


The Fundamental Theorem of Galois Theory

Christoph Schwarzweller 
Institute of Informatics
University of Gdańsk
Poland

Summary. In this article we prove the Fundamental Theorem of Galois Theory using the Mizar formalism.

MSC: 12F10 68V20

Keywords: finite Galois extension; fundamental theorem of Galois theory

MML identifier: GALOIS_4, version: 8.1.15 5.100.1509

INTRODUCTION

This article is the last in a series of five articles formalizing the Fundamental Theorem of Galois Theory [8], [9] using the Mizar formalism [2], [3], [6], as initiated in [15] (see [4] for similar development using Lean proof assistant [10]).

We first show some necessary properties of normal subgroups and normal extensions; then we state and prove that for a finite Galois extension E of F (see also [7], [11]):

1. the functions φ mapping intermediate fields K to $\text{Aut}(E, K)$ and ϕ mapping subgroups G of $\text{Aut}(E, F)$ to $\text{Fix}(E, G)$ are inverse bijections respecting subfields and subgroups in the sense that K_1 is a subfield of K_2 if and only if $\varphi(K_2)$ is a subgroup of $\varphi(K_1)$ and G_1 is a subgroup of G_2 if and only if $\phi(G_2)$ is a subfield of $\phi(G_1)$.
2. for all intermediate fields K the degree of E over K equals the order of $\text{Aut}(E, K)$ and the degree of K over F equals the index of $\text{Aut}(E, K)$ in $\text{Aut}(E, F)$.

3. for all intermediate fields K_1 and K_2 we have that K_1 and K_2 are isomorphic over F if and only if $\text{Aut}(E, K_1)$ and $\text{Aut}(E, K_2)$ are conjugated in $\text{Aut}(E, F)$.
4. for all intermediate fields K we have that E is a Galois extension of K and that K is a Galois extension of F if and only if K is a normal extension of F .
5. an intermediate field K is a normal extension of F if and only if for all F -fixing automorphisms $f \in \text{Aut}(E, F)$ we have $f(K) = K$ if and only if $\text{Aut}(E, K)$ is a normal subgroup of $\text{Aut}(E, F)$. In this case $\text{Aut}(K, F)$ and $\text{Aut}(E, F)/\text{Aut}(E, K)$ are isomorphic [1], [5].

We also prove that for finite Galois extensions the functions φ and ϕ respect the lattice operations \wedge and \vee : for subsets M of intermediate fields and subsets N of $\text{Aut}(E, F)$ we have:

6. $\text{Aut}(E, \vee M) = \wedge\{\varphi(K) \mid K \in M\} = \wedge\{\text{Aut}(E, K) \mid K \in M\}$ and $\text{Aut}(E, \wedge M) = \vee\{\varphi(K) \mid K \in M\} = \vee\{\text{Aut}(E, K) \mid K \in M\}$.
7. $\text{Fix}(E, \vee N) = \wedge\{\phi(G) \mid G \in N\} = \wedge\{\text{Fix}(E, G) \mid G \in N\}$ and $\text{Fix}(E, \wedge N) = \vee\{\phi(G) \mid G \in N\} = \vee\{\text{Fix}(E, G) \mid G \in N\}$.

1. ON NORMAL SUBGROUPS

Now we state the proposition:

- (1) Let us consider a group G , and a subgroup H of G . Then H is normal if and only if for every elements g, h of G such that $h \in H$ holds $h^g \in H$.

Let us consider a group G and a strict subgroup H of G . Now we state the propositions:

- (2) H is normal if and only if for every element g of G , $H^g = H$. The theorem is a consequence of (1).
- (3) H is normal if and only if there exists a group G_1 and there exists a homomorphism f from G to G_1 such that $\text{Ker } f = H$.

Let G, H be groups. Assume H is a subgroup of G . The functor $\text{Index}(H, G)$ yielding a cardinal number is defined by

(Def. 1) there exists a subgroup H_1 of G such that $H_1 = H$ and $it = |\bullet : H_1|$.

Let G, H_1, H_2 be groups. We say that H_1, H_2 are conjugated in G if and only if

(Def. 2) there exist subgroups H_3, H_4 of G such that $H_3 = H_1$ and $H_4 = H_2$ and H_3 and H_4 are conjugated.

