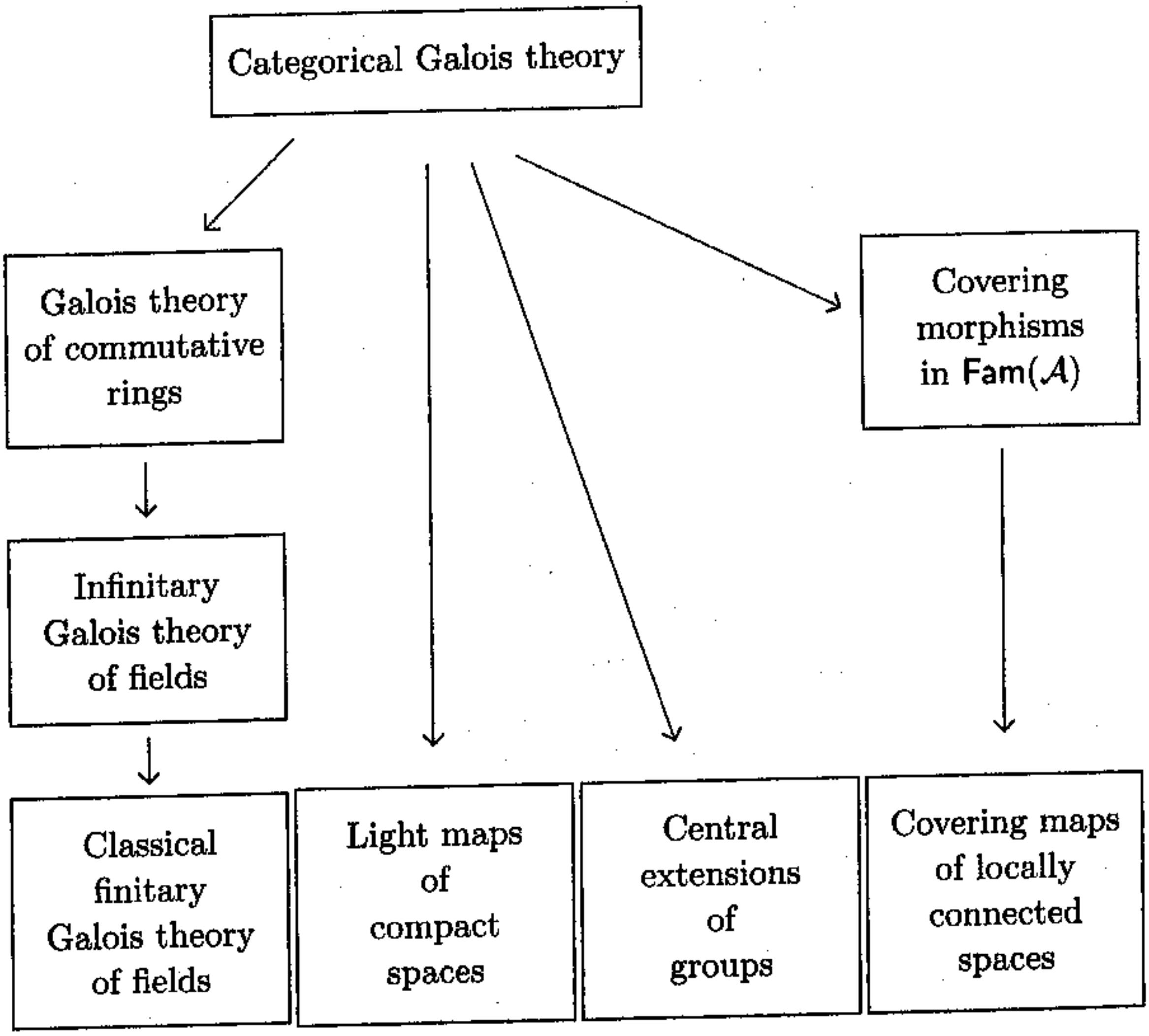

Scheme 2: Levels of generality in Galois theory

[48] and the categorical Galois theory, has nothing to do with [62] (which is related to [22]), but provides an approach to the Tannaka duality different from, for example, P. Deligne [26]. On the other hand [26] itself is in some sense similar to [57].

