representation $\pi_\chi : \mathfrak{U} \to \mathcal{B}(\mathcal{H}_\chi)$ of $\mathfrak{U}$ in a Hilbert space $\mathcal{H}_\chi$ defined by χ. The Hilbert space $\mathcal{H}_\chi$ is the closure of $\mathfrak{U}/\mathcal{N}_\chi$, where $\mathcal{N}_\chi$ is the ideal $\mathcal{N}_\chi = \{f \in \mathfrak{U}/\chi(f^*f) = 0\}$. The representation π_χ of $\mathfrak{U}$ in $\mathcal{H}_\chi$ is given by $\pi_\chi(f)(\bar{g}) \doteq \overline{fg}$, where the bar denotes the equivalence classes in $\mathfrak{U}/\mathcal{N}_\chi$ (see Ref.[25], p. 53). The Gelfand transform $Gel : \mathfrak{U} \to \mathcal{C}_0(Spec(\mathfrak{U}), \mathbb{C})$ associates to each abstract algebra element $f \in \mathfrak{U}$ an observable $\hat{f}$ on the pure state space $\mathcal{P}(\mathfrak{U}) = Spec(\mathfrak{U})$. It is easy to see that the representation π_χ (which is irreducible if $\chi \in Spec(\mathfrak{U})$) of f acting on $\bar{g}$ amounts to multiply $\bar{g}$ by the complex number $\hat{f}(\chi) \in \mathbb{C}$, i.e. that $\pi_\chi(f)(\bar{g}) \doteq \overline{fg} = \hat{f}(\chi)\bar{g}$. Indeed, $\overline{fg} - \hat{f}(\chi)\bar{g} = 0$ in $\mathcal{H}_\chi$ iff $\overline{fg} - \hat{f}(\chi)\bar{g} \in \mathcal{N}_\chi$. Now, $h \in \mathcal{N}_\chi$ iff $\hat{h}(\chi) = 0$ (indeed, $h \in \mathcal{N}_\chi$ iff $\chi(h^*h) = 0$ iff $\widehat{h^*h}(\chi) = \hat{h}^*(\chi)\hat{h}(\chi) = |\hat{h}(\chi)|^2 = 0$ iff $\hat{h}(\chi) = 0$). In our case, $(\widehat{fg - \hat{f}(\chi)g})(\chi) = \hat{f}(\chi)\hat{g}(\chi) - \hat{f}(\chi)\hat{g}(\chi) = 0$. It is also worth noting that the set of numerical values $\left\{\hat{f}(\chi) = \chi(f)\right\}_{\chi \in Spec(\mathfrak{U})}$ that the observable $\hat{f}$ takes coincides with the spectrum of $f \in \mathfrak{U}$ (i.e. with the set of elements $\lambda \in \mathbb{C}$ such that $f - \lambda 1_{\mathfrak{U}}$ has no inverse in $\mathfrak{U}$). Indeed $\hat{f} - \lambda \cdot \hat{1}$ is not invertible iff there is some $\chi \in Spec(\mathfrak{U})$ such that $\hat{f}(\chi) - \lambda = 0$.

[28]By *duality* we merely mean here a functor $Hom_{K\text{-}Alg}(-, A)$ that permits to canonically associate the space $V_p(A) = Hom_{K\text{-}Alg}(\frac{K[x]}{\langle p(x)\rangle}, A)$ to the K-algebra $\frac{K[x]}{\langle p(x)\rangle}$. This duality is for the moment weak in the sense that the functor does not necessarily define an equivalence of categories.

[29]For instance, the set of $\mathbb{R}$-points of the polynomial $x^2 + 1$ is the empty set. Hence, the algebra $\frac{\mathbb{R}[x]}{\langle x^2+1\rangle} \simeq \mathbb{C}$ cannot be faithfully represented into an observable algebra on such a space.

[30]Let's consider an element $f \in K[x]$ such that $\widehat{f}(\alpha) = 0$ for every $\alpha \in V_p(K^p)$. Then, since p is assumed to be separable, the polynomial p divides f. Therefore, $\overline{f} = 0$ in $\frac{K[x]}{\langle p(x)\rangle}$. We have thus shown that a null function $\widehat{f}$ on $V_p(K^p)$ necessarily comes from the null element in $\frac{K[x]}{\langle p(x)\rangle}$. Hence, Gel_{K^p} is injective.

