ON THE GALOISIAN STRUCTURE OF HEISENBERG INDETERMINACY PRINCIPLE

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

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 revisit Heisenberg indeterminacy principle in the light of the Galois-Grothendieck theory for the case of finite abelian Galois extensions. In this restricted framework, the Galois-Grothendieck duality between finite K-algebras split by a Galois extension L and finite $Gal(L:K)$-sets can be reformulated as a Pontryagin-like duality between two abelian groups. We then define a *Galoisian quantum theory* in which the Heisenberg indeterminacy principle between conjugate canonical variables can be understood as a form of Galoisian duality: the larger the group of automorphisms $H \subseteq G$ of the states in a G-set $\mathcal{O} \simeq G/H$, the smaller the "conjugate" observable algebra that can be consistently valuated on such states. We then argue that this Galois indeterminacy principle can be understood as a particular case of the Heisenberg indeterminacy principle formulated in terms of the notion of *entropic indeterminacy*. Finally, we argue that states endowed with a group of automorphisms H can be interpreted as *squeezed coherent states*, i.e. as states that minimize the Heisenberg indeterminacy relations.

1. Introduction

Both Galois theory and quantum mechanics are theories that formalize what appear (at least in a first approximation) as different forms of limitations. In Galois theory, the Galois group of a polynomial $p(x) \in K[x]$ measures the limits of the field K to *discern* the K^p-roots of $p(x)$ (where K^p is a splitting field of p). In quantum mechanics, Heisenberg indeterminacy principle formalizes the limits imposed by the quantum formalism to the joint sharp *determination* of conjugate canonical variables. Whereas Galois theory concerns the relative *indiscernibility* of roots of polynomials, quantum mechanics concerns the partial *indeterminacy* of conjugate variables. Moreover, both kind of limitations appear in different degrees. In Galois theory, the different degrees of relative M-indiscernibility defined by the different intermediate fields $K \subseteq M \subseteq K^p$ give rise to a lattice of subgroups $Gal(K^p : K) \supseteq Gal(K^p : M) \supseteq Gal(K^p : K^p)$ of the corresponding Galois group $Gal(K^p : K)$. In quantum mechanics, the indeterminacies of conjugate canonical variables can appear in different combinations satisfying Heisenberg indeterminacy principle.

In Ref.[1], Bennequin conjectured that it might be possible to understand quantum mechanics in the light of Galois theory. Now, there is an important conceptual obstruction to the hypothetical existence of a positive relation between both kinds of "limitations". On the one hand, the indiscernibility between numerically different roots in Galois theory is relative to a particular field. If two roots of a polynomial are indiscernible with respect to a field K, it is always possible to extend K to a field M endowed with a higher "resolving power" such that the two roots are M-discernible. Whereas K-indiscernible individuals differ *solo numero* from the viewpoint of K, they differ in some predicative respect when "observed" from M (see Ref.[7] for such an "epistemic" interpretation of Galois theory). On the contrary, the quantum indeterminacy cannot be broken. This means that it is not possible to jointly determinate the values of two conjugate variables in a sharp manner by increasing the "resolving power" of the measuring devices. We could say that whereas the Galoisian indiscernibility seems to be an *epistemic* notion resulting from the "limits" of the different "domains of rationality" M, the quantum indeterminacy seems to be an *ontologic* (or intrinsic) property of quantum systems. Now, in what follows we argue that it is after all possible to understand the quantum indeterminacy in the light of the Galoisian notion of indiscernibility. In principle, we could foresee two strategies for doing so. Firstly, we could try to adapt our comprehension of quantum mechanics to the epistemic scope of Galois theory by endorsing an epistemic view of the former (for such an epistemic view of quantum mechanics see for instance Ref.[18]). Alternatively, we could try to adapt our comprehension of Galois theory to an ontologic interpretation of quantum mechanics by endorsing an ontologic interpretation of both theories. In what follows, we explore this last alternative.

On the one hand, we proposed in Refs.[4, 5, 6] an ontologic interpretation of quantum mechanics by arguing that quantum states describe structure-endowed entities characterized by non-trivial *phase groups* of automorphisms. We argued that Heisenberg indeterminacy principle results from a compatibility condition between the internal symmetries of the states and the observables that can be consistently valuated on such states, i.e. that are compatible with their internal phase symmetries. On the other hand, the proposed ontologic interpretation of Galois theory is based on Grothendieck's reformulation and generalization of the original Galois theory [3, 20]. According to Grothendieck's generalization, the Galois correspondence can be reformulated as an anti-equivalence of categories between the categories of finite commutative K-algebras split by a field L (where $(L : K)$ is a finite Galois field extension) and the categories of finite $Gal(L : K)$-sets. Considered from the proposed ontologic perspective, the elements in a homogeneous G-set $\mathcal{O} \simeq G/H$ will not be interpreted as *H-coarsegrained individuals* (as it was done in Ref.[7]), but rather as *structure-endowed entities whose automorphism group is H*. From this viewpoint, the group H does not measure the *relative coarsegrainedness* of the "observed" individuals with respect to a given observable algebra, but rather the *intrinsic symmetries* of the structures parameterized by $\mathcal{O}$. In other terms, whereas in Ref.[7] the Galois groups were interpreted as a measure of the relative indiscernibility of the corresponding individuals with respect to different "domains of rationality", we now interpret these groups as automorphism groups of *non-rigid* (or *automorphic*) structures. We then interpret the Galois correspondence as a correspondence between "moduli spaces" of H-automorphic structures on the one hand and the observable algebras that can be consistently valuated on such structures (i.e. that are compatible with their automorphism group H) on the other. Roughly speaking, the bigger the group of automorphisms of the structures, the smaller the observable algebra that satisfies this compatibility condition.