A.2 Back to the classical Galois theory

Excluding the "non-galoisian" situations studied in chapter 7, scheme 2 on this page presents roughly the levels of generality in Galois theory considered in this book so far.

In this section we will explain that the classical Galois theory is a special case of the theory of covering morphisms in $\mathsf{FinFam}(\mathcal{A})$, which is the obvious finite version of $\mathsf{Fam}(\mathcal{A})$. The important conclusion is that the classical theories of separable algebras and covering maps are much

Three Lectures on Galois Theory

Jean-Jacques Szczeciniarz

Content:

Classical Galois Theory and Some Generalizations

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

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

The essential question was to find the roots of a polynomial. But we can also ask what is the meaning of the search for the roots. This means to set up all possible links between the indeterminates. There exists in the substance of a polynomial some power of exploration which is situed in the relation between the coefficients (that are known) and some symmetrical links between the unknowns (X in polynomial P(X)).

An essential element of this theory is the field extension. That means that an extension of a set of elements provided with the field structure in a greater set, so that one can dispose roots of a polynomial, which was not in the basic field.

But there exists another way to work on the roots and on the links between these roots.

Definition:

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

Important proposition

Let $K \subseteq L$ be an algebraic field extension. Then every K-endomorphism of L is necessarily an automorphism.

We shall denote $Aut_K(L)$ the group of K-automorphism of L. This structure allows us to work specifically on the links between the roots.
This analysis of the links between the roots becomes an analysis of the links between the elements of the field extension.
Now return to the polynomial and recall the following two important notions.

Definition:

A field extension $K \subseteq L$ is called *separable* when
i) the extension is algebraic
ii) all the roots of the minimal polynomial of every $l \in L$ are simple.
The concept of separability allows us to suppose the existence of a structure by which the polynomial gets decomposed into simple elements.

Definition:

A field extension $K \subseteq L$ is called *normal* when:
i) the extension is algebraic
ii) for every element $l \in L$ the minimal polynomial of l over K factors entirely in $L[X]$ into polynomials of degree 1.
Every polynomial that has at least one zero in L, splits in L. There is a close connection between normal extensions and splitting fields, which provides a wide range of normal extensions. I recall the definition of a splitting field : a polynomial $p(X) \in K[X]$ *splits* in $L[X]$ when it can be expressed as a product of linear factors over L.

Definition:

A field extension $K \subseteq L$ is called a *Galois extension* when it is normal and separable. The group of K-automorphisms of L is called the *Galois group* of this extension and is denoted by $Gal[L : K]$.

I would like to make some remarks on the notion of Galois extension. Normality and separability are complementary properties. From a philosophical point of view Galois extension sets up a place for roots of a given polynomial and also provides a possibility of linking each root with any other by a set of relations that form a group (of automorphisms). We get a set of roots and a block of roots with a set of their mutual links. That means that :
(1) we assume a structure of field extension, in which all roots are given;
(2) roots are presented by their relations. In a certain sense a field extension given by adjunction of a root pulls the set of all other roots with their mutual relations. In order to solve a polynomial equation one needs a new "place", which is given by a field extension. Such an extension is of "operational" character.

Galois correspondence

Given an intermediate field extension $K \subseteq M \subseteq L$ consider the Galois group $Gal[L : M] = Aut_M(L)$ of those automorphisms of L that fix M. Given a subgroup $G \subseteq Gal[L : K]$ denote $Fix(G) = \{l \in L | \forall g \in G; g(l) = l\}$; $Fix(G)$ is a subfield of L.

The great idea and the thesis of Galois theory is to consider elements fixed by Galois group. It is a way to focus on the set of roots and, more precisely, to select some block of roots. Making an extension (normal and separable) means a "local" introduction of set of roots. Adjunction of roots (it is a field extension) allows one to disregard the fixed basic field and make permutations of the new adjoint roots.

