Journal of Pure and Applied Algebra 19 (1980) 21–42

ABSTRACT GALOIS THEORY

Michael BARR
Department of Mathematics, McGill University, Montreal, Quebec, Canada

Introduction

This paper arose after several discussions with D.K. Harrison on the possibility of applying the methods which I had developed to describe a certain class of toposes — the finite atomic toposes of Section 7.A below — to an exposition of the Galois theory of commutative algebras as well to some closely related theories. It is indeed possible, and the required theory is developed here.

I presented the earlier work on finite atomic toposes — now absorbed into this one — in a series of lectures at the University of Chicago in the Spring of 1979. Saunders even managed to come to some of the lectures; he sandwiched them in between meetings of the American Philosophical Society in Philadelphia and the National Science Board in Washington.

I would like to give thanks to the University of Chicago for inviting me there for a month as well as to the Département de l'Education du Québec and the National Science and Engineering Research Council for supporting this research.

1. Statement of results

This paper is concerned with a category $\mathscr{A}$ that satisfies some or all of the conditions listed below.

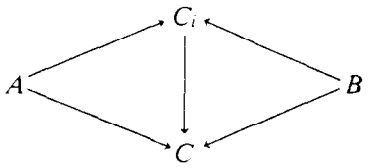
(1) (*Regular*) *monomorphism condition* ((R)MC). Every morphism in $\mathscr{A}$ is a (regular) monomorphism.

(2) *Amalgamation property* (AP). Every pair of morphisms $B \leftarrow A \rightarrow C$ can be put into a commutative square

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow \\ C & \longrightarrow & D. \end{array}$$

(3) *Uniformly bounded multisums* (UBM). For each object A there is a natural number $R(A)$ (which will always be assumed to be as small as possible so that in the

inequality below, equality is always attained at least once) with the property that for all B there are objects $C_1, \ldots, C_n$ and pairs of morphisms $A \to C_i \leftarrow B$ such that $n \leq R(A)$ and whenever $A \to C \leftarrow B$ there is a unique i and a unique $C_i \to C$ for which



commutes.

(4) *Initial object* (IO). There is an initial object 0.

(5) *Exactness condition* (EC). Every parallel pair $A \rightrightarrows B$ has an equalizer and coproducts in $\prod \mathscr{A}$ preserve them.

This last condition will be explained more fully in Section 2 below. For the present it is sufficient to think of $\mathscr{A}$ as the category of finite extensions of a field k in which case $\prod \mathscr{A}$ is the category of commutative semi-simple k-algebras, each is of which is a finite product of fields.

An object A of $\mathscr{A}$ is called normal if for any $A \overset{f}{\underset{g}{\rightrightarrows}} B$ there is an automorphism σ of A for which $f\sigma = g$. A map $f : A \to B$ is called a normal envelope of A if B is normal and every normal object that contains A contains B.

The main purpose of this paper is to prove:

Theorem 1. *Suppose $\mathscr{A}$ satisfies* MC, AP, UBM *and* IO. *Then every object of $\mathscr{A}$ has a normal envelope.*

Theorem 2. *Suppose $\mathscr{A}$ satisfies, in addition,* RMC *and* EC. *Then $\mathscr{A}^{\mathrm{op}}$ is equivalent to the category of transitive discrete G-sets for a uniquely determined profinite group G. (Conversely, such a category satisfies all these conditions.)*

In the process we will see how most of the elementary properties of the category of finite extensions of a field follow from these few properties. As well we will derive the finitary connected part of the theory of covering spaces of [7], the finitary part of the covering simplicial complexes of [8] and the Galois theory of connected commutative rings [2, 4] as applications.

2. The category $\prod \mathscr{A}$

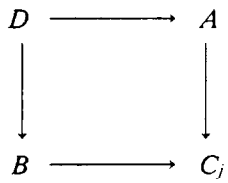
It will be our uniform hypothesis that $\mathscr{A}$ is a category satisfying MC, AP, UBM *and* IO.

The category $\prod \mathscr{A}$ has objects formal finite products of objects of $\mathscr{A}$. If $\prod_{i \in I} A_i$ and $\prod_{j \in J} B_j$ are two such formal products a map $\prod A_i \to \prod B_j$ is a J-indexed family

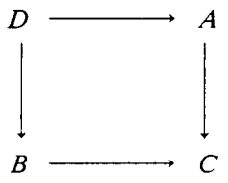
of maps $\prod A_i \to B_j$ which is clearly necessary if $\prod B_j$ is to be the product. A map $\prod A_i \to B$ is a composite $\prod A_i \to A_i \to B$ for one $i \in I$. The composition of these maps is obvious and gives a category, denoted $\prod \mathscr{A}$, which contains $\mathscr{A}$ as a full subcategory and for which each object is a finite product of objects of $\mathscr{A}$. $\prod \mathscr{A}$ may also be efficiently described as the opposite of the full subcategory of the functor category $\mathscr{S}^{\mathscr{A}}$ whose objects are finite sums of representable functors. A map $f : \prod_{i \in I} A_i \to \prod_{j \in J} B_j$ may be described as a pair (σ, φ) where $\sigma : J \to I$ and $\varphi : J \to \mathscr{A}$ are functions such that $\varphi j : A_{\sigma j} \to B_j$.

2.1. Proposition. *The category* $\prod \mathscr{A}$ *has finite colimits.*

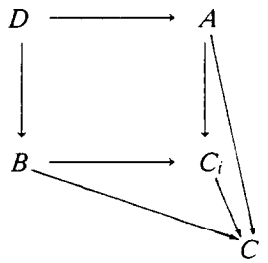
Proof. It is evident that the initial object remains initial. If $A \leftarrow D \to B$ are maps in $\mathscr{A}$, let $C_1, \ldots, C_n$ and $A \to C_i \leftarrow B$ be as in the definition of UBM. I claim that $\prod C_j$ where j ranges over all indices for which



commutes, is the pushout. If we have a commutative square

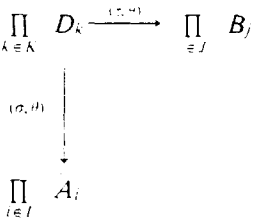


there is a unique i and unique map $C_i \to C$ for which the triangles in

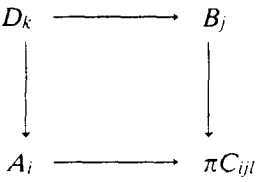


commute. Since the outer square commutes and $C_i \to C$ is mono, so does the inner square.

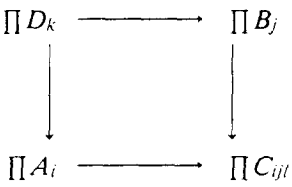
Next, given



For each pair of indices $i \in I$, $j \in J$ such that $\sigma i = \tau j = k$, let

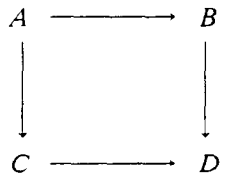


be a pushout, where $l \in L_{ij}$. Then



is easily seen to be a pushout, first with respect to objects of $\mathscr{A}$, then those of $\prod \mathscr{A}$.

Notation. If



is a pushout in $\prod \mathscr{A}$, write $D = B \otimes_A C$. If $A = 0$, then we write $B \otimes C$ for the sum.