[31]Take for instance $K = \mathbb{R}$ and $p(x) = x^2 + 1$. Then $K^p \cong \frac{K[x]}{\langle p(x)\rangle} \cong \mathbb{C}$ and $V_p(\mathbb{C}) \cong 2$. But by no means $Gel_{\mathbb{C}} : \mathbb{C} \to \mathbb{C}^2$ can be surjective. In the general case, it can happen that a K-algebra B does not induce, via the corresponding Gelfand transform, all the A-valued observables on the A-dual space $V_B(A)$. For instance, if we take $B = K$ et $A = K^p$, the A-dual space is composed of a single point $V_K(K^p) = Hom_K(K, K^p) = \{id_K\}$ corresponding to the inclusion $K \hookrightarrow K^p$. Now, the image of the K-algebra K by the Gelfand transform is the algebra of K-valued functions on a one-point set, which coincides with K itself. Hence, it is evident that this observable algebra is not isomorphic to the algebra of K^p-valued observables on $V_K(K^p)$, which is K^p.

[32]A K-algebra A is *split* by an extension L of K if 1) A is algebraic over K and 2) the minimal polynomial over K of every element $\alpha \in A$ factorizes in $L[x]$ into linear polynomials with distinct roots. It can be shown that A is split by L if and only if there is some n such that $A \otimes L \cong L^n$ as L-algebras ([5], p. 23-24). It can also be shown that a K-algebra B split by L is a product $\prod_i B_i$ of intermediate fields $K \subseteq B_i \subseteq L$. It is worth noting that the fact that a K-algebra A is split by a field L does not mean that L contains all the roots of the minimal polynomials of every $\alpha \in A$. Since L is a field, it cannot contain all the roots belonging to K-algebras that are not fields.

[33]By the Primitive Element Theorem (see Ref.[26], p. 243), L is of the form $L = K(a) \cong K[x]/\langle q(x)\rangle$, where the irreducible and separable polynomial $q(x) \in K[x]$ has all its roots in L. This means that L is a splitting field K^q of $q(x)$. Hence the Gelfand transform is injective (see endnote N°30).

[34]It is worth noting that the possibility of making products in the algebraic category is a consequence of Grothendieck's generalization from fields to K-algebras. Indeed, while the product of K-algebras is a K-algebra, the product of two fields is not a field. This has as a consequence that the geometric category, far from only including *homogeneous* G-sets, includes general G-sets composed of many G-orbits.

[35]If B_1 and B_2 are two K-algebras, it is well-known that $B_1 \otimes_K B_2$ is their coproduct in the category of commutative K-algebras. Now if B_1 and B_2 are split by L, we have to check that $B_1 \otimes_K B_2$ is also split by L. But as K-algebras, $B_1 \otimes_K L \cong L^n$ and $B_2 \otimes_K L \cong L^m$ imply that $B_1 \otimes_K B_2 \otimes_K L \cong B_1 \otimes_K L^m \cong (B_1 \otimes_K L)^m \cong L^{nm}$, where we have used that $B \otimes_K L^m \cong (B \otimes_K L)^m$ (see Ref.[26], p. 608).

[36]Indeed, it can be shown that the application $\mu : K^X \otimes K^Y \to K^{X \times Y}$ defined by $\mu(f \otimes g)(x, y) \doteq f(x)g(y)$ is an isomorphism if X and Y are finite sets.

[37]Indeed, let's consider the restriction map $\varphi_{res} : \frac{G}{H} \to Hom_K(Fix(H), L)$ defined by $[g] \mapsto g|_{Fix(H)}$. This map is well-defined in the sense that it does not depend on the choice of g in the class $[g]$. If we take another $g' \in [g]$, we have $g' = g \cdot h$ for some $h \in H = Gal(L : Fix(H))$ and $g'|_{Fix(H)} = g|_{Fix(H)}$ since $h|_{Fix(H)} = id_{Fix(H)}$. The map φ_{res} is surjective because every $f \in Hom_K(Fix(H), L)$ can be extended to a $g \in Hom_K(L, L) = G$. Indeed, if $\overline{K}$ is an algebraic closure of K that contains L, f can be extended to a K-morphism $\overline{f} : L \to \overline{K}$ (see theorem 2.8 in Ref.[26], p. 233). We can then take $g = \overline{f}|_{Fix(H)}$. The normality of $(L : K)$ implies that $Im(g) \subseteq L$. Indeed, every a in $Fix(H)$

is a root of $p_{K,a}$ that belongs to L. Then $g(a)$ is also a root of $p_{K,a} \in K[x]$. By normality $g(a) \in L$ and thus $g \in G$. Finally, φ_{res} is injective since $\varphi_{res}(g) = \varphi_{res}(g') \Rightarrow (g' \cdot g^{-1})|_{Fix(H)} = id_{Fix(H)} \Rightarrow g' \cdot g^{-1} \in H \Leftrightarrow \overline{g'} = \overline{g}$. The map φ_{res} is obviously a G-morphism.