Definition:

A Galois connection between two posets A, B consists in two order reversing maps
$f : A \longrightarrow B,\ g : B \longrightarrow A$
$a \leq g(f(a)),\ b \leq f(g(b))$
$\forall a \in A, \forall b \in B$
Viewing A and B as categories and f, g as contravarinat functors this is just the usual definition of adjoint functors.

Proposition:

Let K, L be fixed and consider a Galois field extension of the form $K \subseteq M \subseteq L$. Maps
$\{M|K \subseteq M \subseteq L\} \longrightarrow \{G|G \subseteq Gal[L:K]\}$
and
$\{M|K \subseteq M \subseteq L\} \longleftarrow Fix(\{G|G \subseteq Gal[L:M]\})$
constitute a Galois connection.
$Fix(Gal(M)) = M \subseteq Fix(Gal[L:M])$.
Indeed,
$G \subseteq Gal(Fix(G))$

Galois theorem

Let $[K : L]$ be a finite dimensional Galois extension. In this case, the adjunction is a contravariant isomorphism. Moreover, for every intermediate field extension $K \subseteq M \subseteq L$ we have
$dim[L : M] = card(Gal[L : M])$

Algebra on a field

An algebra A on a field K is a vector space on K provided with a multiplication that makes it into a ring and that satisfies $k(aa') = (ka)a'$, for all a, a' in A. The idea is to generalize the Galois theory, which was initially developed for field extensions, to a more general case of K-algebras .

Proposition

Let K be a field and $p(X)$ be a polynomial. Then the following conditions are equivalent:
(i) $p(X)$ is irreducible;
(ii)ideal $\langle p(X) \rangle$ generated by $p(X)$ is maximal;
(iii) K-algebra $K[X]/p(X)$ is a field.
The structure of algebra allows one to extend the operation of vector space that gives one back the field structure.

I want to make some remarks on the role played by the polynomials. Galois' original intention was to treat the problem of solving polynomial equations by studying coefficients of a polynomial. These coefficients belong to the basic field. When we work in an extension field we act *upon* the roots. In this case we dispose of the whole permutation group $Aut_K(L)$ that we can apply to the roots. That shows that in order to find roots of a given polynomial one needs an extension of the basic field. The polynomial formulation of Galois theory brings this theory into a structural setting. The irreductibility property allows one to present $K[X]/\langle p(X)\rangle$ as a field.

When we consider a maximal ideal $\langle p(X) \rangle$ its maximality implies that the quotient $K[X]/\langle p(X) \rangle$ is a field.
And this quotient gives one an extension of $K(a)$ with a root of the polynomial.

The formulation in terms of algebra is the following.
Let K be a field, A be a K-algebra, $0 \neq a \in A$ be an algebraic element with the minimal polynomial $p(X)$ of degree n. The K-subalgebra $K(a) \subseteq A$ generated by a is isomorphic to $K(a) \cong \frac{K[X]}{\langle p(X) \rangle} \cong \{k_0 + k_1 X + \ldots k_{n-1} X^{n-1} \mid k_i \in K\}$
The properties of the K-algebra allow one to dispose of a supplementary structure besides the field structure. A problem concerning the notion of field extension was to find the best structure allowing for "horizontal" extensions. Like fields algebras allow for splitting. Splitting is a way to obtain all simple roots of a given polynomial. Given an algebra one can restrict and extend scalars.

Let $K \subseteq L$ be a field extension. Every L-algebra B is trivially a K-algebra by restriction of the scalar multiplication to the elements of K. On the other hand every K-algebra A yields an L-algebra $L \bigotimes_K A$ where the algebra multiplication is determined by
$(l \otimes a)(l' \otimes a') = (ll' \otimes aa')$
and the scalar multiplication is given by
$l(l' \otimes a) = (ll') \otimes (aa')$
for all $l, l' \in L$ and $a, a' \in A$

These constructions extend to functors
$L - Alg \longrightarrow K - Alg, B \to B'$
$K - Alg \longrightarrow L - Alg, A \to L \bigotimes_K A$
The latter functor is the left adjoint of the former.
We observe that the extension of scalars is made through the tensor product. Algebra gives a better vision of the decomposed polynomial and of the scalar extension. It gives a way to enlarge a polynomial structure independently of unknowns. This new introduction of algebra reflects the spirit of Galois' idea; it enlarges what I would like to call an observational structure of roots.

