LE MATEMATICHE
Vol. LI (1996) – Supplemento, pp. 127-136

ON SEPARABLE ALGEBRAS IN GROTHENDIECK GALOIS THEORY

FEDERICO G. LASTARIA

To the memory of Umberto Gasapina

We give an explicit proof of the fundamental theorem of Grothendieck Galois theory: the category of separable algebras over a field K is anti-equivalent to the category of continuous actions on finite sets of the profinite fundamental group of K.

1. Introduction.

The aim of this note is to give an exposition of Grothendieck theorem on Galois theory, emphasizing the rôle of continuous actions and of separable algebras in that context.

Galois theory for field extensions that are algebraic normal and separable but of possibly infinite degree, requires regarding Galois groups as topological groups. Galois groups are profinite groups; the converse also holds (see [3], [6], [8]). Recall that profinite groups are (projective) limits, in the category of topological groups, of diagrams whose vertices are finite discrete groups. Equivalently, profinite groups are totally disconnected compact Hausdorff groups ([7]). Then we have the following:

Theorem 1.1. (Fundamental Theorem of Infinite Galois Theory). *Let $K \subset L$ be a Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. Then there is a*

bijection between the set $\mathcal{F}$ of all intermediate fields between K and L and the set $\mathcal{S}$ of all closed subgroups of G. More precisely, $F \longrightarrow \mathrm{Gal}(L/F)$ is a one-to-one mapping from $\mathcal{F}$ to $\mathcal{S}$. Its inverse is the mapping $H \longrightarrow L^H = \{x \in L \mid \sigma(x) = x \quad \forall \sigma \in H\}$. Furthermore, let the intermediate field F correspond to the closed subgroup H. Then:

i) $K \subset F$ is finite $\Longleftrightarrow$ H is open. When this occurs, $[F: K] = [G: H]$;
ii) $K \subset F$ is Galois $\Longleftrightarrow$ H is normal.

(See e.g. [3] or [6] for a proof).

The largest Galois extension of any field K is the *separable closure* K_s of K, that is the subfield of the algebraic closure $\overline{K}$ consisting of all elements separable over K; $K_s = \overline{K}$ if $\mathrm{char}(K) = 0$.

Now let E be any intermediate field between K and K_s, with $[E: K]$ finite. Then the subgroup $H = \mathrm{Gal}(K_s/E) \subset G$ is open and the set of left cosets G/H is finite. Furthermore, the transitive action of G on the finite discrete set G/H is continuous, because the stabilizer H is open. This allows to see the Galois connection $E \longleftrightarrow K$ as an order reversing bijection between intermediate fields $K \subset E \subset K_s$ of finite dimension over K and continuous transitive actions of G on the finite discrete sets G/H with H open.

Once this point of view is adopted, one is led to extend the Galois connection by taking into account all coproducts of such continuous transitive actions - i.e., up to isomorphisms, all continuous actions – on the one hand and all products of such intermediate fields – i.e., up to isomorphisms, all separable K-algebras - on the other. Indeed this can be done in a functorial way exhibiting an equivalence of categories, as Grothendieck theorem shows (see Theorem 2.1 below).

This theorem is a special instance of Grothendieck Galois theory for schemes, which classifies the finite étale coverings of a connected scheme X in terms of the fundamental group $\pi(X)$ of X (see Remark 2.2). Nevertheless, a direct approach, even if it may appear as a mere reformulation of infinite Galois theory, is worthy both as a motivating example for further developments and for its intrinsic interest. Clearly the new aspects of this paper regard some detailed proofs which, though essentially known to the specialists, are usually difficult to find in the literature.

A very useful introduction to Galois theory for schemes, to which the author and the present paper are indebted, is [4]. For a related approach, at least for finite Galois groups, see [1].