[38]We shall show that this is the case for a homogeneous G space $\mathcal{O} \simeq G/H$. Given a G-morphism $\phi : \frac{G}{H} \to L$, we want to define an element $a \in Fix(H)$. Let's take $a = \phi(\overline{e})$. We have to verify that a is in $Fix(H)$: for all $h \in H$, $h(a) = h(\phi([e])) = \phi(h \cdot [e]) = \phi([h \cdot e]) = \phi([h]) = \phi([e]) = a$. Reciprocally, given $a \in Fix(H)$ we want to define a morphism $\phi_a : \frac{G}{H} \to L$ and show that it is indeed a G-morphism. Let's define ϕ_a by $\phi_a([g]) = g(a)$. This definition does not depend on the choice of the representative g in the class $[g]$. For example if we take another $g' \in [g]$, we have $g' = g \cdot h$ for some $h \in H = Gal(L : Fix(H))$. Hence $h(a) = a$ and $g'(a) = g \cdot h(a) = g(a)$. Moreover, $\phi_a(g' \cdot [g]) = \phi_a([g' \cdot g]) = (g' \cdot g)(a) = g' \cdot g(a) = g' \cdot \phi_a([g])$, which means that ϕ_a is indeed a G-morphism. It is easy to verify that the two processes are inverse one of the other.

[39]As we argued in Section N°5, it is the L-algebra $B \otimes_K L$ that is isomorphic to the whole algebra of L-valued observables on $Spec_L(B)$.

[40]According to the Galois correspondence, $H = Gal(L : Fix(H))$. For every $f \in Fix(H)$, $\widehat{f}([g_1]) = \widehat{f}([g_2]))$ if and only if $\widehat{f}(g_1|_{Fix(H)}) = \widehat{f}(g_2|_{Fix(H)})$, where we have used the isomorphism (4). Now, this will be the case if and only if $g_1(f) = g_2(f)$, that is if and only if $g_2^{-1} g_1 \in H$. This implies that $[g_1] = [g_2]$.

[41]Indeed the L-valued observable algebra induced by $Fix(H'')$ is $\mathcal{C}(G/H'', L)$, which can be identified with the algebra of functions $f : G \to L$ that are constant on every H''-orbit.

[42]The relationship between Galois theory and the notion of individuals was also addressed in Ref.[35], notably in §32, pp. 286-289.

[43]With respect to the relationship between Galois theory and the problem of absolute indiscernibility see also Ref.[23]. In Ref.[16], the notion of (what the authors call) *non-individuals* (i.e. of entities that are absolutely indiscernible) is extensively addressed.