2.2. Proposition. *If $\mathscr{A}$ satisfies* RMC *and has equalizers it has intersections.*

Proof. Given $A \to C \leftarrow B$, if $A \to C$ is the simultaneous equalizer of a set of pairs of maps $C \rightrightarrows D_i$, it is the equalizer in $\prod \mathscr{A}$ of the single pair $C \rightrightarrows C \otimes_A C$. This means that even in $\mathscr{A}$ it is the equalizer of a *finite* set of pairs of maps. The simultaneous equalizer of the set of pairs $B \to C \rightrightarrows D_i$ is easily seen to be the intersection of A and B.

2.3. Proposition. *Suppose $\mathscr{A}$ has intersections. Then $\prod\mathscr{A}$ has finite limits.*

Proof. Given

$$\prod A_i \underset{(\tau,\varphi)}{\overset{(\sigma,\theta)}{\rightrightarrows}} \prod B_j,$$

let

$$\begin{array}{ccc} C_j & \longrightarrow & A_{\sigma j} \\ \downarrow & & \downarrow \\ A_{\tau j} & \longrightarrow & B_j \end{array}$$

be a pullback (intersection). Then C_j is a subobject of $A_{\sigma j}$ and $A_{\tau j}$. For each index i, a finite number (perhaps none) of the subobjects of A_i thus appear. Let D_i be the intersection of all the subobjects of A_i which arise in this way. The empty intersection is of course A_i. Then

$$\prod D_i \to \prod A_i \rightrightarrows \prod B_j$$

is the equalizer.

2.4. Proposition. *Suppose $\mathscr{A}$ satisfies* RMC *and* EC. *Then $\prod\mathscr{A}$ has finite limits and for each A in $\prod\mathscr{A}$, $A\otimes -$ commutes with them.*

Proof. Begin with A in $\mathscr{A}$. If $B\to C$ is the equalizer of a single pair of maps $C\rightrightarrows D$,

$$A\otimes B\to A\otimes C\rightrightarrows A\otimes D$$

is also an equalizer by hypothesis. If $E\to C$ is another subobject $E\cap C$ is the equalizer of the two maps $E\rightrightarrows D$. Then

$$A\otimes(E\cap C)\to A\otimes E\rightrightarrows A\otimes D$$

is an equalizer. But $(A\otimes B)\cap(A\otimes E)$ is, by the same reasoning, the equalizer of $A\otimes E\rightrightarrows A\otimes D$ so they are equal. An obvious induction gives the same result when $B\to C$ is a finite composite of equalizers of pairs, which is the general case. Thus $A\otimes -$ commutes with intersections. It also commutes with products as it is immediate from the formal nature of products that $\prod A\otimes B_i$ has the universal mapping property of $A\otimes\prod B_i$. The way pullbacks are constructed out of products and intersections implies that $A\otimes -$ commutes with pullbacks. The terminal object 1 (empty $\prod$) is the domain of no map except its own identity from which $A\otimes 1 = 1$ is evident.

3. The factorization system

For generalities on factorizations, see [6]. We will construct here a class $\mathscr{E}$ of epis

and a class $\mathcal{M}$ of monos of $\prod \mathcal{A}$ such that every map in $\prod \mathcal{A}$ factors uniquely (up to isomorphism) as a map in $\mathcal{E}$ followed by one in $\mathcal{M}$. Moreover, $\mathcal{M}$ is stable under pushout. We say that $(\sigma, \theta) : \prod_{i\in I} A_i \to \prod_{j\in J} B_j$ is in $\mathcal{M}$ if $\sigma : J \to I$ is onto and is in $\mathcal{E}$ if σ is 1-1 and for each $j \in J$, θj is an isomorphism. It is clear that a map in $\mathcal{E}\cap\mathcal{M}$ is an isomorphism and conversely. To get the basic factorization, begin with (σ, θ) as above. Factor σ as $J \xrightarrow{\tau} K \xrightarrow{\varrho} I$ with τ onto and ϱ 1-1. Then we have

$$\prod_{i\in I} A_i \to \prod_{k\in K} A_{\varrho k} \to \prod_{j\in J} B_j$$

which is evidently a factorization of the required kind. The uniqueness is immediate. To see that $\mathcal{M}$ is stable under pushouts, consider

$$\begin{array}{ccc} \prod A_i & \xrightarrow{(\sigma,\theta)} & \prod B_j \\ {\scriptstyle (\tau,\varphi)}\downarrow & & \\ \prod C_k & & \end{array}$$

where $\sigma : J \to I$ is onto. For each k, let $j = \psi k$ be such that $\sigma j = \tau k$. Let

$$\begin{array}{ccc} A_{\sigma j} & \longrightarrow & B_j \\ \downarrow & & \downarrow \\ C_k & \longrightarrow & D_k \end{array}$$

be a commutative square whose existence is guaranteed by AP. The result is a commutative square

$$\begin{array}{ccc} \prod A_i & \longrightarrow & \prod B_j \\ \downarrow & & \downarrow \\ \prod C_k & \longrightarrow & \prod D_k \end{array}$$

in which the lower arrow belongs to $\mathcal{M}$. That the pullback also belongs to $\mathcal{M}$ is a consequence of the fact that when every map in $\mathcal{E}$ is epi, $\mathcal{M}$ is closed under left cancellation.

As usual we denote a map in $\mathcal{E}$ (resp. $\mathcal{M}$) by $\twoheadrightarrow$ (resp. $\rightarrowtail$).

4. Proof of Theorem 1

If A is an object of $\prod A$ and n a natural number, let nA denote the sum (tensor

product) of n copies of A. If $f_1, \ldots, f_n : A \to B$ there is induced a unique map $nA \to B$ whose restriction to the ith sum of nA is f_i.

4.1. Proposition. *Let A, B in $\mathscr{A}$ and $f_1, \ldots, f_m : A \to B$ be distinct. Then $m \leq R(A)$.*

Proof. Let $A \xleftarrow{p_i} C_i \xrightarrow{g_i} B$, $i = 1, \ldots, n$ be as in UBM. For each $j = 1, \ldots, m$ there is a unique i dependent on j and map $g_j : A \to C_i$ such that $p_i g_j = 1$ and $q_i g_j = f_j$. Since p_i is mono we can cancel on the left from $p_i q_j p_i = p_i$ to get $g_j p_i = 1$ so that p_i is an isomorphism, $g_j = p_i^{-1}$ and $f_j = q_i p_i^{-1}$. Thus the number of distinct maps $A \to B$ is exactly the number of C_i for which p_i is an isomorphism.

4.2. Corollary. *Every map $A \to A$ is an isomorphism.*

Proof. For $\mathrm{Hom}(A, A)$ is a finite monoid with left cancellation, hence a group.