2. Galois indiscernibility principle

In this section, we introduce the Galois-Grothendieck duality (for more details see Ref.[3] and Ref.[7] for a conceptual analysis). This duality can be understood as an enrichment of the original Galois correspondence by placing it in the framework of the Gelfand duality between algebras and spaces. Given a finite Galois extension $(L : K)$ with Galois group $G \doteq Gal(L : K)$, the Galois theory provides a correspondence between intermediate fields $K \subseteq F = Fix(H) \subseteq L$ and subgroups $H = Gal(L : F)$ of G. Grothendieck reformulated and generalized this correspondence in terms of an anti-equivalence of categories between the category $Split_K(L)_f$ of finite commutative K-algebras split by L and the category G-$FSet$ of finite G-sets. The so-called *spectrum functor*

$$Spec_K(-) \doteq Hom_{K\text{-}Alg}(-, L) : Split_K(L)_f \to G\text{-}FSet$$

associates to each intermediate field F (considered as a K-algebra) a *homogeneous* G-set isomorphic to G/H for $H = Gal(L : F)$. The G-action on $Spec_K(\mathcal{B}) = Hom_{K\text{-}Alg}(\mathcal{B}, L)$ (for $\mathcal{B}$ a K-algebra) is given by the following composition

$$\begin{array}{rcl} G \times Hom_{K\text{-}Alg}(\mathcal{B}, L) & \to & Hom_K(\mathcal{B}, L) \\ (g, \chi) & \mapsto & g \circ \chi. \end{array}$$

The so-called *Gelfand transform* associates to each abstract K-algebra $\mathcal{B}$ a subalgebra of the *observable algebra* over its spectrum. Indeed, the Gelfand transform

$$\begin{array}{rcl} Gel_L : \mathcal{B} & \rightarrow & \mathcal{C}(Spec_K(\mathcal{B}), L) = L^{Spec_K(\mathcal{B})}, \\ f & \mapsto & \hat{f} \end{array}$$

defined by

$$\hat{f}(\chi) = \chi(f), \qquad \chi \in Spec_K(\mathcal{B})$$

sends each abstract K-algebra $\mathcal{B}$ to a subalgebra of the observable algebra of L-valued functions on the spectrum $Spec_L(\mathcal{B})$ of $\mathcal{B}$. It is possible to obtain an isomorphism between an abstract algebra and the whole observable algebra $\mathcal{C}(Spec_K(\mathcal{B}), L)$ by extending the scalars of the K-algebras $\mathcal{B}$ from K to L. The extension of scalar functor sends K-algebras to L-algebras by means of the expression $\mathcal{B} \mapsto \mathcal{B} \otimes_K L$. It can be shown that the Gelfand transform is an isomorphism between the abstract L-algebra $\mathcal{A} \doteq \mathcal{B} \otimes_K L$ and the observable L-algebra $\hat{\mathcal{A}} \doteq \mathcal{C}(Spec_K(\mathcal{B}), L) = L^{Spec_K(\mathcal{B})}$ (see Ref.[3], p. 24).[1]

The observable L-algebra $\hat{\mathcal{A}}$ (isomorphic to $\mathcal{A}$) is endowed with a semilinear G-action (called *descent action*) given by the expression[2]

$$(g \cdot \hat{a})(\chi) = g(\hat{a}(g^{-1}\chi)),$$

where $\chi \in Spec_K(\mathcal{B})$. Thanks to the isomorphism between $\mathcal{A}$ and $\hat{\mathcal{A}}$, we can transpose this G-action to $\mathcal{A}$. Then the original K-algebra $\mathcal{B}$ can be reobtained as the G-invariant part of $\mathcal{A}$:

$$\mathcal{B} = Fix_G(\mathcal{A}) = \{a \in \mathcal{A} / \forall g \in G, g \cdot a = a\}.$$

This invariance condition can be rewritten as $\hat{a}(g\chi) = g(\hat{a}(\chi))$. This means that the G-invariant elements in the L-algebra $\mathcal{A}$, i.e. the elements in the K-algebra $\mathcal{B}$, define L-valued observables on $Spec_K(\mathcal{B})$ that are G-morphisms between $Spec_K(\mathcal{B})$ and L. In what follows, the observables that are G-morphisms are called *G-observables*. The algebra $\mathcal{B}$ can be directly obtained from the "space" $Spec_K(\mathcal{B})$ by means of a functor adjoint to the spectrum functor, namely the *functor of G-observables* $\mathcal{C}^G(-, L) \doteq Hom_{G\text{-}Set}(-, L)$. Conceptually, whereas the spectrum functor $Spec_K(-)$ associates a "space" to an abstract algebra, the functor $\mathcal{C}^G(-, L)$ recovers the algebra as the subalgebra of G-observables of the whole observable algebra on the "space".

