


The Galois Connection between IntermediateFields(E,F) and Subgroups of $\text{Aut}(E,F)$

Christoph Schwarzweller 
Institute of Informatics
University of Gdańsk
Poland

Summary. In this article we establish the Galois connection between the intermediate fields of an extension E over F and the subgroups of the automorphism group $\text{Aut}(E, F)$. We show that if E is a finite Galois extension of F , then this connection induces a bijection between all intermediate fields of E and F and all subgroups of $\text{Aut}(E, F)$.

MSC: 12F10 68V20

Keywords: Galois connection; closed field; closed group; finite Galois extension

MML identifier: GALOIS_3, version: 8.1.15 5.100.1509

INTRODUCTION

This article is the fourth in a series of five articles formalizing the Fundamental Theorem of Galois Theory [5], [11], [9] using the Mizar formalism [2], [3], [7] as introduced in [15] (see [4] for similar development using Lean proof assistant [10]).

Following [8] we establish the Galois connection between the intermediate fields of an extension E over F and the subgroups of the automorphism group $\text{Aut}(E, F)$. This connection induces a bijection between the closed fields and closed groups, that is fields K with $\text{Fix}(E, \text{Aut}(E, K)) = K$ and groups G with $\text{Aut}(E, \text{Fix}(E, G)) = G$.

For E being a finite field extension of F it is easy to show that E is a Galois extension of F if and only if the closed fields are exactly the intermediate fields [16], [17].

To show that for a finite extension E of F the closed groups coincide with the subgroups of $\text{Aut}(E, F)$ we use group actions: $\text{Aut}(E, F)$ acts on the set R of roots of a polynomial $p \in F[X]$ in E . If E is generated by R the group $\text{Aut}(E, F)$ acts faithfully on R and is therefore of finite degree, because it can be embedded into the symmetric group over R . Together with Artin's lemma [1], [6] that for a finite subgroup G of $\text{Aut}(E)$ the field E is a finite Galois extension of $\text{Fix}(E, G)$ (where the order of $\text{Aut}(E, \text{Fix}(E, G))$ equals the degree of E over $\text{Fix}(E, G)$) this implies the desired result.

1. PRELIMINARIES

Let F be a field and E be an extension of F . The functor $\text{SubgroupsAut}(E)$ yielding a lattice is defined by the term

(Def. 1) $\mathbb{L}_{\text{Aut}(E, F)}$.

One can verify that every SubGroup of $\text{Aut}(E, F)$ is E -functional.

Let G be a SubGroup of $\text{Aut}(E, F)$. Note that the carrier of G is E -functional and every element of the carrier of G is F -fixing, additive, multiplicative, unity-preserving, and isomorphism.

Now we state the propositions:

- (1) Let us consider a field F , an extension E of F , an E -extending extension K of F , an element a of E , and an element b of K . Suppose $b = a$. Then $\text{RAdj}(F, \{a\}) = \text{RAdj}(F, \{b\})$.
- (2) Let us consider a field F , an extension E of F , an E -extending extension K of F , an F -algebraic element a of E , and an F -algebraic element b of K . Suppose $b = a$. Then $\text{FAdj}(F, \{a\}) = \text{FAdj}(F, \{b\})$.

Let us consider a field F , an extension E of F , a non empty, finite, F -algebraic subset T of E , and F -fixing automorphisms f, g of $\text{FAdj}(F, T)$. Now we state the propositions:

- (3) If for every element a of E such that $a \in T$ holds $f(a) = g(a)$, then $f = g$.
- (4) $f = g$ if and only if $f \upharpoonright T = g \upharpoonright T$. The theorem is a consequence of (3).
- (5) Let us consider a field F , and an F -finite extension E of F . Then E is F -simple if and only if $\text{IntermediateFields}(E, F)$ is finite.
- (6) Let us consider fields F_1, F_2 , an extension E_1 of F_1 , and an extension E_2 of F_2 . Suppose $E_1 \approx E_2$ and $F_1 \approx F_2$. Then $\text{Aut}(E_1, F_1) = \text{Aut}(E_2, F_2)$.

2. ON SYMMETRIC GROUPS AND GROUP ACTIONS

Let X be a set. The functor $\text{SymmetricGroup}(X)$ yielding a strict, constituted of functions multiplicative magma is defined by

(Def. 2) the carrier of $it = \text{permutations } X$ and for every elements x, y of it ,
 $x \cdot y = (x \text{ qua function}) \cdot y$.