It follows that the maps from A to B are in $1-1$ correspondence with the i for which $C_i \cong A$. Let $r(A)$ be the least integer such that for all B in $\mathscr{A}$, $\mathrm{Hom}(A, B)$ has $\leq r(A)$ elements. Being the least upper bound, it is of course attained. Suppose $m = r(A)$ and C is chosen in $\mathscr{A}$ for which there are m distinct maps

$$g_1, \ldots, g_m : A \to C.$$

There is induced a single map $g : mA \to C$ where, of course, mA is no longer an object of $\mathscr{A}$. This map has an $\mathscr{E}, \mathscr{M}$ factorization

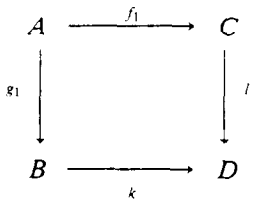
$$mA \xrightarrow{f} B \overset{h}{\rightarrowtail} C.$$

If the components of f are $f_1, \ldots, f_m$, then $hf_i = g_i$. The maps $g_1, \ldots, g_m$ are all distinct, so *a fortiori* are $f_1, \ldots, f_m$. Note that B belongs to $\mathscr{A}$ since a map in $\mathscr{M}$ cannot have more components in the domain than range.

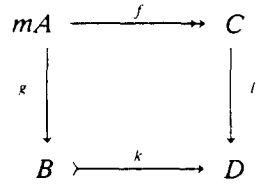
We are going to show that B is a normal envelope of A. Until that proof — which will demonstrate Theorem 1 — is finished let A and B be as above.

4.3. Proposition. *Suppose $g_1, \ldots, g_m : A \to C$ are distinct. Then there is a map $h : B \to C$ and a permutation σ of $2, \ldots, m$ such $g_1 = f_1 h$ and $g_{\sigma i} = f_i h$, $i = 2, \ldots, m$.*

Proof. Begin by finding a commutative square



Now observe that since k, l are mono, each of the sets of maps $lf_1, \ldots, lf_m$ and $kg_1, \ldots, kg_m$ are a set of $r(A)$ distinct maps $A \to D$. Since that is the largest possible number, the two sets must be permutations of each other. Thus there is a permutation σ of $1, \ldots, m$ with $lf_i = kg_{\sigma i}$, $i = 1, \ldots, m$. Since $lf_1 = kg_1$, $\sigma 1 = 1$. Finally since every morphism in $\mathscr{A}$ belongs to $\mathscr{U}$, we have

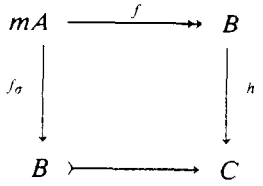


whose diagonal fill-in (see [6]) is the desired map.

4.4. Corollary. *For any i, j there is an $h : B \to B$ with $hf_i = f_j$.*

4.5. Proposition. *B is normal.*

Proof. Let $g, h : B \to C$. We want to find $k : B \to B$ such that $h = gk$. As above the sets $\{gf_i\}$ and $\{hf_i\}$ as permutations of each other so that there is a permutation σ of $1, \ldots, m$ such that $gf_{\sigma i} = hf_i$. Then the diagonal fill-in in



gives the required $k : B \to B$.

4.6. Proposition. *Let C be normal. Then $C \otimes C = \prod C$, a finite power of C.*

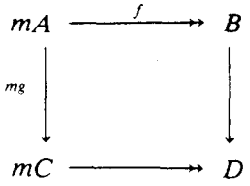
Proof. This is essentially the definition of normal. Form $\prod C$, indexed by $\mathrm{Hom}(C, C)$ and for $f : C \to C$ let $\langle f \rangle : \prod C \to C$ be the projection. Let $u, v : C \to \prod C$ by $\langle f \rangle u = 1$ and $\langle f \rangle v = f$. If $g, h : C \to D$ then from the definition of normal there is an $f : C \to C$ such that $g = hf$. Since h is mono, f is unique. Then $h\langle f \rangle : \prod C \to D$ is the unique map such that $h\langle f \rangle u = h$ and $h\langle f \rangle v = g$, thus showing that $\prod C$ has the universal mapping property of the sum.

4.7. Corollary. *Let C be normal. Then mC is a power of C for any finite m.*

Proof. This follows easily from the previous proposition and the distributivity of sums over products.

4.8. Corollary. *Suppose C is normal. If* $\mathrm{Hom}(A, C)$ *is non-empty, so is* $\mathrm{Hom}(B, C)$.

Proof. Let $g : A \to C$ and consider the pushout



in which the lower map is in $\mathscr{E}$ because the epi half of a factorization is always stable under pushout. It is clear from the definition of $\mathscr{E}$ that D can only be a power of C indexed by a subset of the index set. Since $B \to D$, there is some map $B \to C$.

4.9. Corollary. *Suppose C is normal. Then every map $A \to C$ extends to a map $B \to C$.*

Proof. The fact that there is a map $B \to C$ implies there are m maps $A \to C$ and (4.3) gives the conclusion.

This completes the proof of Theorem 1.

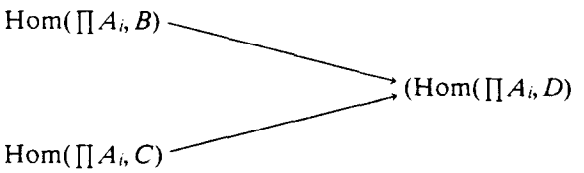
5. Proof of Theorem 2

We will prove Theorem 2 by showing that $(\prod \mathscr{A})^{\mathrm{op}}$ is a "galois category" (catégorie galoisienne) in the sense of [3, V.4]. We must verify the existence of a functor $M : (\prod \mathscr{A})^{\mathrm{op}} \to \mathscr{S}_{\mathrm{fin}}$, the category of finite sets, that preserves finite limits and colimits. We will give two equivalent descriptions of M, one useful for showing it preserves limits and the second for preserving colimits.

Let $A = \prod A_i$. By repeatedly using IO, AP and Theorem 1 we can find an object B which is normal and which admits a morphism from each A_i. Let

$$MA = \mathrm{Hom}(\prod A_i, B) = \bigcup \mathrm{Hom}(A_i, B).$$

If C is another normal object containing all the A_i, there is a normal D containing B and C. Then each of



is an isomorphism. This shows that MA does not depend on the choice of B. If $A' \to A$, choose B sufficient for A and A'. Then $MA \to MA'$ is induced. Given a finite colimit diagram in $\mathscr{A}$, a B can be found which is normal and which contains every object in the diagram. Then $\mathrm{Hom}(-, B)$ converts it to a limit diagram. This shows that M preserves finite limits. It is evident that M preserves coproducts.

Before we can begin showing that M preserves coequalizers, we observe that in any category $\mathscr{A}$, there is a natural transformation $\alpha(A, C) : A \otimes C \to C^{\mathrm{Hom}(A,C)}$ where restriction to C gives the identity in each factor and to A has the value g in the coordinate corresponding to $g : A \to C$. Moreover, if $f : A \to B$, the diagram

$$\begin{array}{ccc} A \otimes C & \xrightarrow{\alpha(A,C)} & C^{\mathrm{Hom}(A,C)} \\ {\scriptstyle f \otimes C}\downarrow & & \downarrow{\scriptstyle C^{\mathrm{Hom}(f,C)}} \\ B \otimes C & \xrightarrow{\alpha(B,C)} & C^{\mathrm{Hom}(B,C)} \end{array}$$

commutes.

5.1. Proposition. *Suppose C contains a normal envelope of A. Then $\alpha(A, C)$ is an isomorphism.*

Note. By (4.9) any normal object containing A contains a normal envelope of A.

