ON GENERAL GALOIS THEORY

By Julio R. Bastida

1. Introduction

It is the purpose of this note to give a presentation of the general Galois correspondence between subgroups and intermediate subfields, based on the most elementary properties of algebraic field extensions and of topological groups. We proceed directly to the case of field extensions of arbitrary degree. The theory for field extensions of finite degree is seen to be an easy particular case; for this reason, we shall concern ourselves only with those results which do not involve finiteness assumptions.

We feel that this presentation of Galois theory has some advantages. First of all, direct and simple proofs can be given of some of the interesting results, based solely on the normality of the field extensions under consideration. On the other hand, the properties of the topological Galois group play an essential role in many questions of Commutative Algebra and Algebraic Number Theory, so that the introduction of topological considerations in Galois Theory at the earliest possible moment may not be considered misplaced.

2. Prerequisites and Notation

We shall assume familiarity with the main properties of algebraic extensions, especially normality and separability; the most convenient references for our purposes are the texts by Bourbaki [1], Jacobson [4], Lang [5], and McCarthy [6] (in fact, all the background on algebraic extensions that we need here is contained in pp. 1–36 of [6]). We shall also assume familiarity with the most elementary properties of topological groups; particularly suitable references on this subject are the texts by Bourbaki [2] and [3].

We now introduce some notation. Let K be a field; we denote by Aut (K) the group of all automorphisms of K; for every subgroup H of Aut (K), we denote by $I(H)$ the field of invariants of H (that is, the fixed field of H). If K is a field, and L is a field extension of K, we denote by $G(L/K)$ the subgroup of Aut (L) consisting of all K-automorphisms of L.

An obvious fact, which will be used later, is the following: if K is a field, and if H is a subgroup of Aut (K), then

$$H \subseteq G(K/I(H)) \quad \text{and} \quad I(H) = I(G(K/I(H))).$$

3. The Finite Topology

In this section we consider a non-empty set X. We are concerned here with the description of a topology on the set of all mappings from X to X.

For every mapping σ from X to X and every finite subset E of X, we denote by $\langle\sigma; E\rangle$ the set of all mappings from X to X which agree pointwise with σ on E.

It is then easily verified that there exists a unique topology on the set of all mappings from X to X such that, for every mapping σ from X to X, a fundamental system of neighborhoods of σ is formed by the sets of the form $\langle\sigma; E\rangle$, where E is a finite subset of X.

This topology is said to be the *finite topology* on the set of all mappings from X to X. From now on we shall use the symbol $M(X)$ to denote the topological space formed by the set of all mappings from X to X with its finite topology.

Compactness of subsets of $M(X)$ will play an essential role in the sequel. For this reason, it is important for us to observe that $M(X)$ can be naturally identified with the product space $\prod_{x\in X} D_x$, where for each $x \in X$ we denote by D_x the discrete topological space having X as underlying set.

4. The Topological Galois Group

In this section we consider a field K and an algebraic field extension L of K.

Proposition 1. *$G(L/K)$ is a compact subset of $M(L)$.*

Proof. First of all, we verify that $G(L/K)$ is a closed subset of $M(L)$. Thus let $\sigma \in M(L)$, and suppose that σ is an adherent point of $G(L/K)$; we want to show that $\sigma \in G(L/K)$, or that σ is a K-automorphism of L; since L is algebraic over K, it suffices to show that σ is a K-endomorphism of L. To do this, let $x \in K$ and $y, z \in L$; let us denote by E the finite subset of L consisting of $x, y, z, y + z, yz$; we then know that $G(L/K) \cap \langle\sigma; E\rangle \neq \phi$; let us choose $\tau \in G(L/K) \cap \langle\sigma; E\rangle$, so that τ is a K-automorphism of L and $\sigma(u) = \tau(u)$ for every $u \in E$; but then $\sigma(x) = \tau(x) = x$, $\sigma(y + z) = \tau(y+z) = \tau(y) + \tau(z) = \sigma(y) + \sigma(z)$, and $\sigma(yz) = \tau(yz) = \tau(y)\tau(z) = \sigma(y)\sigma(z)$.