We introduce the notation $\text{SymGr}(X)$ as a synonym of $\text{SymmetricGroup}(X)$.
 Now we state the proposition:

(7) Let us consider a set X . Then every element of $\text{SymGr}(X)$ is a permutation of X .

Let X be a set. One can check that $\text{SymGr}(X)$ is non empty, associative, and group-like. Now we state the propositions:

(8) Let us consider a set X . Then $\mathbf{1}_{\text{SymGr}(X)} = \text{id}_X$. The theorem is a consequence of (7).

(9) Let us consider a set X , and an element x of $\text{SymGr}(X)$. Then $x^{-1} = (x \text{ qua function})^{-1}$. The theorem is a consequence of (7) and (8).

Let X be a finite set. One can check that $\text{SymGr}(X)$ is finite.

Let G be a group and X be a set. Assume X is not empty.

An action of G on X is a function from (the carrier of G) $\times X$ into X defined by

(Def. 3) for every element a of X , $it(\mathbf{1}_G, a) = a$ and for every element a of X and for every elements g_1, g_2 of the carrier of G , $it(g_1, it(g_2, a)) = it(g_1 \cdot g_2, a)$.

Let A be an action of G on X . We say that A is faithful if and only if

(Def. 4) for every elements g_1, g_2 of G such that for every element x of X , $A(g_1, x) = A(g_2, x)$ holds $g_1 = g_2$.

We say that A is free if and only if

(Def. 5) for every element g of G such that there exists an element x of X such that $A(g, x) = x$ holds $g = \mathbf{1}_G$.

We say that A acts transitively on X if and only if

(Def. 6) for every elements a, b of X , there exists an element g of G such that $A(g, a) = b$.

We say that G acts on X if and only if

(Def. 7) there exists a function f from (the carrier of G) $\times X$ into X such that f is an action of G on X .

We say that G acts transitively on X if and only if

(Def. 8) there exists an action A of G on X such that A acts transitively on X .

Let X be a non empty set. The functor $\text{trivialAction}(G, X)$ yielding an action of G on X is defined by

(Def. 9) for every element a of X and for every element g of G , $it(g, a) = a$.

Let G be a non trivial group. Observe that $\text{trivialAction}(G, X)$ is non faithful.

Let G be a trivial group. One can check that $\text{trivialAction}(G, X)$ is faithful.

Let G be a group. The functors: $\text{regularAction}(G)$ and $\text{conjugationAction}(G)$ yielding actions of G on the carrier of G are defined by conditions

(Def. 10) for every elements g_1, g_2 of G , $\text{regularAction}(G)(g_1, g_2) = g_1 \cdot g_2$,

(Def. 11) for every elements g_1, g_2 of G , $\text{conjugationAction}(G)(g_1, g_2) = g_1 \cdot g_2 \cdot (g_1^{-1})$,

respectively. Let us note that $\text{regularAction}(G)$ is free.

Let X be a non empty set, A be an action of G on X , and g be an element of G . The functor $\text{apply}(A, g)$ yielding a permutation of X is defined by

(Def. 12) for every element a of X , $it(a) = A(g, a)$.

The functor $\text{canHom}(A)$ yielding a function from G into $\text{SymGr}(X)$ is defined by

(Def. 13) for every element g of G , $it(g) = \text{apply}(A, g)$.

Now we state the proposition:

(10) Let us consider a group G , a non empty set X , an action A of G on X , and elements g_1, g_2 of G . Then $\text{apply}(A, g_1 \cdot g_2) = \text{apply}(A, g_1) \cdot \text{apply}(A, g_2)$.

Let G be a group, X be a non empty set, and A be an action of G on X . Let us observe that $\text{canHom}(A)$ is multiplicative. Now we state the propositions:

(11) Let us consider a group G , a non empty set X , and an action A of G on X . Then $\text{canHom}(A)$ is a homomorphism from G to $\text{SymGr}(X)$.

(12) Let us consider a group G , and a non empty set X . Then G acts on X if and only if there exists a function h from G into $\text{SymGr}(X)$ such that h is multiplicative. The theorem is a consequence of (8).