Proof. Since A has $r(A)$ maps to its normal envelope, it has that many maps to C. If $A \xrightarrow{g} D \xleftarrow{h} C$, the composite of h with the $r(A)$ maps $A \to C$ gives $r(A)$ maps $A \to D$. That is as many as there can be so g must be among them. That is, there is a $k : A \to C$ such that $hk = g$. Of course, h is mono so k is unique. For $k : A \to C$, let $\langle k \rangle : C^{MA} \to C$ denote the corresponding projection. Define $u_A : A \to C^{MA}$ by $\langle k \rangle u_A = k$ and $u_B : C \to C^{MA}$ by $\langle k \rangle u_B = 1$. For $A \xrightarrow{g} D \xleftarrow{h} C$, $h\langle k \rangle : C^{MA} \to D$ is the required map and shows that $\alpha(A, C)$ is an isomorphism.

Now we are in a position to use EC to prove that M preserves coequalizers. For if

$$A \to B \rightrightarrows C$$

is an equalizer, let D be a normal object containing C. Then

$$A \otimes D \to B \otimes D \rightrightarrows C \otimes D$$

is an equalizer. This is

$$D^{MA} \to D^{MB} \rightrightarrows D^{MC}$$

which is an equalizer iff for any object E of $\mathscr{E}$,

$$\mathrm{Hom}(E, D^{MA}) \to \mathrm{Hom}(E, D^{MB}) \rightrightarrows \mathrm{Hom}(E, D^{MC})$$

is. This sequence is

$$\mathrm{Hom}(E,D)^{MA} \to \mathrm{Hom}(E,D)^{MB} \rightrightarrows \mathrm{Hom}(E,D)^{MC}. \qquad (*)$$

Now choose E and D so that $\mathrm{Hom}(E,D)$ has at least two elements. For example, if D is any normal object different from 0, $0 \to D$ is a regular mono so that there is an equalizer

$$0 \to D \rightrightarrows D \otimes_0 D \cong D \times \cdots \times D$$

and so there are non-identity maps $D \to D$. Write $(*)$ as

$$\mathrm{Hom}(MA, X) \to \mathrm{Hom}(MB, X) \rightrightarrows \mathrm{Hom}(MC, X)$$

with $X = \mathrm{Hom}(E,D)$. Now any set with two or more elements is a cogenerator in the category of sets so the above is an equalizer iff

$$MC \rightrightarrows MB \to MA$$

is a coequalizer.

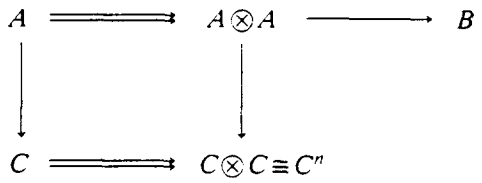
The only remaining condition on a Galois category that is not immediate is (G3). We have to show that every map in $\mathscr{E}$ is a product projection (that is obvious) and that every one in $\mathscr{M}$ is a strict mono. But a map in $\mathscr{M}$ is a product of maps of the form $A \to B_1 \times \cdots \times B_n$. That is a composite

$$A \to A^n \to B_1 \times \cdots \times B_n$$

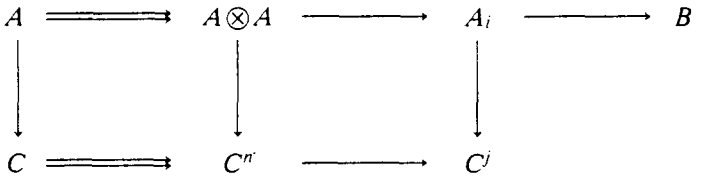
and the first is a split, hence strict mono while in the presence of RMC, the second is a product of regular, hence strict monos. Since strict monos are stable under composition and product, the conclusion follows. Grothendieck's theorem 4.1 now implies that $\prod \mathscr{A}^{\mathrm{op}}$ is equivalent to the category of finite G-sets for a profinite group G, from which our Theorem 2 follows.

6. Alternate hypotheses

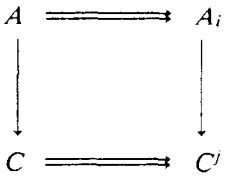
In this section, we examine some alternate hypotheses that might be useful in certain applications. The most important of these is that EC may be replaced by the same hypothesis with respect to a group of automorphisms. That is we suppose for each A and each group G of automorphisms of A, the equalizer of all the maps in G exists and is preserved by sums. This is not altogether surprising since Grothendieck's theorem only requires such equalizers exist and be preserved but that hypothesis is on all of $\prod \mathscr{A}$. Call this new hypothesis ECG (exactness condition for groups). We could either show that ECG for $\mathscr{A}$ implies the same for $\prod \mathscr{A}$ or that in the presence of the remaining hypotheses of Theorem 2, ECG implies EC. So let $A \rightrightarrows B$ be a parallel pair in $\mathscr{A}$. Suppose C is a normal object that contains B, hence also A. Choose a map $A \rightarrowtail C$. We have



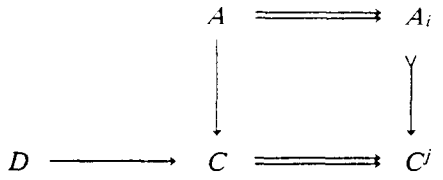
with $A \otimes A \rightarrowtail C \otimes C$ because $/\!\!/$ is stable under pushouts. If $A \otimes A = A_1 \times \cdots \times A_m$, the function $\sigma : n \to m$ is onto. The map $A \otimes A \to B$ factors through one index i and there is a non-empty subset $j \subset n$ such that there is a factorization



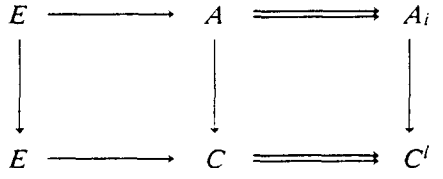
Moreover, with $A_i \rightarrowtail B$, the equalizer of the two maps $A \rightrightarrows A_i$ are the same as that of $A \rightrightarrows B$. Thus we have a commutative diagram



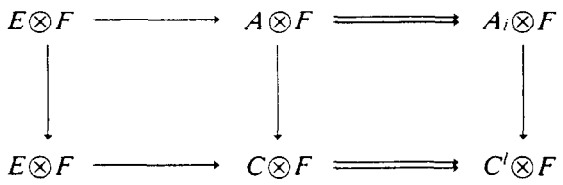
The equalizer of two maps $C \rightrightarrows C^j$ is the simultaneous equalizer of a set of pairs $f_k, g_k : C \to C$ which is the simultaneous equalizer of all pairs, 1, $\sigma_k = f_k^{-1} g_k$. This is the same as the equalizer of the subgroup G generated by the σ_k. We now suppose by ECG that the equalizer exists. Thus we have



and it is immediate that $A \cap D$, if it exists, is the required equalizer. But by RMP, $A \to C$ is the equalizer of the two maps $C \rightrightarrows C \otimes_A C \cong C^l$ and by a similar argument it is the equalizer of a group H of automorphisms of C. If K is the subgroup of aut(C) generated by G and H, the equalizer of K is the required intersection. As for preservation, once we have that both rows of

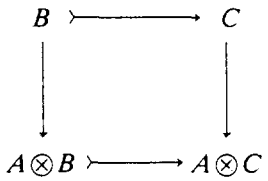


are equalizers, tensor with an arbitrary F to get



If the second row is an equalizer, so is the first.