To conclude this argument, we only need to verify that $G(L/K)$ is contained in a compact subset of $M(L)$. For each $x \in L$, let X_x be the set of all roots in L of the minimal polynomial of x over K, so that S_x is a compact subset of the discrete topological space L; applying now the natural identification of $M(L)$ with a product space mentioned above, we deduce from the theorem of Tihonov that $\prod_{x\in L} S_x$ is a compact subset of $M(L)$; but if $\sigma \in G(L/K)$, then $\sigma(S_x) \subseteq S_x$ for every $x \in L$, which showa that $G(L/K) \subseteq \prod_{x\in L} S_x$. q.e.d.

We now introduce the symbol $N(L/K)$ to denote the collection of all subgroups of $G(L/K)$ of the form $G(L/Q)$, where Q is an intermediate field between K and L which is of finite degree over K. It is clear that $N(L/K) \neq \phi$, because $G(L/K) \in N(L/K)$; since $G(L/PQ) = G(L/P) \cap G(L/Q)$ for every two intermediate fields P and Q between K and L, we see that the intersection of every two members of $N(L/K)$ is a member of $N(L/K)$; and since $\sigma G(L/Q)\sigma^{-1} = G(L/\sigma(Q))$ for every $\sigma \in G(L/K)$ and every intermediate field Q between K and L, we see that all the conjugates of a member of $N(L/K)$ are members of $N(L/K)$.

It then follows from the elementary theory of topological groups that there exists a unique topology on $G(L/K)$ which is compatible with the group structure and with respect to which $N(L/K)$ is a fundamental system of neighborhoods of the neutral element. This topology is said to be the *Krull topology* of $G(L/K)$; whenever we consider $G(L/K)$ as a topological group, it will be understood that it is provided with its Krull topology.

PROPOSITION 2. *The Krull topology of $G(L/K)$ is the topology on $G(L/K)$ induced by that of $M(L)$.*

Proof. Let $\sigma \in G(L/K)$; we shall verify that the neighborhood filters of σ with respect to the two topologies in question are identical.

Consider first an intermediate field Q between K and L which is of finite degree over K; we can then write $Q = K(E)$, where E is a finite subset of L. It is evident that $G(L/K) \cap \langle\sigma; E\rangle \subseteq \sigma G(L/Q)$, hence we conclude that $\sigma G(L/Q)$ is a neighborhood of σ with respect to the topology on $G(L/K)$ induced by the topology of $M(L)$.

Now let E be a finite subset of L. If we let $Q = K(E)$, then Q is an intermediate field between K and L which is of finite degree over K. But it is clear that $\sigma G(L/Q) \subseteq G(L/K) \cap \langle\sigma; E\rangle$, which shows that $G(L/K) \cap \langle\sigma; E\rangle$ is a neighborhood of σ with respect to the Krull topology of $G(L/K)$. q.e.d.

PROPOSITION 3. *$G(L/K)$ is a compact topological group.*

Proof. This is clear from Propositions 1 and 2.

PROPOSITION 4. *If L is of finite degree over K, then $G(L/K)$ is discrete; and conversely, if L is Galois over K and $G(L/K)$ is discrete, then L is of finite degree over K.*

Proof. If L is of finite degree over K, then $G(L/L) \in N(L/K)$, so that $G(L/L)$ is open in $G(L/K)$; but $G(L/L)$ is a singleton, and we see that $G(L/K)$ is discrete.

Now assume that L is Galois over K and that $G(L/K)$ is discrete. Then there exists an intermediate field Q between K and L which is of finite degree over K and such that $G(L/Q)$ is a singleton; but then $G(L/Q) = G(L/L)$, so that $I(G(L/Q)) = I(G(L/L)) = L$; but L is Galois over Q, so that

$$Q = I(G(L/Q)) = L,$$

which shows that L is of finite degree over K. q.e.d.

PROPOSITION 5. *If L is normal over K, then a fundamental system of neighborhoods of the neutral element of $G(L/K)$ is formed by the subgroups of $G(L/K)$ of the form $G(L/Q)$, where Q is an intermediate field between K and L which is normal and of finite degree over K.*

Proof. In fact, if P is an intermediate field between K and L which is of finite degree over K, then there exists an intermediate field Q between P and L which is normal and of finite degree over K; since $P \subseteq Q$, we see that $G(L/Q) \subseteq G(L/P)$. q.e.d.