2. A categorical version of Galois theory.

Let K be any field. By a *K-algebra* we mean a commutative ring A with an identity element, along with a ring morphism $f : K \longrightarrow A$. Equivalently, a K-algebra is a commutative ring A with an identity element, which is also a K-vector space and satisfies

$$k(ab) = (ka)b = a(kb)$$

for every $k \in K$ and every $a, b \in A$.
Let $\overline{K}$ be the algebraic closure of K. A K-algebra A is *separable* (over K) if $\overline{A} = A \otimes_K \overline{K}$ has zero Jacobson radical, that is, if the maximal ideals of A have intersection zero. A finite-dimensional K-algebra A is separable if and only if A is isomorphic to a finite product of finite dimensional field extensions of K each of which is separable in the usual sense: the irreducible polynomial over K of any of its elements has no repeated roots in any splitting field.

Theorem 2.1. (Grothendieck). *There is an equivalence of categories*

$$(\mathrm{SepAlg}_K)^{\mathrm{op}} \simeq \mathrm{Set}^G_{\mathrm{fin}}$$

between the dual of the category of separable K-algebras over a field K and the category of continuous actions on finite sets of the profinite Galois group $G = \mathrm{Gal}(K_s/K)$ of a separable closure K_s of K.

Proof. We must prove that there exist two functors

$$\Phi : (\mathrm{SepAlg}_K)^{\mathrm{op}} \longrightarrow \mathrm{Set}^G_{\mathrm{fin}}$$

$$\Gamma : \mathrm{Set}^G_{\mathrm{fin}} \longrightarrow (\mathrm{SepAlg}_K)^{\mathrm{op}}$$

for which $\Gamma\Phi$ and $\Phi\Gamma$ are naturally equivalent to the identity functors of $(\mathrm{SepAlg}_K)^{\mathrm{op}}$ and $\mathrm{Set}^G_{\mathrm{fin}}$ respectively.

1) Definition of the functor Φ.
If A is any separable K-algebra, let

$$\Phi(A) = \mathrm{Alg}_K(A, K_s)$$

be the set of all K-algebra morphisms from A to K_s. The Galois group $G = \mathrm{Gal}(K_s/K)$ acts on $\Phi(A)$ by composition on the left. Fix a K-algebra isomorphism

$$A \simeq \prod_{i=1}^{h} K_i \,,$$

where $K \subseteq K_i \subseteq K_s$ for each $i = 1, \ldots, h$ and every $K \subseteq K_i$ is a finite separable extension of the field K. By the fundamental theorem of infinite Galois theory,

$$K_i = K_s^{G_i},$$

where $G_i \subseteq G$ is the open subgroup:

$$G_i = \{\sigma \in G \mid \sigma(x) = x \quad \forall x \in K_i\}.$$

Since

$$\mathrm{Alg}_K(K_s^{G_i}, K_s) \simeq G/G_i$$

(Lemma 2.4) and

$$\mathrm{Alg}_K\Big(\prod_{i=1}^{h} K_i, K_s\Big) \simeq \coprod_{i=1}^{h} \mathrm{Alg}_K(K_i, K_s)$$

as G-sets (Lemma 2.5), we have the following G-set isomorphisms:

$$\begin{aligned}
\mathrm{Alg}_K(A, K_s) &\simeq \mathrm{Alg}_K\Big(\prod_{i=1}^{h} K_i, K_s\Big) \\
&\simeq \coprod_{i=1}^{h} \mathrm{Alg}_K(K_i, K_s) \\
&\simeq \coprod_{i=1}^{h} \mathrm{Alg}_K(K_s^{G_i}, K_s) \\
&\simeq \coprod_{i=1}^{h} G/G_i.
\end{aligned}$$

Each index $[G: G_i]$ is finite, because the subgroups G_i are open: thus $\mathrm{Alg}_K(A, K_s)$ is a finite set. Furthermore the action of G on each finite discrete set G/G_i is continuous, because the stabilizer G_i is open; therefore the action of G on $\mathrm{Alg}_K(A, K_s) \simeq \coprod_{i=1}^{h} G/G_i$ is continuous too. At last, Φ is defined on arrows in the obvious way: for any K-algebra morphism $f : A \longrightarrow B$, $\Phi(f) : \Phi(B) \longrightarrow \Phi(A)$ maps $g \in \Phi(B)$ to $gf \in \Phi(A)$.

