FORMALIZED MATHEMATICS
Vol. **34**, No. **1**, pp. 15–22, **2026**
DOI: 10.2478/forma-2026-0002
e-ISSN: 1898–9934

Paradigm
reference-global.com

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

MSC: 68V20

Keywords:

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 [6], [4], [5] using the Mizar formalism [1], [2], [3].

Following [4] we establish the Galois connection between the intermediate fields of an extension E over F and the subgroups of the automorphism group $\mathrm{Aut}(E, F)$. This connection induces a bijection between the closed fields and closed groups, that is fields K with $\mathrm{Fix}(E,\mathrm{Aut}(E, K)) = K$ and groups G with $\mathrm{Aut}(E,\mathrm{Fix}(E, G)) = G$.

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.

To show that for a finite extension E of F the closed groups coincide with the subgroups of $\mathrm{Aut}(E, F)$ we use group actions: $\mathrm{Aut}(E, F)$ acts on the set R of roots of a polynomial $p \in F[X]$ in E. If E is generated by R the group $\mathrm{Aut}(E, F)$ 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 theorem that for a finite subgroup G of $\mathrm{Aut}(E)$ the field E is a finite Galois extension of $\mathrm{Fix}(E, G)$ (where the order of $\mathrm{Aut}(E,\mathrm{Fix}(E, G))$ equals the degree of E over $\mathrm{Fix}(E, G)$) this implies the desired result.

1. Preliminaries

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

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

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

Let G be a SubGroup of $\mathrm{Aut}(E, F)$. 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 $\mathrm{RAdj}(F, \{a\}) = \mathrm{RAdj}(F, \{b\})$.

(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 $\mathrm{FAdj}(F, \{a\}) = \mathrm{FAdj}(F, \{b\})$.

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 $\mathrm{FAdj}(F, T)$. 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 $f{\restriction}T = g{\restriction}T$. The theorem is a consequence of (3).

Now we state the propositions:

(5) Let us consider a field F, and an F-finite extension E of F. Then E is F-simple if and only if $\mathrm{IntermediateFields}(E, F)$ 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 $\mathrm{Aut}(E_1, F_1) = \mathrm{Aut}(E_2, F_2)$.

2. On Symmetric Groups and Group Actions

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

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

We introduce the notation SymGr(X) as a synonym of SymmetricGroup(X).

Now we state the proposition:

(7) Let us consider a set X. Then every element of SymGr(X) is a permutation of X.

Let X be a set. One can check that SymGr(X) is non empty, associative, and group-like.

Now we state the propositions:

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

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

Let X be a finite set. One can check that 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 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 trivialAction(G, X) is non faithful.

Let G be a trivial group. One can check that trivialAction(G, X) is faithful.

Let G be a group. The functors: regularAction(G) and 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, regularAction$(G)(g_1, g_2) = g_1 \cdot g_2$,

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

respectively. Let us note that 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 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 $A \overset{\text{canHom}}{\hookrightarrow}$ Polynom-Ring A yielding a function from G into 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 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. Observe that $A \overset{\text{canHom}}{\hookrightarrow}$ Polynom-Ring 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 $A \overset{\text{canHom}}{\hookrightarrow}$ Polynom-Ring A is a homomorphism from G to 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 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) Ker$(A \overset{\text{canHom}}{\hookrightarrow}$ Polynom-Ring $A) = \{\mathbf{1}\}_G$ 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 $A \overset{\text{canHom}}{\hookrightarrow}$ Polynom-Ring 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. Let us 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 SymmetricGroup((the 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 Aut(E,F)

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

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

The functor $\Phi(E)$ yielding a function from Poset(SubgroupsAut(E)) into Poset(Intermedia is defined by

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

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 $(\Phi(E))((\Psi_E)(K)) = \mathrm{Fix}(E, \mathrm{Aut}(E, K))$.

(18) Let us consider a field F, an extension E of F, and a SubGroup G of $\mathrm{Aut}(E, F)$. Then $(\Psi_E)((\Phi(E))(G)) = \mathrm{Aut}(E, (\mathrm{Fix}(E, G)))$.

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

(Def. 16) $\langle \Psi_E, \Phi(E) \rangle$.

Note that Ψ_E is antitone and $\Phi(E)$ is antitone and GalCon(E) is co-Galois.

The functor ClosedFields(E) yielding a subset of Poset(IntermediateFields(E)) is defined by the term

(Def. 17) Closed($\Phi(E)$).

The functor ClosedGroups(E) yielding a subset of Poset(SubgroupsAut(E)) is defined by the term

(Def. 18) Closed(Ψ_E).

One can check that ClosedFields(E) is non empty and (ClosedGroups(E))-bijective and ClosedGroups(E) is non empty and (ClosedFields(E))-bijective.

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

(19) (i) $\Psi_E \restriction$ ClosedFields(E) is a bijection of ClosedFields(E), ClosedGroups(E), and

(ii) $(\Psi_E \restriction \text{ClosedFields}(E))^{-1} = \Phi(E) \restriction \text{ClosedGroups}(E)$.

(20) (i) $\Phi(E) \restriction$ ClosedGroups(E) is a bijection of ClosedGroups(E), ClosedFields(E), and

(ii) $(\Phi(E) \restriction \text{ClosedGroups}(E))^{-1} = \Psi_E \restriction \text{ClosedFields}(E)$.