Let us consider a group G , a non empty set X , and an action A of G on X . Now we state the propositions:

(13) $\text{Ker canHom}(A) = \{\mathbf{1}\}_G$ if and only if for every element g of G such that for every element x of X , $A(g, x) = x$ holds $g = \mathbf{1}_G$. The theorem is a consequence of (8).

(14) A is faithful if and only if $\text{canHom}(A)$ is one-to-one.

(15) A is faithful if and only if for every element g of G such that for every element x of X , $A(g, x) = x$ holds $g = \mathbf{1}_G$. The theorem is a consequence of (14) and (13).

Let G be a group and X be a non empty set. Note that every action of G on X which is free is also faithful. Now we state the proposition:

- (16) Let us consider a group G . Then there exists a subgroup H of SymGr (the carrier of G) such that H and G are isomorphic. The theorem is a consequence of (14).

3. THE GALOIS CONNECTION BETWEEN INTERMEDIATE FIELDS AND SUBGROUPS OF $\text{AUT}(E,F)$

Let F be a field and E be an extension of F . The functor Ψ_E yielding a function from $\text{Poset}(\text{IntermediateFields}(E))$ into $\text{Poset}(\text{SubgroupsAut}(E))$ is defined by

- (Def. 14) for every intermediate field K of E, F , $it(K) = \text{Aut}(E, K)$.

The functor Φ_E yielding a function from $\text{Poset}(\text{SubgroupsAut}(E))$ into $\text{Poset}(\text{IntermediateFields}(E))$ is defined by

- (Def. 15) for every SubGroup G of $\text{Aut}(E, F)$, $it(G) = \text{Fix}(E, G)$.

Now we state the propositions:

- (17) Let us consider a field F , an extension E of F , and an intermediate field K of E, F . Then $\Phi_E(\Psi_E K) = \text{Fix}(E, \text{Aut}(E, K))$.
- (18) Let us consider a field F , an extension E of F , and a SubGroup G of $\text{Aut}(E, F)$. Then $\Psi_E(\Phi_E G) = \text{Aut}(E, \text{Fix}(E, G))$.

Let F be a field and E be an extension of F . The functor $\text{GalCon}(E)$ yielding a connection between $\text{Poset}(\text{IntermediateFields}(E))$ and $\text{Poset}(\text{SubgroupsAut}(E))$ is defined by the term

- (Def. 16) $\langle \Psi_E, \Phi_E \rangle$.

Note that Ψ_E is antitone and Φ_E is antitone and $\text{GalCon}(E)$ is co-Galois.

The functor $\text{ClosedFields}(E)$ yielding a subset of $\text{Poset}(\text{IntermediateFields}(E))$ is defined by the term

- (Def. 17) $\text{Closed}(\Phi_E)$.

The functor $\text{ClosedGroups}(E)$ yielding a subset of $\text{Poset}(\text{SubgroupsAut}(E))$ is defined by the term

- (Def. 18) $\text{Closed}(\Psi_E)$.

One can check that $\text{ClosedFields}(E)$ is non empty and $(\text{ClosedGroups}(E))$ -bijective and $\text{ClosedGroups}(E)$ is non empty and $(\text{ClosedFields}(E))$ -bijective.

Let us consider a field F and an extension E of F . Now we state the propositions:

- (19) (i) $\Psi_E \upharpoonright \text{ClosedFields}(E)$ is a bijection of $\text{ClosedFields}(E)$, $\text{ClosedGroups}(E)$, and

- (ii) $(\Psi_E \upharpoonright \text{ClosedFields}(E))^{-1} = \Phi_E \upharpoonright \text{ClosedGroups}(E)$.
- (20) (i) $\Phi_E \upharpoonright \text{ClosedGroups}(E)$ is a bijection of $\text{ClosedGroups}(E)$, $\text{ClosedFields}(E)$, and
- (ii) $(\Phi_E \upharpoonright \text{ClosedGroups}(E))^{-1} = \Psi_E \upharpoonright \text{ClosedFields}(E)$.

Let us consider a field F , an extension E of F , and an intermediate field K of E , F . Now we state the propositions:

- (21) $K \in \text{ClosedFields}(E)$ if and only if $\Phi_E(\Psi_E K) = K$.
- (22) $K \in \text{ClosedFields}(E)$ if and only if $\text{Fix}(E, \text{Aut}(E, K)) = K$. The theorem is a consequence of (21) and (32).