Let's consider now an intermediate field $F = Fix(H)$ for H a subgroup of the Galois group G. The spectrum functor $Spec_K(-)$ yields the *minimal* space of "states" $Spec_K(F) \simeq G/H$ that supports the observables defined by F. Indeed, $F = Fix(H)$ does not induce well-defined observables on the smaller G-set $Spec_K(Fix(H')) \simeq G/H'$ for $H' \supset H$. Conversely, the fact that the states in $Spec_K(F)$ are interpreted as structures endowed with a non-trivial group of automorphisms H implies that not every algebraic element in L defines an observable over $Spec_K(F)$. Indeed, only the elements in L that are H-invariant induce well-defined observables on $Spec_K(F)$. The intermediate field F obtained from $Spec_K(F)$ by means of the functor $\mathcal{C}^G(-, L)$ is the *maximal* K-algebra that satisfies this compatibility condition, i.e. that can be consistently evaluated on the H-automorphic states parameterized by $Spec_K(F)$. The *maximality* of the K-algebras yield by the functor $\mathcal{C}^G(-, L)$ means that these algebras *completely discern* the states in the corresponding G-sets. Indeed, F does induce well-defined observables on spaces of states $Spec_K(Fix(H'')) \simeq G/H''$ (with $H'' \subset H$) that are *bigger* than $Spec_K(H)$. However, the observable algebra on $Spec_K(Fix(H''))$ induced by F cannot *separate* (or *completely discern*) the H''-automorphic structures parameterized by $Spec_K(Fix(H''))$. In particular, F is isomorphic to the K-algebra of L-valued G-observables on $Spec_K(L) = Hom_{K\text{-}Alg}(L, L) = G$ *that take the same value on elements related by a transformation in* H:

$$F \cong_{K\text{-}Alg} \{\widetilde{f} \in Hom_G(G, L) / \widetilde{f}(g \cdot h) = \widetilde{f}(g), \forall g \in G, \forall h \in H\}.$$

[1] It is worth noting that the L-spectrum of $\mathcal{B} \otimes_K L$, that is $Spec_L(\mathcal{B} \otimes_K L) = Hom_{L\text{-}Alg}(\mathcal{B} \otimes_K L, L)$, coincides with $Spec_K(\mathcal{B})$ [3].

[2] The semilinearity of the action means that $g \cdot (la + bb') = g(l)g(a) + (g \cdot b)(g \cdot b')$ for all $l \in L$ and all a, b, b' in $\mathcal{A}$.

In Ref.[7], we have summarized the duality between abstract K-algebras and G-sets by means of what we have called *Galois indiscernibility principle*. By using the fact that every finite K-algebra $\mathcal{B}$ split by L is a product of some intermediate fields F of the extension $(L:K)$, we can restrict the analysis to the case $\mathcal{B}=F$. In the framework of the ontologic interpretation of Galois-Grothendieck theory advocated here, we can restate the principle proposed in Ref.[7] as follows: *the "size" of the group of automorphisms H of the pure states parameterized by a G-set $\mathcal{O}\simeq G/H$ is inversely correlated to the "size" of the maximal observable algebra that can be consistently evaluated on these states, i.e. of the observable algebra that completely discerns the states in $\mathcal{O}$.* In other terms, *the bigger is the group of automorphisms $H=Gal(L:F)$ of the states in the homogeneous G-space $Spec_K(F)\cong G/H$, the smaller is the maximal L-algebra of observables $F\otimes_K L\cong L^{G/H}$ that can be consistently valuated on $Spec_K(F)$* (and reciprocally). If the automorphism group is trivial $H=1_G$, i.e. if the structures parameterized by $\mathcal{O}\simeq G/1_G=G$ are *rigid structures*, then the compatibility condition becomes trivial: all the elements in L induce well-defined observables on $\mathcal{O}$. At the other extreme, if the automorphism group of the structures is G itself, then only the elements in K define observables on the unique G-automorphic structure described by the one-point space $\mathcal{O}\simeq G/G=\{*\}$. We can give a quantitative formulation of this principle as follows. On the one hand, the L-algebra $\mathcal{A}\doteq F\otimes_K L\simeq L^{G/H}$ is isomorphic to $L^{Card(G/H)}$. Hence, the dimension of $\mathcal{A}$ as an L-vector space is $dim_L(\mathcal{A})=Card(G/H)$. On the other hand, we can define the degree of symmetry of the automorphic states in $Spec_L(\mathcal{A})\simeq G/H$ as $sym(Spec_L(\mathcal{A}))=Card(H)$. Then, the Galois indiscernibility principle takes the following (trivial) numerical expression:

$$dim_L(\mathcal{A})sym(Spec_L(\mathcal{A}))=Card(G/H)Card(H)=Card(G).$$

3. Harmonic interpretation of the Galoisian indiscernibility

In this section, we restrict the Galois-Grothendieck duality to the case of finite abelian Galois groups. This restriction allows us to reformulate the Galois-Grothendieck duality between finite K-algebras split by L and finite G-sets as a Pontryagin duality between two finite abelian groups. Now, the Pontryagin duality between two locally compact abelian (LCA) groups encodes the complementarity between conjugate variables (such as q and p) in quantum mechanics. Therefore, the restriction to finite (and thus locally compact) abelian groups allows us to establish a link between the Galois-Grothendieck duality on the one hand and the Pontryagin duality between conjugate canonical variables in quantum mechanics on the other.