The second potentially useful variation on a hypothesis would be to replace UBM by the suppositions that finite multisiums exist and for each A there is an $r(A)$ such that for any B there are no more than $r(A)$ maps $A \to B$. Then the proof of Theorem 1 would go through almost without change. Moreover, I claim $R(A)$ exists and is equal to $r(A)$. As seen earlier it is only necessary to show that $R(A) \leq r(A)$. So let B be any object. Let C be any object that contains B as well as a normal envelope of A. Such exists by applying AP to $D \leftarrow 0 \to B$, where D a normal envelope of A. Then



is a pushout. Thus $A \otimes B$ has no more components that $A \otimes C \cong C^{r(A)}$ by (5.1).

Somewhat surprisingly, it seems that in actual applications it is UBM rather than the above variation which seems most useful.

7. Applications

A. Finite atomic toposes

A finite atomic topos (FAT) is one in which the dual of the subcategory of atoms satisfies UBM. The terminal object in an atomic topos (AT) is an atom iff the topos is connected. (Any AT is a cartesian product — as a category — of connected ATs.) The remaining hypotheses of Theorem 2 — in particular EC — are automatic. The result is that the full subcategory of atoms in a connected FAT is the category of transitive G-sets for a profinite group G. If the topos is also complete, it is the category of all G-sets. Conversely, the category G-sets is a complete connected FAT for any profinite group G.

B. Galois theory

Let K be a commutative ring with no idempotents except 0 and 1. In that case

spec(K) is connected. In fact a closed set is classified by an ideal and if I_1 and I_2 are two ideals for which every maximal ideal contains either I_1 or I_2 and none contains both, we must have $I_1 + I_2 = K$ and every element of $I_1 I_2$ must be nilpotent. Write $1 = e_1 + e_2$, $e_i \in I_i$. Then $(e_1 e_2)^n = 0$ for some n. Let e_1 and e_2 be chosen as above so that n is as small as possible. If $n > 1$, we have

$$1 = 1^3 = e_1^2(e_1 + 3e_2) + e_2^2(3e_1 + e_2)$$

and $e_1^2(e_1 + 3e_2)$, $e_2^2(3e_1 + e_2)$ is another representation with a smaller exponent than n. Hence we can suppose $e_1 e_2 = 0$ from which it is immediate that they are orthogonal idempotents. Hence one of them, say $e_1 = 1$, while $e_2 = 0$. Now given a finitely generated projective module E, the sheaf over spec K corresponding to E is locally a sum of a certain number of copies of K. The function that assigns to each prime P the rank of E_P is continuous, hence constant, on spec K. To see that it is sufficient to find an element $a \notin P$ with E_a free. For the free rank of E_a is then the rank at all Q with $a \notin Q$ which is an open neighborhood of P. To find a, let $x_1, \ldots, x_r \in E$ be elements which give a basis of E_P. Then we have an exact sequence

$$0 \to C \to F \to E \to D \to 0$$

where F is free of rank r mapping in the obvious way to $(x_1, \ldots, x_r)$. Since E is finitely generated so is D. Since $D_P = 0$, there is a $b \notin P$ with $D_b = 0$. We then have an exact sequence

$$0 \to C_b \to F_b \to E_b \to 0$$

of R_b modules. Since E_b is projective, C_b is finitely generated projective so there is an element $c/b^n \notin P_b$ with $c/b^n C_b = 0$ from which $cC = 0$. Then $a = bc \notin P$ and both $aC = aD = 0$, whence E_a is free. Thus we have,

7.1. Proposition. *If K has no idempotents other than 0 and 1, then for each finitely generated projective module E, there is a number $R(E)$ such that at any prime P, E_P is free of rank $R(E)$. If E' is another finitely generated projective, $R(E \oplus E') = R(E) + R(E')$, $R(E \otimes E') = R(E)R(E')$.*

All K-algebras will be understood to be commutative rings with 1 which are unitary K-modules.

A strongly separable K-algebra is a K-algebra A which is K-projective as well as $A \otimes A$-projective (here and below, an undecorated $\otimes$ is $\otimes_K$). If A is such an algebra, $A \otimes A \cong A \oplus J$ and we can write $1 = e + e'$ with e in the first summand and e' in the second. Evidently e is idempotent and if $\mu : A \otimes A \to A$ is multiplication, $\mu(e) = 1$. Since J is the kernel of μ, it is generated by all $a \otimes 1 - 1 \otimes a$, $a \in A$, we have $(a \otimes 1)e = (1 \otimes a)e$. We often refer to e as the separability idempotent of A. Fix a representation $e = \sum a_i' \otimes a_i''$.

7.2. Proposition. *Let A be strongly separable. Then A is finitely generated over K.*

Proof. Since A is K projective, there is a family $\{f_j\}$ of maps $A \to K$ and a family $\{a_j\}$ of elements of A such that for all $a \in A$, $f_j(a) \neq 0$ for only finitely many indices and

$$a = \sum f_j(a)a_j.$$

This is just a formulation of the existence of a retraction $A \to J \cdot K \to A$. We let $1 \otimes f_j : A \otimes A \to A$ be defined by $(1 \otimes f_j)(a' \otimes a'') = a' f_j(a'')$. It is purely formal that $a' \otimes a'' = \sum (1 \otimes f_j)(a' \otimes a'')(1 \otimes a_j)$, where A acts on the left factor of $A \otimes A$. In particular,

$$(*) \qquad e = \sum (1 \otimes f_j)(e)(1 \otimes a_j).$$

The crucial observation is that the above sum is finite. For any $a \in A$,

$$\begin{aligned} a &= \mu(a \otimes 1) = \mu((a \otimes 1)e) \\ &= \mu((a \otimes 1) \sum (1 \otimes f_j)(e)(1 \otimes a_j)) \\ &= \mu(\sum ((a \otimes 1)(1 \otimes f_j)(e))(1 \otimes a_j)) \\ &= \mu(\sum (1 \otimes f_j)((a \otimes 1)e)(1 \otimes a_j)) \\ &= \mu(\sum (1 \otimes f_j)((1 \otimes a)e)(1 \otimes a_j)) \\ &= \mu(\sum_{j,i} a_i' f_j(a\, a_i'') \otimes a_j) \\ &= \sum_{j,i} f_j(a\, a_i'') a_i' a_j \end{aligned}$$

where the sum is taken over the finite set of indices i as well as over the finite set of j involved in the equation $(*)$ above. Thus $\{a_i' a_j\}$ is a K-generating set for A.

For future reference, we temporarily suspend, for the next proposition, the standing hypothesis that K has no idempotents.

7.3. Proposition. *Suppose A is a K-algebra which is a finitely generated projective K-module and $u : K \to A$ is the structural homomorphism. Then both the kernel and cokernel of u are K-projective.*

Remark. It follows ker u is an ideal generated by an idempotent. If there are no non-zero idempotents, u is a split mono.