References

1. Adams, R. M.: 1979, Primitive thisness and primitive identity, The Journal of Philosophy 76(1), 526.
2. André, Y.: 2011, Idées galoisiennes, in Histoires de Mathématiques, Journes X-UPS, May 2011 (arXiv:1207.3381), published by Ecole Polytechnique, France.
3. André, Y.: 2008, Ambiguity theory, old and new, arXiv:0805.2568 [math.GM].
4. Bennequin, D.: 1994, Questions de physique galoisienne, in M. Porte (eds), Passion des Formes, à René Thom, E.N.S. Éditions Fontenay - Saint Cloud, Fontenay - Saint Cloud, pp. 311-410.
5. Borceux, F. and G. Janelidze: 2001, Galois theories, Cambridge University Press, Cambridge.
6. Cartier, P.: 2001, A Mad's Day Work: From Grothendieck to Connes and Kontsevich. The Evolution of Concepts of Space and Symmetry, Bulletin (New Series) of the American Mathematical Society 38(4), 389-408.
7. Chargois, F.: 2005, L'influence de la théorie de Galois sur l'œuvre de Grothendieck, in J. Kouneiher, D. Flament, P. Nabonnand and J.-J. Szczeciniarz (eds), Géométrie au XXe Siècle. Histoire et horizons, Hermann Éditeurs, Paris, pp. 78-92.
8. Châtelet, G.: 2010, L'enchantement du virtuel. Mathématique, physique, philosophie, Éditions rue dUlm, Paris.
9. Connes, A. and M. Marcolli: 2004, Renormalization and motivic Galois theory, International Mathematics Research Notices 76, 4073-4091.
10. Connes, A., F. Fauvet and J.-P. Ramis: 2009, Renormalization and Galois Theories, European Mathematical Society Publishing House, Zurich.
11. Da Costa, N.C.A. and A.A.M. Rodrigues: 2007, Definability and Invariance, Studia Logica : An International Journal for Symbolic Logic 86(1), 1-30.
12. Da Costa, N.C.A. and O. Bueno: 2011, Remarks on Abstract Galois Theory, Manuscrito Rev. Int. Fil., Campinas 34(1) 151-183.
13. Dixmier, J.: 1977, C*-Algebras, North-Holland Publishing Compagny, Amsterdam.
14. Douady, R. and A. Douady: 2005, Algèbres et théories galoisiennes, Cassini, Paris.
15. Eisenbud, D. and J. Harris: 2001, The Geometry of Schemes, Springer-Verlag, New York.
16. French, S. and D. Krause: 2006]: Identity in Physics : A Historical, Philosophical, and Formal Analysis, Oxford University Press, Oxford.
17. Goethe, J.W.: 1998, Maxims and Reflections, transl. by E. Stopp, Penguin Books, London.
18. Grothendieck A.: 1960, Technique de descente et théorèmes d'existence en géométrie algébrique, II. Le théorème d'existence en théorie formelle des modules, Séminaire Bourbaki 195.
19. Grothendieck, A.: 1971, Revêtements étales et groupe fondamental, SGA1, 1960-61, Lecture Notes in Math. 224, Springer-Verlag, Berlin, New York.
20. Grothendieck, A. and J.A. Dieudonné: 1971, 'Eléments de Géométrie Algébrique I, Springer-Verlag, Berlin-Heidelberg.
21. Halvorson, H. and M. Mueger: 2006, Algebraic Quantum Field Theory, in Handbook of the Philosophy of Physics, North Holland, Amsterdam.
22. Joyal, A. and S. Ross: 1991, An Introduction to Tanaka Duality and Quantum Groups in A. Carboni, M.C. Pedicchio and G. Rosolini (eds), Category Theory, Proceedings, Como 1990, Lecture Notes in Math. 1488, Springer-Verlag Berlin, Heidelberg, pp. 411-492.
23. Krause, D.: 2011, The Metaphysics of Non-individuality, in D. Krause and A. Videira (eds), Brazilian Studies in Philosophy and History of Science. An Account of Recent Works, Springer, New-York, pp.257-267.

24. Kronecker, L.: 1895-1930, Werke, vol. 2, Teubner, Leipzig.
25. Landsman, N.P.: 1998, Mathematical Topics Between Classical and Quantum Mechanics, Springer, New York.
26. Lang S.: 2005, Algebra, Springer, New-York.
27. Lastaria, F.: 1996, On Separable Algebras in Grothendieck Galois Theory, Le Matematiche LI, 127-136.
28. Lautman, A.: 2011, Mathematics, Ideas and the Physical Real, trans. by S.B. Duffy, Continuum, London.
29. Lavwere, F.W. and R. Rosebrugh: 2003, Sets for Mathematics, Cambridge University Press, Cambridge.
30. Marker, D.: 2002, Model theory : an introduction, Springer-Verlag, New-York.
31. Saunders, S.: 2003, Physics and Leibniz's principles, in K. Brading and E. Castellani (eds), Symmetries in Physics: Philosophical Reflections, Cambridge University Press, Cambridge.
32. Szamuely T.: 2009, Galois Groups and Fundamental Groups, Cambridge Studies in Advanced Mathematics, vol. 117, Cambridge University Press, Cambridge.
33. Szczeciniarz, J.-J.: 2013, The mysterious strength of the Galois theory, in Evariste Galois - Bicentenary - Meeting, November 21-25, 2011 Proceedings, Editions du CLE Campinas and Hermann, Paris, in print.
34. Szyld, M.: 2011, On Tannaka duality, Tesis de Licenciatura, Universidad de Buenos Aires (arXiv:1110.5293).
35. Vuillemin, J.: 1962, La philosophie de l'algèbre, Presses Universitaires de France, Paris.
36. Weyl, H.: 1949, Philosophy of mathematics and natural science, Princeton University Press, Princeton.
37. Zalamea, F.: 2013, Synthetic Philosophy of Contemporary Mathematics, Urbanomic/Sequence Press.