The Pontryagin duality between a LCA group G and its unitary dual $\hat{G}\doteq Hom_{Group}(G,U(1))$ is given by a canonical isomorphism $G\simeq\hat{\hat{G}}$. This isomorphism is defined by the Gelfand transform $g\mapsto\hat{\hat{g}}$ given by $\hat{\hat{g}}(\chi)=\chi(g)$ (where $\chi\in\hat{G}$). Let's consider now a Galois extension $(L:K)$ such that the corresponding Galois group is a finite abelian group G. Then, $Spec_K(L)=Hom_{K\text{-}Alg}(L,L)\simeq G$. Therefore, we have two alternative descriptions of G, namely 1) as the spectrum of L, and 2) as the dual of $\hat{G}$. In turn, the field L, considered as a K-algebra, defines the algebra $\hat{L}=\mathcal{C}(Spec_K(L),L)=L^G$ of L-valued observables on $Spec_K(L)\simeq G$. On the other hand, $\hat{G}$ defines $U(1)$-valued observables on G. Now, what is the relationship between these two observable structures? Let's assume that L contains the n distinct nth-roots of unity in $\mathbb{C}$, where $n=Card(G)$. These roots form a multiplicative subgroup $\mu_n(L)$ of $(L^*,\times)$. Under this condition, the group $\widehat{G}\doteq Hom_{Group}(G,U(1))=Hom_{Group}(G,(\mathbb{C}^*,\times))$ can be expressed as $\widehat{G}\cong Hom_{Group}(G,(L^*,\times))$.[3] This means that the multiplicative characters in $\hat{G}$ can be interpreted as L-valued observables on G, i.e. as elements in L^G. Moreover, it can be shown that the characters in $\hat{G}$ define a basis of the whole observable algebra L^G as a L-vector space ([12], p. 283). This means that among all the L-valued observables on G, there are n privileged observables

[3]Indeed, $Hom_{Group}(G,(L^*,\times))\cong Hom_{Group}(G,(\mu_n(L),\times))\cong Hom_{Group}(G,(\mu_n(\mathbb{C}),\times))\cong\widehat{G}$. This results from the fact that $\chi(g)^n=\chi(g^n)=\chi(1_G)=1_L$ for every $\chi\in Hom_{Group}(G,(L^*,\times))$ and every $g\in G$. Therefore, $Im\chi\subseteq\mu_n(L)=\mu_n(\mathbb{C})$.

that form an abelian group and span the whole observable algebra L^G. Hence, the Galois-Grothendieck duality for the case of an abelian Galois group (provided that L satisfies the aforementioned condition) contains a hidden Pontryagin duality, namely the duality between $Spec_K(L) = G$ and the subgroup $\hat{G} \subset ((L^*)^G, \times)$ of multiplicative characters on G. We can schematize what we have said by means of the following diagram:

$$\begin{tikzcd} & \hat{L} = \mathcal{C}(G, L) & \\ L \arrow[ur, "Gel_L"] \arrow[r, "Spec_K(-)"'] & G & \hat{G} \arrow[ul, hook'] \end{tikzcd}$$

Since G is abelian, its subgroups H are necessarily normal. Then, the G-sets G/H are always (abelian) groups. Therefore, the previous reasoning can be repeated at each level of the Galois-Grothendieck duality. More precisely, the $n_{G/H} = Card(G/H)$ multiplicative characters in $\widehat{G/H}$ span the observable algebra $L^{G/H}$ as a L-vector space.

In what follows the elements in G and $\hat{G}$ are called *pure states* and *elementary observables* respectively. Now, in the aforementioned construction there is a significant asymmetry between these two notions: whereas we can obtain any observable in L^G by linearly superposing the *elementary observables* in $\hat{G}$, for the moment we have not considered any superposition of the pure states in G. Now, by duality the pure states in G define (elementary) "observables" on $\hat{G}$. Moreover, any element in $L^{\hat{G}}$ can be obtained by superposing the elementary "observables" on $\hat{G}$ defined by G. In other terms, $\hat{\hat{G}} \simeq G$ defines a basis of $L^{\hat{G}}$. Hence, the symmetry of the situation (i.e. the interchangeability of G and $\hat{G}$) suggests that we must also consider superpositions of the pure states in G. Now, the L-superposition of the group elements in G defines the so-called *group algebra* $L[G]$.