Two propositions

Proposition 1:
Let $K \subseteq L$ be a field extension and A be a K-algebra. Then the following isomorphism holds:
$Hom_K(A, L) \cong Hom_L(L \bigotimes_K A, L)$
Proposition 2:
Let $K \subseteq L$ be a field extension and $p(X) \in K[X]$ a polynomial. Then the following isomorphim holds
$L \bigotimes_K \frac{K[X]}{\langle p(X) \rangle} \cong \frac{L[X]}{\langle p(X) \rangle}$
On the right side the polynomial is viewed as a polynomial with coefficients in L.

Split algebra

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

Definition:

Let $K \subseteq L$ be a field extension and Abe a K-algebra . The extension L splits the K-algebra A when
(i) A is algebraic over K
(ii) the minimal polynomial $p(X) \in K[X]$ of every element of A factors in $L[X]$ into factors of degree 1 with distinct roots.
The K-algebra A is called an *étale* K-algebra when it is split by the algebraic closure of K.
Recall that an algebra A on a field K is a vector space provided with a multiplication, which makes it into a ring and which satisfies $k(aa') = (ka)a'$ for all elements $k \in K$, $a, a' \in A$.

Theorem

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

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

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

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

$l \otimes a \rightarrow (f(l \otimes a))$ where $f \in Hom_L(L \bigotimes_K A, L)$

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

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

$l \otimes a \rightarrow (lg(a))$; where $g \in Hom_K(A, L)$

Theorem (continued)

(iv) $\sharp Hom_L(L \bigotimes_K, L) = n$
(v) $\sharp Hom_K(A, L) = n$
(vi)$L \bigotimes_K A$ is isomorphic to L^n as an L-algebra
(vii)$\forall x \in L \bigotimes_K A, x \neq 0, \exists f \in Hom_L(L \bigotimes_K A, L)$ such that $f(x) \neq 0$

Theorem (continued)

There are various relatively simple proofs of this theorem. I prefer to begin with a comment on (iv) and then explain the idea of Gelfand transformation.

The theorem provides for a sort of translation of the structural situation of Galois theory into the terms of Grothendieck' interpretation of this theory.

This theorem is essential for understanding the notion of Galois correspondence. The tensor product is related to the set of maps from the product in the basic field into this basic field. We deal here with a twofold duality.

The tensor product makes an A-algebra K into a L-algebra. It gives a way to preserve the algebra structure through its extension.

Now we can present the second Galois generalization.

Recall

Let me recall that given a group G whose composition law is written multiplicatively , a left G-set is a set X provided with a left action of G $G \times X \to X$, $(g, x) \to gx$

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

A morphism

$f : X \to Y$ of left G-sets respects the action of G, that is, $f(gx) = g(f(x))$.

Galois theorem

Let $K \subseteq L$ be a finite dimensional Galois extension of fields. Let us write $Gal[L : K]$ for the group of K-automorphisms of L and $Gal[L : K] - Set_f$ for the category of finite $Gal[L : K]$ - sets . Let us also write $Split_K(L)_f$ for the category of those finite dimensional K-algebras which are split by L. The functor on $Split_K(L)_f$, represented by L, factors through the category $Gal[L : K] - Set_f$:
$Hom_K(-, L) : Split_K(L)_f \longrightarrow Gal[L : K] - Set_f$
$A \rightarrow Hom_K(A, L)$
with $Gal[L : K]$ acting by composition on $Hom_K(L)$. This factorization functor is a contravariant equivalence of categories. In the last part of this talk I shall explain the meaning of this theorem.