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) $K \in$ ClosedFields(E) if and only if $(\Phi(E))((\Psi_E)(K)) = K$.

(22) $K \in$ 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 Aut(E, F). Now we state the propositions:

(23) $G \in$ ClosedGroups(E) if and only if $(\Psi_E)((\Phi(E))(G)) = G$.

(24) $G \in$ ClosedGroups(E) if and only if $\text{Aut}(E, (\text{Fix}(E, G))) = G$. The theorem is a consequence of (23) and (18).

Now we state the proposition:

(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 $F \in$ 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) ClosedFields(E) = IntermediateFields(E, F) if and only if the double loop structure of $F \in$ ClosedFields(E). The theorem is a consequence of (25) and (22).

(27) E is a Galois extension of F if and only if ClosedFields(E) = IntermediateFields(E, The theorem is a consequence of (25) and (26).

4. The Order of Aut(E,F)

Let F be a field and E be an extension of F. The functor Action-Aut(E, F) yielding an action of 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 $\mathrm{Aut}(E,F)$, $it(g,a)=g(a)$.

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

(Def. 20) Action-Aut$(E,F)\restriction$((the carrier of $\mathrm{Aut}(E,F)$) $\times\,\mathrm{Roots}(E,p)$).

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 $\mathrm{Roots}(E,p)\neq\emptyset$. Then $\mathrm{Aut}(E,F)$ acts on $\mathrm{Roots}(E,p)$.

(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 $\mathrm{Aut}(E,F)$ acts transitively on $\mathrm{Roots}(E,p)$.

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 $\mathrm{Roots}(E,p)\neq\emptyset$ and $E\approx\mathrm{FAdj}(F,\mathrm{Roots}(E,p))$, then Action-Roots$(E,p)$ is faithful. The theorem is a consequence of (8), (3), and (14).

(31) Suppose $\mathrm{Roots}(E,p)\neq\emptyset$ and $E\approx\mathrm{FAdj}(F,\mathrm{Roots}(E,p))$. Then there exists a homomorphism f from $\mathrm{Aut}(E,F)$ to $\mathrm{SymGr}(\mathrm{Roots}(E,p))$ such that f is one-to-one. The theorem is a consequence of (30) and (14).

(32) Suppose $\mathrm{Roots}(E,p)\neq\emptyset$ and $E\approx\mathrm{FAdj}(F,\mathrm{Roots}(E,p))$. Then there exists a subgroup H of $\mathrm{SymGr}(\mathrm{Roots}(E,p))$ such that $\mathrm{Aut}(E,F)$ 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. Note that $\mathrm{Aut}(E,F)$ is finite.

Let K be an intermediate field of E, F. Let us observe that $\mathrm{Aut}(E,K)$ 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 $\deg(E,F)=\mathrm{order}\,\mathrm{Aut}(E,F)$.

(34) $\mathrm{order}\,\mathrm{Aut}(E,F)\mid\deg(E,F)$. The theorem is a consequence of (33).

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

(35) (i) $G=\mathrm{Aut}(E,(\mathrm{Fix}(E,G)))$, and

(ii) $\mathrm{order}\,\mathrm{Aut}(E,(\mathrm{Fix}(E,G)))=\deg(\mathrm{FieldExt}(E,\mathrm{Fix}(E,G)),\mathrm{Fix}(E,G))$.

Proof: Set $F=\mathrm{Fix}(E_1,G)$. Reconsider $E=E_1$ as an extension of F. There exists an element a of E such that for every element b of E,

$\deg(\mathrm{FAdj}(F,\{b\}),F) \leqslant \deg(\mathrm{FAdj}(F,\{a\}),F)$. Consider a being an element of E such that for every element b of E, $\deg(\mathrm{FAdj}(F,\{b\}),F) \leqslant \deg(\mathrm{FAdj}(F,\{a\}),F)$. $E \approx \mathrm{FAdj}(F,\{a\})$ by [9, (31)], [7, (7)], [8, (4)], [9, (30), (8)]. $\overline{\overline{\mathrm{Aut}(E,F)}} \leqslant \deg(E,F)$. □

(36) E is an $(\mathrm{Fix}(E,G))$-finite Galois extension of $\mathrm{Fix}(E,G)$. The theorem is a consequence of (35).

Now we state the proposition:

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

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, 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.

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, 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.

[3] Adam Grabowski, Artur Korniłowicz, 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.

[4] I. Martin Isaacs. *Algebra: A Graduate Course.* Wadsworth Inc., 1994.

[5] Serge Lang. *Algebra (Revised Third Edition).* Springer Verlag, 2002.

[6] Knut Radbruch. *Algebra I.* Lecture Notes, University of Kaiserslautern, Germany, 1991.

[7] Christoph Schwarzweller. Field extensions and Kronecker's construction. *Formalized Mathematics*, 27(**3**):229–235, 2019. doi:10.2478/forma-2019-0022.

[8] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzweller. Simple extensions. *Formalized Mathematics*, 31(1):287–298, 2023. doi:10.2478/forma-2023-0023.

[9] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzweller. Algebraic extensions. *Formalized Mathematics*, 29(**1**):39–48, 2021. doi:10.2478/forma-2021-0004.

Received January 24, 2026