The next result, which already gives part of the Galois correspondence, is essential in what follows.

PROPOSITION 6. *If L is normal over K, and if H is a closed subgroup of $G(L/K)$, then $H = G(L/I(H))$.*

Proof. Since $I(H)$ is an intermediate field between K and L, we know that L is normal over $I(H)$; the preceding discussion also applies to the field $I(H)$ and its normal extension L; in particular, by Proposition 2, it is clear that the Krull ~~topology of $G(L/I(H))$ is induced by that of $G(L/K)$; in the argument that~~ follows, the topological group under consideration will be $G(L/I(H))$.

We already know that the inclusion $H \subseteq G(L/I(H))$ holds; it shows, in particular, that H is a closed subgroup of $G(L/I(\mathrm{H}))$. To show the opposite inclusion, take $\sigma \in G(L/I(H))$; to show that $\sigma \in H$, we only need to verify that σ is an adherent point of H (recall that the topology under consideration is the Krull topology of $G(L/I(H))$); and we shall do this by invoking Proposition 5; thus consider an intermediate field Q between $I(H)$ and L which is normal and of finite degree over $I(H)$; we need to show that $H \cap \sigma G(L/Q) \neq \phi$.

The normality of Q over $I(H)$ implies that $\psi(Q) = Q$ for every $\psi \in G(L/I(H))$; for every $\psi \in G(L/I(H))$, we denote by ψ^* the $I(H)$-automorphism of Q which ψ defines by restriction. We thus have the mapping $\psi \to \psi^*$ from $G(L/I(H))$ to $G(Q/I(H))$, which clearly is a homomorphism. Let us denote by H^* the image of H under this homorphism; thus H^* is a subgroup of $G(Q/I(H))$.

We claim that $H^* = G(Q/I(H))$: for suppose otherwise; then the finiteness of $G(Q/I(H))$ implies that Card $(H^*) <$ Card $(G(Q/I(H)))$; it is evident that $I(G(Q/I(H))) = I(H)$ and $I(H) \subseteq I(H^*) \subseteq Q$, we then deduce from a theorem of Artin (an elementary proof of which is given in [6], Theorem 3, p. 35; other proofs are given in [1], [4], and [5]) that $[Q{:}I(H^*)] =$ Card $(H^*) <$ Card $(G(Q/I(H))) = [Q{:}I(G(Q/I(H)))] = [Q{:}I(H)] = [Q{:}I(H^*)][I(H^*){:}I(H)]$, whence $[I(H^*){:}I(H)] > 1$ and $I(H) \subset I(H^*)$; now choose an $x \in I(H^*)$ such that $x \notin I(H)$; then $x \in Q$ and there exists a $\psi \in H$ such that $\psi(x) \neq x$; but $\psi^* \in H^*$, so that $\psi^*(x) = x$, which is impossible because $\psi(x) = \psi^*(x)$.

Since $\sigma \in G(L/I(H))$, we have $\sigma^* \in G(Q/I(H))$, so that $\sigma^* \in H^*$. Choose $\psi \in H$ so that $\sigma^* = \psi^*$; then $\sigma(x) = \sigma^*(x) = \psi^*(x) = \psi(x)$ for every $x \in Q$, which means that $(\sigma^{-1}\psi)(x) = \sigma^{-1}(\psi(x)) = x$ for every $x \in Q$; thus $\sigma^{-1}\psi \in G(L/Q)$, so that $\psi \in H \cap \sigma G(L/Q)$; it follows that $H \cap \sigma G(L/Q) \neq \phi$.

q.e.d

Remark. In the proof just given, essential use has been made of a theorem of Artin. This result of Artin is derived in [4] as a consequence of the theorem of Jacobson-Bourbaki, which seems to us to be the best approach, as the latter is also useful in the Galois theory of purely inseparable extensions of exponent one; this material is beautifully presented in [4].