Both the group algebras $L[G]$ and $L[\widehat{G}]$ and the observable algebras L^G and $L^{\widehat{G}}$ are Hopf algebras [14]. Since G and $\hat{G}$ induce basis of $L^{\widehat{G}}$ and L^G respectively, it is easy to show that $L[G] \cong L^{\widehat{G}}$ and $L[\widehat{G}] \cong L^G$ as Hopf algebras, where the isomorphisms are given by the Fourier transforms (see Ref.[14], pp. 12-14).[4] Conceptually, the (inverse) Fourier transform sends the algebra $L[\widehat{G}]$ of superposed multiplicative characters in $\hat{G}$ to the whole observable algebra L^G on the space of pure states G. Therefore, the Fourier transform can be understood as the Gelfand transform for algebras. The described dualities can be summarized by means of the following diagram

$$\begin{tikzcd} L^G & L^{\hat{G}} \\ L[G] \arrow[ur] & L[\hat{G}] \arrow[ul] \end{tikzcd}$$

where the arrows are given by the (inverse) Fourier transforms.

What we have just said about the dualities between $L[G]$, $L[\hat{G}]$, L^G and $L^{\hat{G}}$ remains valid if we substitute G by G/H. Let's consider now the unitary dual $\widehat{G/H}$ of a G-set $Spec_K(Fix(H)) \simeq G/H$. To

[4]For instance, the inverse (discrete) Fourier transform can be defined by

$$\begin{array}{rcl} \mathcal{F}^{-1} : L[\widehat{G}] & \rightarrow & L^G \\ f \doteq \sum_{\chi \in \widehat{G}} f(\chi)\chi & \mapsto & \mathcal{F}^{-1}(f), \end{array}$$

where

$$\mathcal{F}^{-1}(f)(g) \doteq \frac{1}{\sqrt{n}} \sum_{\chi \in \widehat{G}} f(\chi)\chi(g),$$

for $n = Card(G)$. This expression explicitly shows that this inverse Fourier transform is just the linear extension of the Gelfand transform between $\widehat{G}$ and the observables on G.

do so, let's define the *conjugate group* $H^{\perp} \subseteq \hat{G}$ of H as

$$H^{\perp} = \{\chi \in \hat{G} / \chi(gh) = \chi(g), \forall h \in H, \forall g \in G\}. \tag{1}$$

or equivalently as

$$H^{\perp} = \{\chi \in \hat{G} / \chi(h) = 1, \forall h \in H\}.$$

We can now express $\hat{H}$ as

$$\hat{H} \cong \hat{G}/H^{\perp}. \tag{2}$$

This just means that the characters on H are the characters on G modulo the characters that are trivial on H. Conversely, the definition (1) implies that[5]

$$H^{\perp} \cong \widehat{G/H}, \tag{3}$$

i.e. that $H^{\perp}$, being composed of the elements in $\hat{G}$ that take the same value on the H-orbits in G, defines the characters on the quotient G/H.

Now, the bigger H, the smaller $H^{\perp}$ (and reciprocally). If $H = G$ (i.e., in the case in which the G-set of pure states is isomorphic to $G/G = \{*\}$), $H^{\perp} = G^{\perp}$ is composed of all the $\chi \in \hat{G}$ such that $\chi(g) = 1$ *for all* $g \in G$. Now, the only character in $\hat{G}$ that satisfies this condition is $\chi = 1_{\hat{G}}$. Indeed, $1_{\hat{G}}$ is the multiplicative character that defines the trivial representation. Hence, if the automorphism group of the states in a G-set is the biggest possible one (namely G-itself), the G-set is composed of a single state and only the trivial elementary observable $\chi = 1_{\hat{G}}$ in $\hat{G}$ can be valuated on such state. Roughly speaking, in the "universe" defined by the Galois extension $(L : K)$, there can exist a unique structure with the highest possible symmetry (encoded by the whole group G). If we want to define *non-trivial* "moduli spaces" of structures that differ in some predicative respect, we have to consider structures endowed with a smaller group of automorphisms H. By doing so, the compatibility condition on the observables is less restrictive. In turn, this leads to a non-trivial algebra of observables that can assign different properties to the different H-structures. In the limit, if $H = 1_G$ (i.e., in the case in which the G-set of pure states is isomorphic to $G/1_G = G$), the conjugate group $H^{\perp} = 1_G^{\perp}$ is composed of all the $\chi \in \hat{G}$ such that $\chi(1_G) = 1$. Since $\hat{G}$ is composed of group morphisms, all the χ satisfy this property. Hence, if the pure states in G are rigid structures (i.e. if they have no automorphisms), then every elementary observable in $\hat{G}$ can be evaluated on such states.