I have presented you some results of the generalization of Galois theory through the Category theory. This generalization is made in the Grothendieck spirit but without the Scheme theory.
Our starting point is the category $Split_K(L)$. We use the concept of algebra which extends the operational possibilities of the field, and among these algebras we consider those that are split by L.
We begin with a category of split algebras, which provides a decomposition of polynomials. A split algebra can be extended and put in correspondence with double-maps through the Gelfand transform. An essential feature of this structure is the fact that it maintains so called object extensions and morphism extensions.

The Galois theorem says that there exists a functor, which is a sort of translator from one category to another, a map specifically adapted for categories. The Galois correspondence is functorial in the sense that it goes from the category of fields to the category of groups. Now we have a category of algebras, which replaces a category of fields.

What is important is the fact that this functor $Hom_K(-, L)$ factors through the category $Gal[L : K] - Set_f$. We see here a Galois group playing a new role: it determines an action on a set, and thus turns itself into a G-set. Since the functor $Hom_K(-, L)$ is representable it determines the given Galois-group-set
$Gal[L : K] \times Hom_K(A, L) \rightarrow Hom_K(A, L)$
$(f, g) \rightarrow g \circ f$

Epistemological and philosophical remarks

The above theorem shows two possible ways of generalizing the classical Galois theory. First, one generalizes this theory through the category $Split_K(L)$. Second, one generalizes it through the functor $Hom_K(-, L)$. It turns out that all properties of split algebras can be translated into the language of functors. Such a translation involves the category of G-sets with G equal to $Gal[L : K]$. The analysis now aims at the decomposition of algebras through a Galoisian extension. This approach can be furhter applied to structures of other types.

Classical infinitary Galois theory

Proposition 1:
Let $K \subseteq L$ be a Galois extension of fields. Let $K \subseteq M \subseteq L$ be a finite dimensional intermediate Galois extension. The canonical restriction morphism
$p_M : Gal[L : K] \rightarrow Gal[M : K]$
$f \rightarrow f \mid_M$ is a topological quotient by the equivalence relation determined by the subgroup $Gal[L : K] \subseteq Gal[M : K]$.

Classical infinitary Galois theory

Proposition 2:
Let $K \subseteq L$ be a Galois extension of fields. For every finite dimensional intermediate extension $K \subseteq M \subseteq L$ the Galois group $Gal[L:M] = \{f \in Gal[L:K] \forall m \in M f(m) = m\}$ is an open and closed subgroup of $Gal[L:K]$

Theorem

Let $K \subseteq L$ be an arbitrary Galois extension of fields.
Correspondences
$K \subseteq M \subseteq L \to Gal[L : M]$
$G \subseteq Gal[L : M] \to Fix(G)$
induce a contravariant isomorphims between the lattice of arbitrary extensions $K \subseteq M \subseteq L$ and the lattice of closed subgroups $G \subseteq Gal[L : K]$.

Commentary

This theorem is a reformulation of the Galois correspondence in the framework of topology. The introduction of the topology allows one to treat an arbitrary extension.This new possibility has internal and external meaning.

I want to try to explain the significance of the construction of the new topology. The projection defined in the proposition induces a quotient and then the discrete topology in the quotient.

$Gal[L:M]$ is a closed subgroup. We know that the subgroups $Gal[L:M] \subseteq Gal[L:K]$ constitute a fundamental system of open and closed neighborhoods of Id_L.

Commentary (continued)

In the situation of the theorem we dispose the proposition $Id_L \in Gal[L : N] \subseteq Gal[L : M]$. This entails that $Gal[L : M]$ is an open and closed subgroup of $Gal[L : K]$.
It is worth to notice that we use elementary properties of topological groups. Every subgroup of a topological group containing an open subgroup is itself open, and every open subgroup is closed.
Inside the Galois correspondance it is useful to see that the group operation is translated into the language of topological maps that preserve the initial inclusions. The projective limit is a way to consider in general the groups variation. In addition to the refined preservation of the inclusive structure we get the construction of correspondence beyond its polynomial significance. That is the external meaning.