2) Definition of the functor Γ.
For any S in $\mathrm{Set}_{\mathrm{fin}}^{G}$, let

$$\Gamma(S) = \mathrm{Set}_{\mathrm{fin}}^{G}(S, K_s)$$

be the K-algebra of all G-set morphisms from S to K_s. Here K_s is seen as a G-set via evaluation and operations on the K-algebra $\Gamma(S)$ are defined pointwise. We still have to prove that $\Gamma(S)$ is separable as a K-algebra.
Let S be any finite continuous G-set and $S \simeq \coprod_{i=1}^{h} S_i$ its decomposition as coproduct of orbits. For each S_i there is an isomorphism $S_i \simeq G/G_i$ for some open subgroup $G_i \subseteq G$ (choose any point in S_i and let G_i be its stabilizer). Then $S \simeq \coprod_{i=1}^{h} G/G_i$ and

$$\begin{aligned}\mathrm{Set}_{\mathrm{fin}}^{G}(S, K_s) &\simeq \mathrm{Set}_{\mathrm{fin}}^{G}\Big(\coprod_{i=1}^{h} G/G_i, K_s\Big)\\ &\simeq \prod_{i=1}^{h} \mathrm{Set}_{\mathrm{fin}}^{G}(G/G_i, K_s)\\ &\simeq \prod_{i=1}^{h} K_s^{G_i},\end{aligned}$$

where each $K_s^{G_i}$ is a finite separable field extension of K (see Lemma 2.3). This proves $\mathrm{Set}_{\mathrm{fin}}^{G}(S, K_s)$ is a separable K-algebra.
For each G-set morphism $\psi : S \longrightarrow T$, $\Gamma(\psi) : \Gamma(T) \longrightarrow \Gamma(S)$ maps g to the composite $g\psi$. This completes the definition of the functor Γ.

3) The natural isomorphism $1 \Longrightarrow \Gamma\Phi$.
We define a natural isomorphism $\eta : 1 \Longrightarrow \Gamma\Phi$ as follows. For all separable K-algebras A define

$$\eta_A : A \longrightarrow \Gamma\Phi(A) = \mathrm{Set}_{\mathrm{fin}}^{G}(\mathrm{Alg}_K(A, K_s), K_s)$$

by:

$$\eta_A(a)(g) = g(a)$$

for all $a \in A$ and $g \in \mathrm{Alg}_K(A, K_s)$. Commutativity of the square

$$\begin{array}{ccc} A & \xrightarrow{\ f\ } & B \\ {\scriptstyle \eta_A}\downarrow & & \downarrow{\scriptstyle \eta_B} \\ \Gamma\Phi(A) & \xrightarrow[\Gamma\Phi(f)]{} & \Gamma\Phi(B) \end{array}$$

follows easily from the definitions of η, Γ and Φ. In fact, for every $a \in A$ and $g \in \mathrm{Alg}_K(B, K_s)$,

$$\begin{aligned}[(\Gamma\Phi)(f)\eta_A](a)(g) &= [\Gamma(\Phi f)(\eta_A(a))](g)\\ &= (\eta_A(a)\Phi f)(g)\\ &= \eta_A(a)(gf) = g(f(a))\end{aligned}$$

and

$$\begin{aligned}(\eta_B f)(a)(g) &= \eta_B(f(a))(g)\\ &= g(f(a)).\end{aligned}$$