Let us consider a field F , an extension E of F , and a SubGroup G of $\text{Aut}(E, F)$. Now we state the propositions:

- (23) $G \in \text{ClosedGroups}(E)$ if and only if $\Psi_E(\Phi_E G) = G$.
- (24) $G \in \text{ClosedGroups}(E)$ if and only if $\text{Aut}(E, \text{Fix}(E, G)) = G$. The theorem is a consequence of (23) and (18).
- (25) Let us consider a field F , and an extension E of F . Then E is F -Galois if and only if the double loop structure of $F \in \text{ClosedFields}(E)$. The theorem is a consequence of (6), (21), and (32).

Let us consider a field F and an F -finite extension E of F . Now we state the propositions:

- (26) $\text{ClosedFields}(E) = \text{IntermediateFields}(E, F)$ if and only if the double loop structure of $F \in \text{ClosedFields}(E)$. The theorem is a consequence of (25) and (22).
- (27) E is a Galois extension of F if and only if $\text{ClosedFields}(E) = \text{IntermediateFields}(E, F)$. The theorem is a consequence of (25) and (26).

4. THE ORDER OF $\text{AUT}(E, F)$

Let F be a field and E be an extension of F . The functor $\text{ActionAut}(E, F)$ yielding an action of $\text{Aut}(E, F)$ on the carrier of E is defined by

- (Def. 19) for every element a of E and for every element g of the carrier of $\text{Aut}(E, F)$, $it(g, a) = g(a)$.

Let p be a non zero element of the carrier of Polynom-Ring F . Assume $\text{Roots}(E, p) \neq \emptyset$. The functor $\text{ActionRoots}(E, p)$ yielding an action of $\text{Aut}(E, F)$ on $\text{Roots}(E, p)$ is defined by the term

- (Def. 20) $\text{ActionAut}(E, F) \upharpoonright ((\text{the carrier of } \text{Aut}(E, F)) \times \text{Roots}(E, p))$.

Now we state the propositions:

- (28) Let us consider a field F , an extension E of F , and a non zero element p of the carrier of Polynom-Ring F . Suppose $\text{Roots}(E, p) \neq \emptyset$. Then $\text{Aut}(E, F)$ acts on $\text{Roots}(E, p)$.
- (29) Let us consider a field F , an irreducible element p of the carrier of Polynom-Ring F , and a splitting field E of p . Then $\text{Aut}(E, F)$ acts transitively on $\text{Roots}(E, p)$.

Let us consider a field F , an extension E of F , and a non zero element p of the carrier of Polynom-Ring F . Now we state the propositions:

- (30) If $\text{Roots}(E, p) \neq \emptyset$ and $E \approx \text{FAdj}(F, \text{Roots}(E, p))$, then $\text{ActionRoots}(E, p)$ is faithful. The theorem is a consequence of (8), (3), and (14).
- (31) Suppose $\text{Roots}(E, p) \neq \emptyset$ and $E \approx \text{FAdj}(F, \text{Roots}(E, p))$. Then there exists a homomorphism f from $\text{Aut}(E, F)$ to $\text{SymGr}(\text{Roots}(E, p))$ such that f is one-to-one. The theorem is a consequence of (30) and (14).
- (32) Suppose $\text{Roots}(E, p) \neq \emptyset$ and $E \approx \text{FAdj}(F, \text{Roots}(E, p))$. Then there exists a subgroup H of $\text{SymGr}(\text{Roots}(E, p))$ such that $\text{Aut}(E, F)$ and H are isomorphic. The theorem is a consequence of (31).

Let F be a field and E be an F -finite extension of F . Let us note that $\text{Aut}(E, F)$ is finite. Let K be an intermediate field of E, F . One can verify that $\text{Aut}(E, K)$ is finite and every F -finite, F -separable extension of F is F -simple. Let us consider a field F and an F -finite extension E of F . Now we state the propositions:

- (33) E is a Galois extension of F if and only if $\text{deg}(E, F) = \text{order Aut}(E, F)$.
- (34) $\text{order Aut}(E, F) \mid \text{deg}(E, F)$. The theorem is a consequence of (33).