Commentary (continued)

Let us now consider some features of the proof of the above theorem. $Fix(G)$ is a field. Consider a closed subgroup $G \subseteq Gal[L:K]$. If $K \subseteq L$ is a Galois extension $Fix(G) \subseteq L$ is also a Galois extension. On the other hand we have $G \subseteq Gal[L:Fix(G)] \subseteq Gal[L:K]$. Since a subgroup of a Galois group of the automorphisms of the extended field on the field of the fixed elements by Gal is the same group, we have $G = Gal[L:K], K = Fix(G)$ and so $G = Gal[L:Fix(G)]$.
The inverse correspondence is obtained similarly.
Thus we dispose an arbitrary Galois extension of a given field. The intermediate subextensions are finitary and hence classical.

Infinitary Galois group

Here is another generalization: we will define the Galois group of an arbitrary Galois extension $K \subseteq L$. Such a group is a topological group, which is discrete when the extension is finite.
This latter generalization amounts to the introduction of topology; this topology allows one to treat the infinity.

Proposition

Let $K \subseteq L$ be a Galois extension of fields. In the category of groups, $Gal[L:K] = lim_M Gal[M:K]$ where M runs through the poset of finite dimensional Galois extensions $K \subseteq M \subseteq L$ and for $M \subseteq M'$, the corresponding morphism $Gal[M':K] \rightarrow Gal[M:K]$, $f \rightarrow f\mid_M$ is a restriction.
It is worth to notice that we introduce topology in the Galois extension by making this extension continue; thus we get a topological Galois group.

Definition

The topological Galois group of extension $K \subseteq L$ is the group $Gal[L : K]$ provided with the initial topology for all the propositions $Gal[L : K]?lim_M Gal[M : K] \to Gal[M : K]$, $f \to f\mid_M$ where M runs through the finite dimensional Galois subextensions $K \subseteq M \subseteq L$ and $Gal[M : K]$ is provided with the discrete topology. Such a topology can be obtained as follows.

Proposition

Let $K \subseteq L$ be a Galois extension of fields. The field L is the set - theoretical filtred union of the subextensions $K \subseteq M \subseteq L$ where $K \subseteq M$ is a finite dimensional Galois extension. The topological Galois group is thus a cofiltred projective limit in the category of topological groups of a diagram consituted of discrete finite groups : such a group is called a *profinite* group.

Commentary

We can observe how the topology introduced on one side ot the correspondence (field extension) is transferred to the other side (Galois group).
We need this transfer for preserving the Galois correspondence in the topological framework. It is a bit difficult to see what this topology is. Let me explain this.
On one side of the correspondence we have to go over all extensions continuously and find a topological structure for this continuous variation. The same should hold for the Galois groups.
What the gain consists in ?

Proposition

Let L be a Galois extension of fields. The subgroup $Gal[L:M] \subseteq Gal[L:K]$, for $K \subseteq M \subseteq L$, which is a finite dimensional Galois subextension, constitute a fundamental system of open and closed neighborhoods of Id_L.

Lemma

Let $K \subseteq L$ be a Galois extension of fields. The topology of the Galois group $Gal[L : K]$ is the initial topology for all maps $ev_l : Gal[L : K] \longrightarrow L;\ f \longrightarrow f(l)$ where l runs through L and the codomain L of ev_l is provided with the discrete topology.

Corollary

By analogy with the usual description of opens in Algebraic Geometry I give the following corollary.
Let $K \subseteq L$ be a Galois extension of fields. For every $f \in Gal[L : K]$, the subsets
$V_M(f) = \{g \in Gal[L : K] \mid g\mid_M = f\mid_M g\} \subseteq Gal[L : K]$
for $K \subseteq M \subseteq L$ running through the arbitrary finite dimensional subextensions constitute afundamental system of neighborhoods of f.

Definition

Let G be a topological group. A topological G-space is a topological space provided with a continuous action of G ; a morphism of topological space is a continuous morphism of G-sets. A topological G-space is profinite when it is a projective limit, indexed by a cofiltred poset, of finite discrete topological G-spaces. projective limits of topological spaces is computed as in the category of topological spaces, with the corresponding componentwise action of G.