PROPOSITION 7. *If L is normal over K, and if H is a subgroup of $G(L/K)$, then $G(L/I(H))$ is the closure of H in $G(L/K)$.*

Proof. Let F be the closure of H in $G(L/K)$. Then F is a closed subgroup of $G(L/K)$, and from Proposition 6 it follows that $F = G(L/I(F))$. But $H \subseteq F$, so that $I(H) \supseteq I(F)$ and $H \subseteq G(L/I(H)) \subseteq G(L/I(F)) = F$; but $G(L/I(H))$ is a compact, and hence closed, subset of $G(L/K)$, so that $G(L/I(H)) = F$. q.e.d.

PROPOSITION 8. *If L is normal over K, and if H is a subgroup of $G(L/K)$, then the following conditions are equivalent:*

(i) $I(H) = I(G(L/K))$.

(ii) *H is dense in $G(L/K)$.*

(iii) *if Q is an intermediate field between K and L which is of finite degree over K, then every K-automorphism of Q is the restriction of an element of H.*

Proof. The equivalence between (i) and (ii) follows trivially from Proposition 7.

We now prove that (ii) implies (iii); let Q be an intermediate field between K and L which is of finite degree over K, and let $\sigma \in G(Q/K)$; since L is normal over K, there exists $\tau \in G(L/K)$ which is an extension of σ; by (ii), we know that τ is an adherent point of H; thus $H \cap \tau G(L/Q) \neq \phi$, and it is clear that every element of $H \cap G(L/Q)$ is an extension of σ.

To prove that (iii) implies (ii), we must verify that every element of $G(L/K)$ is an adherent point of H; thus let $\psi \in G(L/K)$, and let Q be an intermediate field between K and L which is normal and of finite degree over K; the normality of Q over K implies that $\psi(Q) = Q$, which shows that ψ defines, by restriction, a K-automorphism ψ^* of Q; by (iii), there exists an element of H which is an extension of ψ^*; and since it is evident that every such element of H belongs to $H \cap \psi G(L/Q)$, we conclude that $H \cap \psi G(L/Q) \neq \phi$. q.e.d.

5. The Galois Correspondences

The general Galois correspondences can now be derived directly as easy consequences of the results of the preceding section.

THEOREM 1. *The following assertions are valid for every field K:*

(i) *if H is a subgroup of* Aut (K) *which is a compact subset of $M(K)$, then K is Galois over $I(H)$.*

(ii) *if E is a subfield of K over which K is Galois, then $G(K/E)$ is a subgroup of* Aut (K) *which is a compact subset of $M(K)$.*

(iii) *the mapping $H \to I(H)$ from the set of all subgroups of* Aut (K) *which are compact subsets of $M(K)$ to the set of all subfields of K over which K is Galois is bijective; the mapping $E \to G(K/E)$ from the set of all subfields of K over which K is Galois to the set of all subgroups of* Aut (K) *which are compact subsets of $M(K)$ is bijective; and these mappings are mutually inverse.*

Proof. In order to establish this result, we only need to verify the following statement: if H is a subgroup of Aut (K) which is a compact subset of $M(K)$, then K is algebraic over $I(H)$, and $H = G(K/I(H))$.

Let $x \in K$; identifying $M(K)$ with a product space in the way indicated earlier, the projections of H on the factor spaces are compact, and hence finite; in particular, the set $\{\sigma(x) \mid \sigma \in H\}$ is non-empty and finite; let us write $n =$ Card $(\{\sigma(x) \mid \sigma \in H\})$ and $\{\sigma(x) \mid \sigma \in H\} = \{x_1, \cdots, x_n\}$; we now consider the polynomial $f = (X - x_1)(X - x_2) \cdots (X - x_n) \in K[X]$; it is clear that f is invariant under every element of H, so that the coefficients of f belong to $I(H)$; since $f \neq 0$, and $f(x) = 0$, we conclude that x is algebraic over $I(H)$.

We then know, in particular, that K is normal over $I(H)$; it is evident that H is a closed subgroup of $G(K/I(H))$, hence we conclude that $H = G(K/I(H))$. q.e.d.

THEOREM 2. *If K is a field, and if L is a Galois field extension of K, then the mapping $H \to I(H)$ from the set of all closed subgroups of $G(L/K)$ to the set of all intermediate fields between K and L is bijective, the mapping $Q \to G(L/Q)$ from the set of all intermediate fields between K and L to the set of all closed subgroups of $G(L/K)$ is bijective, and these mappings are mutually inverse.*

Proof. It is only necessary to observe that the mappings involved are restrictions of the mutually inverse bijections associated to L as in Theorem 1. q.e.d.