Proof. Since K and A are finitely generated projectives, $C = \operatorname{coker} u$ is finitely presented. Then by [1, II. 3.3, Proposition 12, corollary 1], $A \to C$ splits iff it does locally at each prime. If $A_P = 0$ at some prime, then obviously $A_P \to C_P$ splits. Otherwise, A_P is a non-zero free K_P-module and any set of elements which give a basis mod P are already a basis of A. But A_P/PA_P is a non-zero K_P/PK_P-module

and the latter is a field so that there is always a basis beginning with the unit element. The remaining elements give a basis for C_P which is then K_P-projective so the map splits. The fact that ker u is projective is trivial.

7.4. Proposition. *Let A be a strongly separable K-algebra. Then any A-module that is k-projective is A-projective.*

Proof. Let e be the separability idempotent in $A \otimes A$. If M and M' are A-modules, $\mathrm{Hom}_K(M, M')$ is an $A \otimes A$-module by $((a \otimes a')f)(m) = af(a'm)$. If $g : M' \to M''$ is A-linear, $g((a \otimes a')f'' = (a \otimes a')gf$. Since $(a \otimes 1)e = (1 \otimes a)e$, $ef \in \mathrm{Hom}_A(M, M')$ whenever $f \in \mathrm{Hom}_K(M, M')$. Also the fact that $\mu(e) = 1$ implies that $ef = f$ whenever $f \in \mathrm{Hom}_A(M, M')$. Then we have, for a sequence of A-modules

$$0 \to M' \to M \xrightarrow{p} M'' \to 0$$

with M'' K-projective, there is a K-linear map $s : M'' \to M$ with $ps = 1$. Then $es : M'' \to M$ is A-linear and $p(es) = e\, ps = e\, 1 = 1$.

It follows that if $f : A \to B$ is a homomorphism of strongly separable K-algebras, then B is A-projective. If f is $1-1$, it has an A-linear splitting.

We say that the strongly separable algebra A is *connected* if it has no non-trivial idempotents. We denote by $\mathscr{A}$ the category of connected strongly separable algebras. I leave to the reader the easy job of verifying that $\prod \mathscr{A}$ is equivalent to the category of all strongly separable algebras. We will now verify the hypotheses of Theorem 1 for $\mathscr{A}$.

We begin with UBM. If A and B are connected and strongly separable, $A \otimes B$ is readily seen to strongly separable. If there are idempotents, let $1 = e_1 + \cdots + e_n$ be a decomposition as a sum of orthogonal ones. Then $A \otimes B = C_1 \times \cdots \times C_n$ where $C_i = (A \otimes B)e_i$. For each i, we have $B \to C_i$, which is $1-1$ by (7.3) so that $R(B) \leq R(C_i)$. Thus $nR(B) \leq \sum R(C_i) = R(A \otimes B) = R(A)R(B)$ so that $n \leq R(A)$. Now if $A \otimes B$ is not connected it can be written as $C_1 \times C_2$. If one or the other of these is not connected, it can be further decomposed. Each such decomposition leads to a set of orthogonal idempotents. No such decomposition can be into more that $R(A)$ factors. The only halt in the process comes when there is a decomposition into connected algebras, at most $R(A)$ in number.

Next consider a map $f : A \to B$. There is an A-linear $s : B \to A$ with $sf = 1$. Then $1 \otimes s : B \otimes B \to B$. If $1 \otimes b = b \otimes 1$, apply $1 \otimes s$ to get $s(b) = b$. Thus $b \in A$ and we see that $A \to B \rightrightarrows B \otimes_A B$ is an equalizer. Decomposing $B \otimes_A B$ as above, we conclude that $A \to B$ is a regular mono in $\mathscr{A}$.

If $B \leftarrow A \to C$ is given in $\mathscr{A}$, let D be any component of $B \otimes_A C$ to verify AP.

Evidently, K is the initial object. This shows that the hypotheses of Theorem 1 are satisfied. We are now in a position to give another characterization of strongly separable algebras. A K-module B is called faithfully flat if $B \otimes -$ is exact and faithful. In view of (7.3) it is clear that any K-projective K-algebra $B \supset K$ is faithfully flat.

7.5. Theorem. *The following conditions are equivalent for a algebra A over the connected ring K.*

(i) *A is strongly separable.*

(ii) *There is a connected strongly separable B such that the canonical map (Section 5)*

$$\alpha(A, B) : A \otimes B \to B^{\mathrm{Hom}(A, B)}$$

is an isomorphism.

(iii) *There is a faithfully flat K-algebra B such that $A \otimes B \cong B^n$ as a B-algebra for some finite integer n.*

That (i) $\Rightarrow$ (ii) follows from (5.1) (in which only the hypotheses of Theorem 1 are used). The next implication is obvious, given the fact that α is a B-algebra homomorphism. To prove (iii) $\Rightarrow$ (i) requires some preparation.

7.6. Proposition. *Let the K-algebra B be faithfully flat and M be a K-module. Then,*

(i) *If $B \otimes M$ is finitely generated as a B-module, M is finitely generated over K.*

(ii) *If $B \otimes M$ is finitely presented as a B-module, M is finitely presented over K.*

(iii) *If $B \otimes M$ is a finitely generated projective B-module, M is finitely generated projective over K.*

Proof. Let $B \otimes M$ be generated by the elements $\{\sum_i b_{ij} \otimes m_{ij} \mid j = 1, \ldots, n\}$. Then M' be the K-submodule of M generated by all the m_{ij}. Then we have

$$0 \to M' \to M \to M'' \to 0$$

exact which gives

$$0 \to B \otimes M' \to B \otimes M \to B \otimes M'' \to 0$$

exact. Clearly $B \otimes M' = B \otimes M$, so $B \otimes M'' = 0$ which implies $M'' = 0$ and $M' = M$. This shows (i). Next suppose $B \otimes M$ is finitely presented over B and we have

$$0 \to N \to B^n \to B \otimes M \to 0$$

with N finitely generated over B. Since M is at least finitely generated over K, we also have an exact sequence

$$0 \to M' \to K^m \to M \to 0$$

which gives an exact sequence

$$0 \to B \otimes M' \to B^m \to B \otimes M \to 0.$$

By Schanuel's lemma, $N \oplus B^m \cong (B \otimes M') \oplus B^n$ and hence $B \otimes M'$ is finitely generated. Hence M' is finitely generated and M finitely presented. Now let $B \otimes M$ be finitely generated projective. Then M is a finitely presented K-module so that

$\mathrm{Hom}(M, -)$ commutes with filtered colimits. Now for a K-module E, there is a natural map

$$E \otimes \mathrm{Hom}_K(M, N) \to \mathrm{Hom}_K(M, E \otimes N) \qquad (*)$$

which is an isomorphism when $E \cong K$, hence by finite additivity when E is finite free. I will sketch below a proof that every flat module is a filtered colimit of finite free modules. Given that, $(*)$ is an isomorphism when M is finitely presented and E is flat. The result is that

$$B \otimes \mathrm{Hom}_K(M, N) \cong \mathrm{Hom}_K(M, B \otimes N) \cong \mathrm{Hom}_B(B \otimes M, B \otimes N);$$

the latter isomorphism is standard. If $B \otimes M$ is B-projective it is now straightforward to show that M is K-projective.