It remains to prove that η_A is an isomorphism for every K-algebra A. Since all K-algebras are isomorphic to some product $B = \prod_{i=1}^{h} K_s^{G_i}$ and η is a natural transformation, it is enough to show that η_B is an isomorphism for every such product B. Now we have the following isomorphisms:

$$\begin{aligned}B &= \prod_{i=1}^{h} K_s^{G_i}\\ &\simeq \prod_{i=1}^{h} \mathrm{Set}_{\mathrm{fin}}^{G}(G/G_i, K_s)\\ &\simeq \mathrm{Set}_{\mathrm{fin}}^{G}\Big(\coprod_{i=1}^{h} G/G_i, K_s\Big)\\ &\simeq \mathrm{Set}_{\mathrm{fin}}^{G}\Big(\coprod_{i=1}^{h} \mathrm{Alg}_K(K_s^{G_i}, K_s)\Big)\\ &\simeq \mathrm{Set}_{\mathrm{fin}}^{G}\Big(\mathrm{Alg}_K\Big(\prod_{i=1}^{h} K_s^{G_i}, K_s\Big), K_s\Big)\\ &= \Gamma\Phi\Big(\prod_{i=1}^{h} K_s^{G_i}\Big)\\ &= \Gamma\Phi(B).\end{aligned}$$

The first isomorphism is defined in Lemma 2.3; the second is categorial; the other two are defined in Lemmas 2.4 and 2.5 respectively. Keeping into account how the above isomorphisms are defined, one sees that their composition is exactly the evaluation η_B. Indeed, let ω be the composition of the above isomorphisms. For any $x = (x_1, \ldots, x_h) \in B$, $\omega(x) \in \Gamma\Phi(B)$ is described as follows. Let f be in $\mathrm{Alg}_K(\prod_{i=1}^{h} K_s^{G_i}, K_s)$; by Lemma 2.5 $f = f_j\pi_j$ where π_j is the j-th projection and $f_j : K_s^{G_j} \longrightarrow K_s$. As in Lemma 2.4, write $f_j = \sigma|_{K_s^{G_j}}$ as the restriction of a suitable $\sigma \in G$. Then

$$\begin{aligned}\omega(x)(f) &= (\sigma|_{K_s^{G_j}})\pi_j(x)\\ &= (f_j\pi_j)(x)\\ &= f(x)\\ &= \eta_B(f)\end{aligned}$$

It follows $\omega = \eta_B$ as claimed.

3) The natural isomorphism $1 \Longrightarrow \Phi\Gamma$.
The existence of a natural isomorphism $\tau : 1 \Longrightarrow \Phi\Gamma$ is proved similarly. For every G-set S, define

$$\tau_S : S \longrightarrow \Phi\Gamma(S) = \mathrm{Alg}_K(\mathrm{Set}^G_{\mathrm{fin}}(S, K_s), K_s)$$

by: $\tau_S(s)(\phi) = \phi(s)$ for all $s \in S$ and $\phi \in \mathrm{Set}^G_{\mathrm{fin}}(S, K_s)$. Naturality, that is commutativity of

$$\begin{array}{ccc} S & \xrightarrow{\alpha} & T \\ {\scriptstyle \tau_S}\downarrow & & \downarrow{\scriptstyle \tau_T} \\ \Phi\Gamma(S) & \xrightarrow[\Phi\Gamma(\alpha)]{} & \Phi\Gamma(T) \end{array}$$

for every $\alpha : S \longrightarrow T$, is easily checked.
It is enough to prove τ_T is an isomorphism for any coproduct $T = \coprod_{i=1}^{h} G/G_i$, because any object in $\mathrm{Set}^G_{\mathrm{fin}}$ is isomorphic to such a T and τ is natural. Indeed, we have the following isomorphisms:

$$\begin{aligned} T &= \coprod_{i=1}^{h} G/G_i \\ &\simeq \coprod_{i=1}^{h} \mathrm{Alg}_K(K_s^{G_i}, K_s) \\ &\simeq \mathrm{Alg}_K\Big(\prod_{i=1}^{h} K_s^{G_i}, K_s\Big) \\ &\simeq \mathrm{Alg}_K\Big(\prod_{i=1}^{h} \mathrm{Set}^G_{\mathrm{fin}}(G/G_i, K_s), K_s\Big) \\ &\simeq \mathrm{Alg}_K\Big(\mathrm{Set}^G_{\mathrm{fin}}\Big(\coprod_{i=1}^{h} G/G_i, K_s\Big), K_s\Big) \\ &= \Phi\Gamma(T) \end{aligned}$$

where the first three isomorphisms are defined respectively in Lemmas 2.4, 2.5, 2.3, while the fourth one is categorial. Unravelling the definitions of the isomorphisms above, we see that their composition is exactly τ_T.
Then $\tau : 1 \Longrightarrow \Phi\Gamma$ is a natural isomorphism. This ends the proof of the theorem.