Remark. Let us mention at this point that Theorem 2 is, in some sense, the best possible result on the correspondence between intermediate fields and subgroups. The reason for this is that the Galois group of a Galois field extension of infinite degree is known to be non-denumerable (this is not difficult to establish; consult the first exercise in the appendix of [1]); and from this fact one can easily deduce that such Galois groups admit non-closed subgroups.

6. Homomorphisms of Topological Galois Groups

Let us introduce at this point the following notational convention: if S and T are non-empty sets such that $S \subseteq T$, and if σ is a mapping from T to T such that $\sigma(S) \subseteq S$, then σ_S will denote the mapping from S to S defined by restriction of σ.

THEOREM 1. *If K is a field, if L is a field extension of K, if M is a field extension of L, and if L and M are normal over K, then we have:*

(i) *if $\sigma \in G(M/K)$, then $\sigma(L) = L$ and $\sigma_L \in G(L/K)$.*

(ii) *the mapping $\sigma \to \sigma_L$ from $G(M/K)$ to $G(L/K)$ is a surjective continuous homomorphism, $G(M/L)$ is its kernel, and it induces an isomorphism of topological groups from $G(M/K)/G(M/L)$ to $G(L/K)$.*

Proof. The first part is an obvious consequence of the normality of L over K.

Let Λ be the mapping $\sigma \to \sigma_L$ from $G(M/K)$ to $G(L/K)$; it is evident that

Λ is a homomorphism, and that $G(M/L)$ is its kernel; and the normality of M over K implies that Λ is surjective.

To verify that Λ is continuous, we only need to observe that, if Q is an intermediate field between K and L which is of finite degree over K, then $\Lambda(G(M/Q)) \subseteq G(L/Q)$.

The isomorphism from $G(M/K)/G(M/L)$ to $G(L/K)$ induced by Λ is continuous; since $G(M/K)/G(M/L)$ is compact and $G(L/K)$ is separated, it follows that it is also a homeomorphism. q.e.d.

THEOREM 2. *If K and L are fields which admit a common field extension, and if L is normal over $K \cap L$, then we have:*

(i) *KL is normal over K.*

(ii) *if $\sigma \in G(KL/K)$, then $\sigma(L) = L$ and $\sigma_L \in G(L/K \cap L)$.*

(iii) *the mapping $\sigma \rightarrow \sigma_L$ from $G(KL/K)$ to $G(L/K \cap L)$ is an isomorphism of topological groups.*

Proof. The first two parts are clear. Let Λ be the mapping $\sigma \rightarrow \sigma_L$ from $G(KL/K)$ to $G(L/K \cap L)$; it is clear that Λ is an injective homomorphism.

To show that Λ is continuous, we only need to observe that, if Q is an intermediate field between $K \cap L$ and L which is of finite degree over $K \cap L$, then KQ is an intermediate field between K and KL which is of finite degree over K, and $\Lambda(G(KL/KQ)) \subseteq G(L/Q)$.

We need to verify that Λ is surjective. Let H be the image of Λ; the continuity of Λ implies that H is a compact subgroup of $G(L/K \cap L)$; it then follows that H is a closed subgroup of $G(L/K \cap L)$, and thus $H = G(L/I(H))$.

We now claim that $I(H) = I(G(L/K \cap L))$. Indeed, the inclusion $I(H) \supseteq I(G(L/K \cap L))$ is evident. Now let $x \in I(H)$; then $x \in L$ and $\sigma_L(x) = x$ for every $\sigma \in G(KL/K)$, so that $x \in KL$ and $\sigma(x) = x$ for every $\sigma \in G(KL/K)$; since KL is normal over K, this means that x is purely inseparable over K; denoting by p the characteristic exponent of K, we have $x^{p^n} \in K$ for some $n \geqslant 0$; but then $x^{p^n} \in K \cap L$, so that x is purely inseparable over $K \cap L$, which implies that $x \in I(G(L/K \cap L))$.

We then have $H = G(L/I(H)) = G(L/I(G(L/K \cap L)) = G(L/K \cap L)$, which means that Λ is surjective.