Lemma

Let K be a field . Every algebraic K-algebra A is the set-theoretical filtred union of its finite dimensional subalgebras.

Lemma

Let $K \subseteq L$ be an arbitrary Galois extension of fields. For every K-algebra A which is split by L, there is a bijection
$Hom_K(A, L) \cong lim_B Hom_K(B, L)$
where the limit is cofiltred and indexed by the finite dimensional subalgebras $B \subseteq A$.
Moreover each $Hom_K(B, L)$ is finite; so the above limit provides $Hom_K(A, L)$ with the structure of profinite space.

Lemma

Let $K \subseteq Lbe$ an arbitrary Galois extension of fields. For every K-algebra A which is split by L the map
$\mu : Gal[L : K] \times Hom_K(A, L) \to Hom_K(A, L)$;
$g, f \to g \circ f$
is a continuous action of the topological group $Gal[L : K]$ on the topological space $Hom_K(A, L)$ when these are proved with the profinite topologies inherited from the initial topology given above.

Lemma

Let $K \subseteq L$ be an arbitrary Galois extension of fields. Consider a homomorphism $f : A \longrightarrow B$ of K-algebras where A and B are split by L. The map $\Gamma(f) : Hom_K(B, L) \longrightarrow Hom_K(A, L)$ is a continnuous homomorphism of $Gal[L : K]$-sets when $Hom_K(B, L)$ and $Hom_K(A, L)$ are provided with the profinite topology.

Lemma

Let K be a field and A be an algebraic K-algebra. Let us write $A = colimB$ where B runs through the finite dimensional subalgebras of A. For every finite dimensional K-algebra C the canonical morphism $\mu : colim_B Hom_K(C, B) \to Hom_K(C, B)$ is bijective.

Lemma

Let $G = lim_{i \in I)} G_i$ be a profinite group , expressed as a cofiltred projective limit of finite discrete groups . Let us assume that the projections $p_i : G \to G_i$ are surjective. Denote $G_i - Set_f$ the category of finite G_i-sets and $G - Top_f$ the category of dicrete finite topological G-spaces. For every index $i \in I$ there is a functor
$\gamma i : G_i - Set_f \to G - Top_f; X \to X$
The G-action is given by $gx = p_i(g)x$ This functor identifies $G_i - Set_f$ with a full subcategory of $G - Top_f$. Moreover the category $G - Top_f$ is the set theoretical filtred union of the full subcategories $G_i - Set_f$.

Theorem

Let $K \subseteq L$ be an arbitrary Galois extension of fields, $Split_K(L)$ be the category of K-algebras-splits by L, and $Gal[L : K] - Prof$ be the category of profinite $Gal[L : K]$-spaces. Then the functor $\Gamma : Split_K(L) \to Gal[L : K] - Prof;\ A \to Hom_K(A, L)$ is a contravariant equivalence of categories.

Commentary

The latter theorem is similar to the Grothendieck Galois theorem. It is an infinitary generalization.
The proof uses properties of a functor, which defines an equivalence. I give here only some descriptive comments on this theorem.

Comment (continued)

First of all it is important to dispose of the category *Split* and the K-algebras which are split by the field L. It expresses the possibility of splitting extension. We know by the first Grotendieck Galois theorem that this splitting property corresponds to the G-action, where G is the Galois group for the extension under consideration. It is also important to prove that this action holds for the profinite spaces (which are topological spaces of a certain kind). So we get, first, the advantage of working in a topological framework and, second, the advantage of the Grotendieck's category-theoretic generalisation.

Comment (continued)

Galois groups are automorphism groups of a given extension. It can be developed in various frameworks. In particular, the classical theory of coverings maps of locally connected topological spaces can be described as a Galois theory.
By examining the above four Galois theorems we can specify a form of mathematical activity that consists in running through one domain in order to get into another domain. Here we have a passage from fields to groups and also a topological passage from the act of extending to the act of controlling this extnesion.
(It should be possible to see the theory of the integral transform as a Galois theory (Abel-Radon- Norguet- Penrose transform)).