Remark 2.2. The equivalence $(\mathrm{SepAlg}_K)^{\mathrm{op}} \simeq \mathrm{Set}_{\mathrm{fin}}^G$ is a special instance of Grothendieck Galois theorem for schemes:
Let X be any connected scheme. Then there exists a profinite group G, unique up to isomorphisms, for which the category FinEt_X *of finite étale coverings of X is equivalent to the category* $\mathrm{Set}_{\mathrm{fin}}^G$ *of finite sets on which G acts continuously.*
(See [4], [5]). The group G is the *fundamental group* of X. If $X = \mathrm{Spec}\, K$ is the spectrum of an arbitrary field K, then $\mathrm{FinEt}_X \simeq (\mathrm{SepAlg}_K)^{\mathrm{op}}$ and $G = \mathrm{Gal}(K_s/K)$. Hence Theorem 2.1 is the special case $X = \mathrm{Spec}\, K$ of the theorem above, up to the claim about uniqueness of the group G.
Notice that the category $(\mathrm{SepAlg}_K)^{\mathrm{op}}$ is a *Galois category* in the sense of Grothendieck (see [2], Exposé 5). Here the fundamental functor is $F : (\mathrm{SepAlg}_K)^{\mathrm{op}} \longrightarrow \mathrm{Set}_{\mathrm{fin}}$ defined by $F(A) = \mathrm{Alg}_K(A, K_s)$ for every K-algebra A. The functor F is pro-representable and a fundamental pro-object is any separable closure K_s of K.

2.1. Some lemmas.

We collect in this section some facts used in the proof of Theorem 2.1.

Lemma 2.3. *Let $G_i \subset G$ be any subgroup. Then*

$$\mathrm{Set}_{\mathrm{fin}}^G(G/G_i, K_s) \simeq K_s^{G_i}$$

as K-algebras.

Proof. Let $\phi : G/G_i \longrightarrow K_s$ be any G-set morphism and let $a = \phi([G_i])$. Then for every $\sigma \in G_i$,

$$\sigma(a) = \sigma(\phi([G_i]) = \phi(\sigma[G_i]) = \phi([G_i]) = a.$$

Thus $a \in K_s^{G_i}$. Then it is easily seen that evaluation in $[G_i]$:

$$\begin{aligned} \mathrm{Set}_{\mathrm{fin}}^G(G/G_i, K_s) &\longrightarrow K_s^{G_i} \\ \phi &\longmapsto \phi([G_i]) \end{aligned}$$

gives the claimed isomorphism.

Lemma 2.4. *Let H be any closed subgroup of the Galois group $G = \mathrm{Gal}(K_s/K)$. Then*

$$G/H \simeq \mathrm{Alg}_K(K_s^H, K_s)$$

as G-sets.

Proof. Define

$$\rho : G/H \longrightarrow \mathrm{Alg}_K(K_s^H, K_s)$$

as restriction to K_s^H: $\rho(gH)(x) = g(x)$ for every left coset gH and every $x \in K_s^H$. It is easy to see that ρ is well defined and that it is an injective G-set morphism. It is also surjective, because every $f \in \mathrm{Alg}_K(K_s^H, K_s)$ extends to an automorphism of the algebraic closure of K and the restriction $f|_{K_s}$ to the separable closure belongs to $G = \mathrm{Gal}(K_s/K)$ because K_s is normal over K.