Let us consider a field E and a finite SubGroup G of $\text{Aut}(E)$. Now we state the propositions:

- (35) (i) $G = \text{Aut}(E, \text{Fix}(E, G))$, and
(ii) $\text{order Aut}(E, \text{Fix}(E, G)) = \text{deg}(\text{FieldExt}(E, \text{Fix}(E, G)), \text{Fix}(E, G))$.

PROOF: Set $F = \text{Fix}(E_1, G)$. Reconsider $E = E_1$ as an extension of F . There exists an element a of E such that for every element b of E , $\text{deg}(\text{FAdj}(F, \{b\}), F) \leq \text{deg}(\text{FAdj}(F, \{a\}), F)$. Consider a being an element of E such that for every element b of E , $\text{deg}(\text{FAdj}(F, \{b\}), F) \leq \text{deg}(\text{FAdj}(F, \{a\}), F)$. $E \approx \text{FAdj}(F, \{a\})$ by [14, (31)], [12, (7)], [13, (4)], [14, (30), (8)]. $\underline{\text{Aut}(E, F)} \leq \text{deg}(E, F)$. \square

- (36) E is a $\text{Fix}(E, G)$ -finite Galois extension of $\text{Fix}(E, G)$. The theorem is a consequence of (35).
- (37) Let us consider a field F , and an F -finite extension E of F . Then $\text{ClosedGroups}(E) = \text{SubGr Aut}(E, F)$. The theorem is a consequence of (35) and (24).

REFERENCES

- [1] Emil Artin. *Galois Theory: Lectures Delivered at the University of Notre Dame*, volume 2 of *Notre Dame Mathematical Lectures*. Dover Publications, Mineola, NY, 1998. ISBN 9780486623429.
- [2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Kornilowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.
- [3] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Kornilowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.
- [4] Thomas Browning and Patrick Lutz. Formalizing Galois theory. *Experimental Mathematics*, 31(2):413–424, 2022. doi:10.1080/10586458.2021.1986176.
- [5] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Wiley and Sons, third edition, 2004.
- [6] Rod Gow and Rachel Quinlan. Galois theory and linear algebra. *Linear Algebra and Its Applications*, 430(7):1778–1789, 2009. doi:10.1016/j.laa.2008.06.030.
- [7] Adam Grabowski, Artur Kornilowicz, and Christoph Schwarzweller. On algebraic hierarchies in mathematical repository of Mizar. In M. Ganzha, L. Maciaszek, and M. Paprzycki, editors, *Proceedings of the 2016 Federated Conference on Computer Science and Information Systems (FedCSIS)*, volume 8 of *Annals of Computer Science and Information Systems*, pages 363–371, 2016. doi:10.15439/2016F520.
- [8] I. Martin Isaacs. *Algebra: A Graduate Course*. Wadsworth Inc., 1994.
- [9] Serge Lang. *Algebra (Revised Third Edition)*. Springer Verlag, 2002.
- [10] Leonardo de Moura and Sebastian Ullrich. The Lean 4 theorem prover and programming language. In *Automated Deduction – CADE 28: 28th International Conference on Automated Deduction, Virtual Event, July 12–15, 2021, Proceedings*, pages 625–635, Berlin, Heidelberg, 2021. Springer-Verlag. doi:10.1007/978-3-030-79876-5_37.
- [11] Knut Radbruch. *Algebra I*. Lecture Notes, University of Kaiserslautern, Germany, 1991.
- [12] Christoph Schwarzweller. Field extensions and Kronecker’s construction. *Formalized Mathematics*, 27(3):229–235, 2019. doi:10.2478/forma-2019-0022.
- [13] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzeweller. Simple extensions. *Formalized Mathematics*, 31(1):287–298, 2023. doi:10.2478/forma-2023-0023.
- [14] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzeweller. Algebraic extensions. *Formalized Mathematics*, 29(1):39–48, 2021. doi:10.2478/forma-2021-0004.
- [15] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzeweller. Introduction to Galois theory. *Formalized Mathematics*, 33(1):175–183, 2025. doi:10.2478/forma-2025-0014.
- [16] Ian Stewart. *Galois Theory*. Chapman and Hall/CRC, fourth edition, 2015.
- [17] Steven H. Weintraub. *Galois Theory*. Springer-Verlag, second edition, 2009.

Received July 9, 2025, Accepted January 24, 2026