Finally, let E be a flat module. The functor defined by $T(M) = E \otimes M$ is, like all functors from Mod K to Ab, a colimit of representables. Using the fact that T is right exact, the standard diagram may be replaced by the subdiagram consisting of free modules. Using that T preserves filtered colimits, the diagram may be further refined to finite free modules. The left exactness implies the standard diagram is filtered and it is easy to see, using right exactness again, that the subdiagrams described above are filtered as well. Now if F is a finite free module, $\mathrm{Hom}(F, -) \cong F^* \otimes -$ where $F^* = \mathrm{Hom}(F, K)$.

Thus

$$TM \cong \operatorname{colim} \mathrm{Hom}(F, M) \cong \operatorname{colim}(F^* \otimes M) \cong (\operatorname{colim} F^*) \otimes M,$$

whence $E \cong \operatorname{colim} F^*$.

To finish (7.5), suppose $B \otimes A \cong B^n$. Then $B \otimes A$ is B-projective so that A is K-projective. Moreover, $B \otimes A$ is $(B \otimes A) \otimes_B (B \otimes A)$ projective (trivial). This may be written as asserting that $(B \otimes A \otimes A) \otimes_{A \otimes A} A$ is $B \otimes A \otimes A$-projective. Assuming $B \otimes A \otimes A$ is faithfully flat as an $A \otimes A$-module, this implies, by another application of (7.6) that A is $A \otimes A$-projective. But

$$(B \otimes A \otimes A) \otimes_{A \otimes A} - \cong B \otimes -$$

and thus the functor on the left is also faithful and exact.

It is clear that (7.5) could be generalized by replacing B by a family $\{B_i\}$ of flat K-algebras that are collectively faithful.

Now we can verify EC. For if $A \rightrightarrows B$ is a pair of maps in $\mathscr{A}$, let

$$C \to A \rightrightarrows B$$

be the equalizer in K-algebras, since tensoring with a K-projective is exact, we get, for a normal envelope D of B,

$$C \otimes D \to D^{\mathrm{Hom}(A, D)} \rightrightarrows D^{\mathrm{Hom}(B, D)}$$

and so $C \otimes D \cong D^X$ where

$$\mathrm{Hom}(B, D) \rightrightarrows \mathrm{Hom}(A, D) \to X$$

is a coequalizer (see the argument of Section 5). Hence C is strongly separable from (7.5).

It is left as a trivial exercise to apply (7.5) to show that $A \to B$ is a map in $\mathscr{A}$, B is a strongly separable A-algebra.

It now follows that $\mathscr{A}$ satisfies Theorem 2 and is dual to the category of transitive G-sets. All the usual Galois theory of commutative rings — and fields — follows immediately. In particular, G is the inverse limit of a functor into the category of finite G-sets. Turning that around we get a functor into the category of strongly separable K-algebras whose direct limit-taken in the category of all K-algebras — is the separable closure of K.

The results here are known and are found by combining results of [2], and work of Harrison found in Section 1 of [4].

In the next two examples we will construct a "profinite fundamental group". Where the usual fundamental group classifies covering maps of arbitrary size, this one is only for finite covering maps. See [5, 8.4] for a construction valid in a general connected topos. I do not understand what further hypothesis has to be made to carry out the construction of the genuine fundamental group. When there is a fundamental group, the construction here gives only its profinite completion.

C. Simplicial complexes

This is the profinite approximation of the theory developed in [8]. A simplicial complex (SC) is a set together with a set of finite subsets called simplexes which are stable under the formation of further subsets. If X and Y are two such sets on admissible map from Y to X is a function $f: Y \to X$ such that f takes a simplex to a simplex. An n-simplex in X is a simplex consisting of $n+1$ distinct elements. f is called a (finite) covering map if the inverse image under f of an n-simplex is a disjoint union of (a finite number of) n-simplexes of Y.

The SC X is called connected if it is not possible to write $X = X_1 + X_2$ where X_1 and X_2 are disjoint and non-empty and such that every simplex of X is wholly contained in X_1 or X_2. It is easily seen to be equivalent to the assertion that for all $\alpha, \beta \subset X$ simplexes, there is a sequence of simplexes $\alpha = \gamma_1, \gamma_2, \ldots, \gamma_n = \beta$ such that for all $1 \leq i < n$, $\gamma_i \cap \gamma_{i+1} = \emptyset$. For take X_1 to be the union of all β that can be "chained" to α in that way and X_2 the complement. If $f: Y \to X$ is a finite covering map and X is connected then the number of simplexes above each α is the same. When $\emptyset \neq \beta \subset \alpha$ this is clear. For the general case, use the chaining condition. This number we call $R(Y)$. From here on, all covering maps will be finite. The following is immediate.

7.7. Proposition. *Suppose $f: Y \to X$ is a covering map and $Y = Y_1 + Y_2$ (disjoint union). Then $f_1 = f \mid Y_1$ and $f_2 = f \mid Y_2$ are covering maps; moreover $R(Y_1 + Y_2) = R(Y_1) + R(Y_2)$.*

7.8. Proposition. *Suppose $f: Y \to X$ and $g: Z \to X$ as covering maps. Then so is the canonical map $h: Y \times_X Z \to X$; moreover $R(Y \times_X Z) = R(Y)R(Z)$.*

Proof. $Y \times_X Z$ consists of all pairs $(y, z) \in Y \times Z$ for which $fy = gz$. A subset

$$\{(y_0, z_0), (y_1, z_1), \ldots, (y_n, z_n)\}$$

of $Y \times_X Z$ is a simplex iff $\{y_0, \ldots, y_n\}$ is a simplex in Y and $\{z_0, \ldots, z_n\}$ is a simplex in Z. Suppose now that $R(Y) = r$ and $R(Z) = s$. Let $\alpha = \{x_0, \ldots, x_n\}$ be an n-simplex in X. This means, in particular, that $x_0, \ldots, x_n$ are all distinct. The simplexes in Y above α are $\{y_{01}, \ldots, y_{n1}\}, \ldots, \{y_{0r}, \ldots, y_{nr}\}$ and those in Z are $\{z_{01}, \ldots, z_{n1}\}, \ldots, \{(z_{0s}, \ldots, z_{ns})\}$. Then for any of the rs choices of $1 \leq i \leq r$, $1 \leq j \leq s$, $\{(y_{0i}, z_{0j}), \ldots, (y_{ni}, z_{nj})\}$ is an n-simplex of $Y \times_X Z$ above α. Suppose $\beta = \{(y_0, z_0), \ldots, (y_m, z_m)\}$ is an m-simplex lying above α. Then $\{y_0, \ldots, y_m\}$ is a simplex in Y lying over α. If there is a repetition, say $y_0 = y_1$ while $z_0 \neq z_1$. But then $\{z_0, z_1\}$ 1-simplex in Z mapping to the 0-simplex $\{fy_0, fy_1\}$ which is a contradiction as then $g^{-1}\{fy_0\}$ will contain a simplex of dimension ≥ 1. Thus $\{y_0, \ldots, y_m\}$ is an m-simplex, and $m = n$. This implies that β is one of the already enumerated simplexes and finishes the proof.