Since Λ is continuous and bijective, $G(KL/K)$ is compact, and $G(L/K \cap L)$ is separated, it follows that Λ is also a homeomorphism. q.e.d.

THEOREM 3. *If K is a field, if L and M are field extensions of K which admit a common field extension, and if L and M are normal over K, then we have:*

(i) *LM is normal over K.*

(ii) *if $\sigma \in G(LM/K)$, then $\sigma(L) = L$ and $\sigma(M) = M$, and $\sigma_L \in G(L/K)$ and $\sigma_M \in G(M/K)$.*

(iii) *the mapping $\sigma \rightarrow (\sigma_L, \sigma_M)$ from $G(LM/K)$ to $G(L/K) \times G(M/K)$ is an injective continuous homomorphism.*

(iv) *if $K = L \cap M$, then the mapping $\sigma \rightarrow (\sigma_L, \sigma_M)$ from $G(LM/K)$ to $G(L/K) \times G(M/K)$ is an isomorphism of topological groups.*

Proof. The first two assertions are clear. Let Λ be the mapping $\sigma \rightarrow (\sigma_L, \sigma_M)$ from $G(\mathrm{LM/K})$ to $G(L/K) \times G(M/K)$; it is evident that Λ is an injective homomorphism.

To show the continuity of Λ, we only need to observe that, if P is an intermediate field between K and L and Q is an intermediate field between K and M, and if P and Q are of finite degree over K, then PQ is of finite degree over K, and $\Lambda(G(LM/PQ)) \subseteq G(L/P) \times G(M/Q)$.

In order to prove the last assertion, we assume that $K = L \cap M$. First of all, it is easy to see that Λ is surjective: for let $(\lambda, \delta) \in G(L/K) \times G(M/K)$; then $\lambda \in G(L/L \cap M)$ and $\delta \in G(M/L \cap M)$, and from Theorem 2 we see that $\lambda = \tau_L$ and $\delta = \psi_M$ for some $\tau \in G(LM/M)$ and $\psi \in G(LM/L)$; and if we put $\sigma = \tau\psi$, then it is clear that $\sigma \in G(LM/K)$ and $\Lambda(\sigma) = (\sigma_L, \sigma_M) = (\lambda, \delta)$. Thus Λ is a bijective continuous homomorphism from $G(LM/K)$ to $G(L/K) \times G(M/K)$; since $G(LM/K)$ is compact and $G(L/K) \times G(M/K)$ is separated, we see that Λ is also a homeomorphism. q.e.d.

THEOREM 4. *If K is a field, if L is a Galois field extension of K, and if V and W are closed subgroups of $G(L/K)$ such that $G(L/K) = VW$ and that $V \cap W$ is the trivial subgroup of $G(L/K)$, then $K = I(V) \cap I(W)$ and $L = I(V)I(W)$.*

Proof. First of all, we have $K = I(G(L/K)) = I(VW) = I(V) \cap I(W)$. And also, since V and W are closed subgroups of $G(L/K)$, we have $V \cap W = G(L/I(\mathrm{V})) \cap G(L/I(\mathrm{W})) = G(L/I(V)I(\mathrm{W}))$; since $V \cap W$ is the trivial subgroup of $G(L/K)$ and L is Galois over $I(V)I(\mathrm{W})$, we conclude that $L = I(V \cap \mathrm{W}) = I(G(L/I(\mathrm{V})I(\mathrm{W})) = \mathrm{I}(\mathrm{V})I(\mathrm{W})$. q.e.d.

FLORIDA ATLANTIC UNIVERSITY

REFERENCES

[1] N. BOURBAKI, Algèbre (Chapitres IV et V), Hermann, Paris, 1950.
[2] ———, Topologie Générale (Chapitres I et II), Hermann, Paris, 1951.
[3] ———, Topologie Générale (Chapitres III et IV), Hermann, Paris, 1951.
[4] N. JACOBSON, Lectures in Abstract Algebra, Vol. III. D. van Nostrand Col. Inc., Princeton, 1964.
[5] S. LANG, Algebra, Addison-Wesley Publishing Col., Reading, 1965.
[6] P. J. MCCARTHY, Algebraic Extensions of Fields, Blaisdell Publishing Co., Waltham, 1966.