According to its definition, $H^{\perp}$ is the solution in $\hat{G}$ of the system of equations $\{\chi(h) = 1\}_{h \in H}$ defined by the pure states in H. Conversely, H is the solution in G of the system of equations $\{\chi(g) = 1\}_{\chi \in H^{\perp}}$ defined by the elementary observables in $H^{\perp}$.[6] By using the language of algebraic geometry, we could say that H can be thought of as the "variety" in G defined by the family of equations $\chi(g) = 1$ for every $\chi \in H^{\perp}$. Conversely, given the "variety" $H \subset G$, we can define the family $H^{\perp}$ of elementary observables χ in $\hat{G}$ that "vanish" on H, i.e. that satisfy $\chi(h) = 1$ for every $h \in H$. This one-to-one correspondence between "varieties" in G and families of elementary observables in $\hat{G}$ is contravariant (or inclusion-reversing). Indeed, $(H')^{\perp} \subset H^{\perp}$ if $H' \supset H$. The bigger the "variety" H' in G, the smaller the family $(H')^{\perp}$ of elementary observables that satisfy the compatibility condition of "vanishing" on it. Conversely, the bigger the family $H^{\perp}$ of elementary observables in $\hat{G}$, the smaller the variety in G that contains the solutions of the system of equations $\{\chi(g) = 1\}_{\chi \in H^{\perp}}$. In Galoisian terms, we could say that a single elementary observable χ_0 in $\hat{G}$ just "discerns" the "variety" of states $g \in G$ satisfying $\chi_0(g) = 1$. But the observable χ_0 cannot "separate" the different points in such a "variety". Conversely, a single state g_0 in G just "discerns" the family of observables χ in $\hat{G}$ such that $\chi(g_0) = 1$. But the state g_0 cannot "discern" any single observable within such a family. This language provides a straightforward interpretation of equation (2): the whole group $\hat{G}$ of elementary observables on G modulo the family $H^{\perp}$

[5]The isomorphism is given by $\chi \in H^{\perp} \mapsto \widetilde{\chi} \in \widehat{G/H}$ such that $\widetilde{\chi}([g]) = \chi(g)$.

[6]Using (3), we have that $\chi(g) = 1$ for all $\chi \in H^{\perp}$ iff $\bar{\chi}([g]) = 1$ for all $\bar{\chi} \in \widehat{G/H}$. Now this is the case iff $[g] = 1$ in G/H, that is if $g \in H$.

of elementary observables that "vanish" on the "variety" H, yields the group of elementary observables on the "variety" H, that is $\hat{H}$.

4. The Galoisian abelian states as squeezed coherent states

Given a finite abelian group G, we can derive the standard notions of a finite version of quantum mechanics as follows. Firstly, one can prove that for every finite abelian group G of cardinal n, there exists a finite Galois extension $(L:K)$ (with $\mathbb{Q}\subseteq K\subseteq L\subseteq\mathbb{C}$) that satisfies the following conditions: (i) $G\cong Gal(L:K)$, (ii) $\mu_n(\mathbb{C})\subseteq K$, (iii) L is stable by complex conjugation, and (iv) $\sqrt{n}\in K$.[7] Condition (i) tells that every finite abelian group G can be interpreted as the Galois group of a Galois extension (inverse Galois problem). Condition (ii) guarantees (as we have explained in the previous section) that the Galois-Grothendieck duality between K-algebras split by L and G-sets can be recasted as a Pontryagin duality between G and its unitary dual $\hat{G}$. Condition (iii) permits to define a kind "Hilbert space structure" on L^G by means of a Hermitian product. Finally, condition (iv) is used to define a discrete version of the Fourier transforms. In what follows a (finite and abelian) Galois extension satisfying these conditions is called a *Galois quantum extension*.

Given a Galois quantum extension, we interpret the group algebra $L[G]$ as the algebra of superposed quantum states (by duality, we could have also chosen $L[\hat{G}]$). Each superposed state $\psi=\sum_{g\in G}\psi(g)g$ defines a wave function $\psi(g)\in L^G$. The group algebra $L[G]$ can be endowed with the L-valued Hermitian form $<\psi_1,\psi_2>\doteq\frac{1}{n}\sum_{g\in G}\psi_1(g)\overline{\psi_2(g)}$, where the bar denotes complex conjugation. Given a state $\psi\in L[G]$, the Fourier isomorphism $L[G]\simeq L^{\hat{G}}$ yields a wave function $\hat{\psi}(\chi)$ on $\hat{G}$. In turn, this wave function defines the vector state $\hat{\psi}=\sum_{\chi\in\hat{G}}\hat{\psi}(\chi)\chi\in L[\hat{G}]$. In particular, we can consider the superposed state $\psi_H=\sum_{g\in H}g\in L[G]$ defined by the indicator wave function $\psi_H(g)$ of H in G. It can be shown that the Fourier transform of this state is $\lambda_H\varphi_{H^\perp}(\chi)$, where $\lambda_H=\frac{Card(H)}{n}$ and $\varphi_{H^\perp}(\chi)$ is the indicator wave function of $H^\perp$ in $\hat{G}$. In turn, the wave function $\lambda_H\varphi_{H^\perp}(\chi)$ defines the state $\widehat{\psi_H}=\lambda_H\sum_{\chi\in H^\perp}\chi\in L[\hat{G}]$. In what follows, the cardinal of the support in G of the state ψ_H is denoted $\Delta\psi_H$ (and analogously for $\widehat{\psi_H}$). Now, H is the support of the state ψ_H in G and $H^\perp$ is the support of the state $\widehat{\psi_H}=\lambda_H\varphi_{H^\perp}$ in $\hat{G}$. Then, $\Delta\psi_H=Card(H)$ and $\Delta\widehat{\psi_H}=Card(H^\perp)=Card(G/H)$. Therefore, the Galois indiscernibility principle can be rewritten as follows:

$$\Delta\psi_H\Delta\widehat{\psi_H}=n, \tag{4}$$

where $n=Card(G)$. It is worth noting that this principle can be understood as a manifestation of the geometry-algebra duality between "subvarieties" in G and the families of observables (induced by the characters in $\hat{G}$) that "vanish" on them. Indeed, the H-automorphic state $\psi_H=\sum_{g\in H}g\in L[G]$ can be understood (as we have explained in the previous section) as the "subvariety" of G defined by the family of equations $\{\chi(g)=1\}_{\chi\in H^\perp}$. Hence, the state ψ_H can be alternatively described in terms of the minimal family of observables that discern the subgroup $H\subset G$ that supports ψ_H, namely the observables defined by the characters in $H^\perp$. Briefly, the state ψ_H can be described in the "momentum" representation $\hat{G}$ by means of its Fourier transform, i.e. by the state $\widehat{\psi_H}$ supported by $H^\perp$.[8] If the support H of ψ_H is minimal (i.e. if $H=1_G$), then we need the observables defined by *all* the characters in $\hat{G}$ to discern ψ_H (i.e. $H^\perp=\hat{G}$). Briefly, if the indetermination in G is minimal ($\Delta\psi_H=1$), the indetermination in $\hat{G}$ is maximal ($\Delta\widehat{\psi_H}=n$), and viceversa.

We shall now argue that the indicator wave functions that we have just described are the discrete analogs (as minimizers of the indeterminacy relation) of the Gaussian distributions of the quantum theory over the phase space $\mathbb{R}^2$. To do so, we shall use the notion of *entropic indeterminacy* associated

[7]These conditions are a combination of classical results for the abelian inverse Galois problem, the cyclotomic extensions and the classical Galois theory (see Ref.[12], pp. 266-268).

[8]In Ref.[13], Majid proposes a similar analysis of the "Fourier-Pontryagin duality" between a structure and the family of "representations" that we need in order to reconstruct it.

to the Shannon entropy [17].[9] In the continuous case of a LCA group G equipped with its Haar measure $d\mu$, the entropy of a function $f \in L^2(G, \mathbb{C})$, is defined by the expression

$$H(f) \doteq -\int_{g\in G} \mid f(g) \mid^2 ln \mid f(g) \mid^2 d\mu. \tag{5}$$

If the function is completely localized, the entropy is minimal. This means that the information content of the state is maximal, in the sense that it singles out a well-defined point of the G-configuration space. On the contrary, a state that is completely delocalized in G has a maximal entropy, which means that its information content is minimal. It can be proved that for any LCA group G, there is an integer m and a LCA group G_c that contains an open compact subgroup, such that $G \cong \mathbb{R}^m \times G_c$. For $f \in L^2(G, \mathbb{C})$ such that $f, \widehat{f} \in (G, \mathbb{C})$ and $\parallel f \parallel = 1$, the corresponding indeterminacy principle reads [15]

$$H(f) + H(\widehat{f}) \geq m(1 - ln(2)). \tag{6}$$

In the continuous case (i.e. if $G = \mathbb{R}^m$) this expression entails the standard Heisenberg indeterminacy relation.[10] In the 1-dimensional case, expression (6) yields $\Delta q \Delta p \geq \frac{\hbar}{2}$. If $G = G_c$ is finite of cardinal n and $m = 0$, expresion (6) yields

$$H(f) + H(\widehat{f}) \geq 0.$$

For $f \neq 0$, this expression implies the Donoho-Stark indeterminacy principle [9]:

$$\Delta(f)\Delta(\widehat{f}) \geq n, \tag{7}$$

where $\Delta(f) \doteq Card(Supp(f))$. Now, expression (4) is a particular case of (7).

In (6), the equality is reached for functions $f = \varphi_{Gau} \otimes \widetilde{\psi_H}$ on $\mathbb{R}^m \times G_c$ (up to the action of the Heisenberg group) that are combinations of a normalized Gaussian $\varphi_{Gau} = Ce^{-Q(\overrightarrow{x})}$ on $\mathbb{R}^m$ (where Q is a positive definite quadratic form on $\mathbb{R}^m$) and a normalized indicator function $\widetilde{\psi_H}$ of a subgroup $H \subset G_c$. In the continuous case, the minima is reached by the normalized Gaussian function φ_{Gau}. This means that the Gaussian distributions are the wave packets that minimize the usual Heisenberg indeterminacy relations, i.e. such that $\Delta q \Delta p = \frac{\hbar}{2}$. In the case of the discrete Donoho-Stark principle, the minima is reached by the normalized indicator functions $\widetilde{\psi_H} = \sqrt{\frac{Card(G)}{Card(H)}}\psi_H$ of subgroups $H \subset G_c$. Hence, the indicator functions (like the wave functions that define the Galoisian quantum states ψ_H satisfying (4)) can indeed be interpreted as the discrete version of the Gaussian functions, that is of the so-called *squeezed coherent states*.