7.8. Proposition. *Let $f : Y \to X$, $g : Z \to Y$ and $h = fg$ be admissible maps with g onto. If any two are coverings, so is the third.*

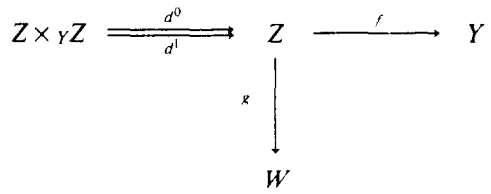
Proof. In the case of f and g, this is immediate. If h and f are coverings, let $\alpha = \{y_0, \ldots, y_n\}$ be an n-simplex in Y. Then $g^{-1}(\alpha) \subset h^{-1}f(\alpha)$ and the latter is a disjoint union of n-simplexes. Now suppose $z \in g^{-1}(\alpha)$. There is an n-simplex $\beta = \{z = z_0, z_1, \ldots, z_n\}$ in Z mapping to $f(\alpha)$. Then $g\beta = \{gz_0, gz_1, \ldots, gz_n\}$ is an n-simplex in Y. See the proof of (7.7) for an argument that h, hence g is $1-1$ on simplexes. Now α and $g\beta$ are n-simplexes in $f^{-1}(f(\alpha))$ and hence are either equal or disjoint. Since they have y_0 in common, $\alpha = g\beta$. Thus β is an n-simplex in $g^{-1}(\alpha)$. Hence every element and consequently every simplex in $g^{-1}(\alpha)$ can be extended to an n-simplex. Thus $g^{-1}(\alpha)$ is a sum of some of n-simplexes in $h^{-1}(f\alpha)$.

Next suppose that g and h are coverings. Suppose α is an n-simplex in X. Suppose β and γ in $f^{-1}(\alpha)$ are two simplexes with $\beta \cap \gamma \neq \emptyset$ but $\beta \cup \gamma$ not a simplex. Let $\delta = \beta \cap \gamma$. With g onto there is a simplex $\delta' \subset Z$ lying above δ. Since $\delta' \subset g^{-1}(\delta) \subset g^{-1}(\beta)$ there is a simplex β' lying above β. Similarly there is a simplex γ' lying over γ. $\beta' \cup \gamma'$ cannot be a simplex as $g(\beta' \cup \gamma') = \beta \cup \gamma$ isn't. But then $h^{-1}(\alpha)$ is not a disjoint union of complexes. This shows that $f^{-1}(\alpha)$ is a disjoint union of simplexes. If one of them, β, is an m-simplex, $m \neq n$, there is an m-simplex β' lying above β. Since $\beta' \subset h^{-1}(\alpha)$, $\beta' \subset \gamma'$ where γ' is an n-simplex. $\gamma = g\gamma'$ is evidently an n-simplex containing β and lying over α.

Now fix a connected X. We let $\mathscr{A}^{\mathrm{op}}$ denote the category of non-empty connected coverings of X. It is readily seen that $(\prod \mathscr{A})^{\mathrm{op}}$ is the category of all covering maps. I claim that $\mathscr{A}$ satisfies the hypotheses of theorem 2. First we observe that if $Z \to Y$ is a map it is onto. Then

$$Z \times_Y Z \rightrightarrows Z \to Y$$

is a coequalizer in sets and can easily be seen to be one in the category of SCs. If we have



with $gd^0 = gd^1$ and both f and g coverings, the induced $Y \to W$ is also a covering by (7.8). Thus $Z \to Y$ is a regular epi in $(\pi\mathscr{A})^{\mathrm{op}}$ from which it is in $\mathscr{A}^{\mathrm{op}}$ by using the components of $Z \times_Y Z$. A similar argument with $Z \times_Y W$ verifies the dual of AP for $Z \to Y \leftarrow W$. Conditions BMS and IO are routine. We are only left to verify EC. Let $f: Y \to X$ be a covering and G be a group of automorphisms of Y such that $\sigma f = f$ for all $\sigma \in G$. Suppose $\alpha = \{y_0, \ldots, y_n\}$ is an n-simplex in Y and $\beta = \{y_0, \ldots, fy_n\} \subset X$. If $\sigma\alpha \cap \alpha \neq \emptyset$, we have $f^{-1}(\beta) \supset \alpha \cup \sigma\alpha$, each being n-simplexes so that $\alpha = \sigma\alpha$. If $\sigma y_i = y_j$, $i \neq j$ we have $x_i = fy_i = f\sigma y_i = fy_j = x_j$, a contradiction so that $\sigma y_i = y_i$ is the only possibility. In other words the orbit of α under G is a set of disjoint n-simplexes. If Z is the orbit space, the inverse image of an n-simplex in Z is that set of disjoint n-simplexes. Hence $Y \to Z$ is a covering map and by (7.8) so is $Z \to Y$. Now the image in $Y \times Y$ of the canonical maps

$$G \times Y \underset{d^1}{\overset{d^0}{\rightrightarrows}} Y, \qquad d^0(\sigma, y) = y, \quad d^1(\sigma, y) = \sigma y,$$

is an equivalence relation; the unit, inverse and multiplication in G give the reflexive, symmetric and transitive properties, respectively. Thus we have

$$G \times Y \twoheadrightarrow Y \times_Z Y \rightrightarrows Y \twoheadrightarrow Z.$$

If $W \to X$ is any other covering, $W \times_X -$ is computed at the underlying set level and preserves regular epis. It certainly preserves kernel pairs so we have

$$W \times_X (G \times Y) \twoheadrightarrow (W \times_X Y) \times_Z (W \times_X Y) \rightrightarrows W \times_X Y \twoheadrightarrow W \times_X Z$$

from which we see that

$$G \times (W \times_X Y) \rightrightarrows W \times_X Y \twoheadrightarrow W \times_X Z$$

is a coequalizer. This verifies ECG and shows that $\mathscr{A}^{\mathrm{op}}$ is equivalent to the category of G-sets for a profinite group G. This gives the finite part of the Galois connection noted in [8].

D. Topological spaces

If X is a topological space, a (finite) covering of X is a map $f: Y \to X$ such that for all $x \in X$ there is an open neighborhood U of x with the property that $f^{-1}(U)$ is a disjoint union of (a finite number of) open sets mapped homeomorphically to U by

f. When X is connected, the number is constant and the theory proceeds almost identically to the preceding example. The only thing to note is that although it is not generally true in topological spaces that a pullback of a regular epi is a regular epi, it is here since a covering map is star open. The Galois connection here was first observed in [7].

References

[1] N. Bourbaki, Commutative Algebra (Addison Wesley, Reading, MA, 1972).
[2] S.U. Chase, D.K. Harrison, A. Rosenberg, Galois theory and cohomology of commutative rings, Mem. Amer. Math. Soc. 52 (1965) 15–33.
[3] A. Grothendieck, Revêtements étales et groupe fondamental, (SGA1), Springer Lecture Notes in Math. 224 (Springer-Verlag, Berlin, 1971).
[4] G.J. Janusz, Separable algebras over commutative rings, Trans. Amer. Math. Soc. 122 (1966) 461–479.
[5] P.T. Johnstone, Topos Theory (Academic Press, New York, 1977).
[6] G.M. Kelly, Monomorphisms, epimorphisms and pullbacks, J. Austral. Math. Soc. 9 (1969) 124–142.
[7] S. Lubkin, Theory of covering spaces, Trans. Amer. Math. Soc. 104 (1962) 204–238.
[8] J.J. Rotman, Covering complexes with applications to algebra, Rocky Mountain J. Math. 4 (1973) 641–674.