Lemma 2.5. *Let $K \subset K_i$, $i = 1, ..., h$, and $K \subset L$ be any field extensions. Then there is a bijection of sets:*

$$\coprod_{i=1}^{h} \mathrm{Alg}_K(K_i, L) \simeq \mathrm{Alg}_K\Big(\prod_{i=1}^{h} K_i, L\Big).$$

Proof. We prove the map

$$\Lambda : \coprod_{i=1}^{h} \mathrm{Alg}_K(K_i, L) \longrightarrow \mathrm{Alg}_K\Big(\prod_{i=1}^{h} K_i, L\Big)$$
$$(g : K_j \longrightarrow L) \longmapsto g\pi_j$$

is a bijection. Let f be in $\mathrm{Alg}_K\big(\prod_{i=1}^{h} K_i, L\big)$.
The elements $e_i = (0, \ldots, 1, \ldots, 0)$ (all zeroes except 1 at the i-th position), $i = 1, \ldots, h$, are idempotents ($e_i^2 = e_i$). Therefore the elements $f(e_i) \in L$ are idempotents as well. Since L is a field, this means $f(e_i) = 0$ or 1. Since f preserves units, that is

$$1 = f(1, \ldots, 1) = f(e_1 + \cdots + e_h) = f(e_1) + \cdots + f(e_h),$$

there is at least one index, say j, for which $f(e_j) = 1$. If $i \neq j$,

$$0 = f(0) = f(e_i e_j) = f(e_i) f(e_j) = f(e_i).$$

Thus for every $(x_1, \ldots, x_h) \in \prod_{i=1}^{h} K_i$

$$\begin{aligned} f(x_1, \ldots, x_h) &= f((x_1, \ldots, 0)e_1 + \cdots + (0, \ldots, x_h)e_h) \\ &= f(x_1, \ldots, 0) f(e_1) + \cdots + f(0, \ldots, x_h) f(e_h) \\ &= f(0, \ldots, x_j, \ldots, 0) f(e_j) \\ &= f(0, \ldots, x_j, \ldots, 0). \end{aligned}$$

Then we see that there is a unique $g \in \coprod_{i=1}^{h} \mathrm{Alg}_K(K_i, L)$ such that $\Lambda(g) = g\pi_j = f$, namely $g : K_j \longrightarrow L$ defined by $g(x_j) = f(0, \ldots, x_j, \ldots, 0)$ for all $x_j \in K_j$.

Acknowledgments. The author wishes to thank Renato Betti and Sandra Mantovani for fruitful discussions and suggestions, and Ieke Moerdijk for his lectures on Galois theory at the Politecnico of Milano and for pointing out and making available reference [4].

REFERENCES

[1] A.W.M. Dress, *One more shortcut to Galois theory,* Adv. Math., 110 (1995), pp. 129-140.

[2] A. Grothendieck, *Révetements Etales et Groupe Fondamental,* Lecture Notes in Math. No. 224, Springer, Berlin, 1971.

[3] K. Gruenberg, *Profinite Groups,* In Cassels, J.W.S. and Frölich, A. *Algebraic Number Theory,* Academic Press, London, 1967.

[4] H.W. Lenstra, *Galois Theory for Schemes,* Mathematisch Instituut, Universiteit von Amsterdam, 1985.

[5] J.S. Milne, *Étale Cohomology,* Princeton University Press, Princeton, New Jersey, 1980.

[6] P. Ribenboim, *L'Arithmétique des Corps,* Hermann, Paris, 1972.

[7] S. Shatz, *Profinite Groups, Arithmetic and Geometry,* Annals of Math. Study No. 67, Princeton, Princeton University Press, 1972.

[8] W.C. Waterhouse, *Profinite groups are Galois groups,* Proc. Amer. Math. Soc., 42 (1974), pp. 639-640.

Dipartimento di Matematica,
Politecnico di Milano,
Piazza Leonardo da Vinci 32,
20133 Milano (ITALY)
e-mail: fedlas@mate.polimi.it