5. Conclusion

We have interpreted the Galois-Grothendieck theory as a formalization of the correspondence between G-spaces parameterizing states endowed with non-trivial groups of automorphisms $H \subset G$ and the H-compatible observables that can be consistently valuated on such states. This duality between H-automorphic states and H-compatible observables entails (what we have called in Ref.[7]) a *Galois indiscernibility principle*: the larger the automorphism group H of a state, the smaller the H-compatible observable algebra that discerns the state (and viceversa). In order to argue that these Galoisian ideas can be used to understand the rationale behind Heisenberg indeterminacy principle, we have defined a *Galois quantum theory* on a finite homogeneous $Gal(L:K)$-configuration space $Spec_K(L) \simeq G$, where $(L:K)$ is a finite abelian Galois extension. We have shown that in this restricted framework the Galois indeterminacy principle does coincide with the Heisenberg indeterminacy principle formulated in terms of the notion of *entropic indeterminacy*. It remains to analyze to what extent this Galoisian interpretation

[9]Some authors argue that the notion of *entropic indeterminacy* encodes the quantum indeterminacy in a more efficient way than the standard deviations Δx and Δp (see Ref.[2]).

[10]In the continuous case, the unitary dual of $G = \mathbb{R}^m$ is $\widehat{G} \cong \mathbb{R}^m$. A particular value of the "momentum" $\chi \in \widehat{G}$ defines the elementary observable on G given by $\tilde{\chi} : g \mapsto e^{i\chi \cdot g}$. The discrete case is very similar. The unitary dual of $G = \mathbb{Z}/n\mathbb{Z}$ is given by $\widehat{G} = \mathbb{Z}/n\mathbb{Z}$. A particular value of the "momentum" $\chi \in \widehat{G}$ defines the elementary observable on G given by $\tilde{\chi} : g \mapsto e^{\frac{2i\pi\chi \cdot g}{n}}$.

of Heisenberg indeterminacy principle can be extended to more general quantum theories, such as for instance the quantum theory over the phase space $\mathbb{R}^{2n}$.

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, Mathieu Anel, and Alexandre Afgoustidis for helpful discussions.

References

1. Bennequin, D.: Questions de physique galoisienne, in M. Porte (eds), Passion des Formes, à René Thom. Éditions Fontenay - Saint Cloud, Fontenay - Saint Cloud, 311-410 (1994).
2. Bialynicki-Birula, L.: Entropic uncertainty relations in quantum mechanics, in Quantum Probability and Applications. Eds. L. Accardi and W. von Waldenfels, Lecture Notes in Mathematics 1136, Springer, Berlin (1984).
3. Borceux, F. and Janelidze, G.: Galois theories. Cambridge University Press, Cambridge (2001).
4. Catren, G.: Quantum Foundations in the Light of Gauge Theories, to appear in C. de Ronde, S. Aerts and D. Aerts (eds.), Probing the Meaning of Quantum Mechanics: Physical, Philosophical, and Logical Perspectives, World Scientific (2014).
5. Catren, G.: Can Classical Description of Physical Reality be Considered Complete?, in Constituting Objectivity: Transcendental Approaches of Modern Physics. M. Bitbol, P. Kerszberg and J. Petitot (eds.), Paris (2009).
6. Catren, G.: On Classical and Quantum Objectivity. Foundations of Physics, doi:10.1007/s10701-008-9216-2 (2008).
7. Catren, G. and Page, J.: On the notion of symmetry in the light of Galois-Grothendieck Theory, submitted (2013).
8. Da Costa, N.C.A. and Rodrigues, A.A.M.: Definability and Invariance. Studia Logica: An International Journal for Symbolic Logic, Vol. 86, No. 1, 1-30 (2007).
9. Donoho D. L., & Stark P. B.: Uncertainty principles and signal recovery. SIAM, Journal on Applied Mathematics, 49(3), 906-931 (1989).
10. French, S. & Krause, D.: Identity in Physics: A Historical, Philosophical, and Formal Analysis. Oxford University Press, Oxford (2006).
11. Grothendieck, A.: Revêtements étales et groupe fondamental, SGA1. Lecture Notes in Math. 224, Springer-Verlag, Berlin New-York (1971).
12. Lang S.: Algebra. Springer, New-York (2005).
13. Majid, S.: Principle of Representation-Theoretic Self-Duality. Physics Essays, volume 4, number 3, 395-405 (1991).
14. Majid, S.: Foundations of Quantum Group Theory. Cambridge University Press, Cambridge (1995).
15. Özaydin, M. & Przebinda, T.: An entropy-based uncertainty principle for a locally compact abelian group. Journal of Functional Analysis, Volume 215, issue 1, 241-252 (2004).
16. Perelomov, A.: Generalized Coherent States and Their Applications. Spinger-Verlag, Berlin New-York (1986).
17. Shannon, B.E.: A mathematical theory of communication. The Bell System Technical Journal, Vol XXVII, numero 3 (1948).
18. Spekkens, R.: Evidence for the epistemic view of quantum states: A toy theory. Phys. Rev. A 75, 032110 (2007).
19. Sudarshan, E.C.G.: Uncertainty relations, zero-point energy and the linear canonical group. Paper presented at the Second International Workshop on Squeezed States and Uncertainty Relations at the Lebedev Institute, Moscow (1992).
20. Szamuely T.: Galois Groups and Fundamental Groups. Cambridge Studies in Advanced Mathematics, vol. 117, Cambridge University Press, Cambridge (2009).