2. ON NORMAL EXTENSIONS

Let F be a field, E be an extension of F , h be a homomorphism of E , and K be an intermediate field of E, F . The functor $\text{rng}(h, K)$ yielding a subset of E is defined by the term

(Def. 3) $\text{rng}(h \upharpoonright (\text{the carrier of } K))$.

One can verify that $\text{rng}(h, K)$ is inducing subfield.

The functor $h^\circ K$ yielding a subfield of E is defined by the term

(Def. 4) $\text{InducedSubfield}(\text{rng}(h, K))$.

Let f be an F -fixing automorphism of E . Let us note that $f^\circ K$ is F -extending. Now we state the propositions:

- (4) Let us consider a field F , an F -finite extension E of F , an intermediate field K of E, F , and an F -fixing automorphism f of E . Suppose K is F -normal. Then $f \upharpoonright (\text{the carrier of } K)$ is an F -fixing automorphism of K .
- (5) Let us consider a field F , an F -finite extension E of F , and an intermediate field K of E, F . Suppose K is F -normal. Let us consider F -fixing automorphisms f_1, f_2 of E . Then $f_1 \cdot f_2 \upharpoonright (\text{the carrier of } K) = (f_1 \upharpoonright (\text{the carrier of } K)) \cdot (f_2 \upharpoonright (\text{the carrier of } K))$. The theorem is a consequence of (4).
- (6) Let us consider a field F , an F -finite extension E of F , and an intermediate field K of E, F . Suppose K is F -normal. Let us consider an element f of the carrier of $\text{Aut}(E, F)$. Then $f^\circ K = K$. The theorem is a consequence of (4).
- (7) Let us consider a field F , an F -finite extension E of F , and an intermediate field K of E, F . Suppose K is F -normal. Then $\text{Fix}(K, \text{Aut}(K, F))$ is a subfield of $\text{Fix}(E, \text{Aut}(E, F))$. The theorem is a consequence of (4).
- (8) Let us consider a field F , an F -normal extension E of F , and an F -algebraic element a of E . Suppose $E \approx \text{FAdj}(F, \{a\})$. Then E is a splitting field of $\text{MinPoly}(a, F)$.
- (9) Let us consider a field F , an F -finite Galois extension E of F , intermediate fields K_1, K_2 of E, F , and a function h from K_1 into K_2 . Suppose h is F -fixing and isomorphism. Then there exists an F -fixing automorphism f of E such that $f \upharpoonright K_1 = h$.

PROOF: Consider a being an element of E such that $E \approx \text{FAdj}(F, \{a\})$. Set $p = \text{MinPoly}(a, F)$. Reconsider $p_1 = p$ as an element of the carrier of $\text{Polynom-Ring } K_1$. E is splitting field of p and K_1 -extending. Reconsider $L = E$ as a splitting field of p_1 . Reconsider $K_3 = K_2$ as a K_1 -isomorphic, K_1 -homomorphic field. Reconsider $h_1 = h$ as an isomorphism between K_1 and K_3 . $\text{PolyHom}(h_1)(p_1) = p_1$. L is a splitting field of $\text{PolyHom}(h_1)(p_1)$

by [14, (4)], [12, (7)], (8), [13, (29)]. Consider f being a function from L into L such that f is h_1 -extending and isomorphism. \square

- (10) Let us consider a field F , an extension E of F , an intermediate field K of E , F , and an element f of the carrier of $\text{Aut}(E)$. Then
- (i) $\text{Aut}(E, f^\circ K)^f = \text{Aut}(E, K)$, and
 - (ii) $\text{Aut}(E, K)^{f^{-1}} = \text{Aut}(E, f^\circ K)$.
- (11) Let us consider a field F , an extension E of F , a subgroup H of $\text{Aut}(E, F)$, and an element f of the carrier of $\text{Aut}(E, F)$. Then $f^\circ(\text{Fix}(E, H)) = \text{Fix}(E, H^{f^{-1}})$.

3. THE FUNDAMENTAL THEOREM

Now we state the propositions:

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

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

- (14) Ψ_E is a bijection of $\text{IntermediateFields}(E, F)$, $\text{SubGr Aut}(E, F)$.
- (15) Φ_E is a bijection of $\text{SubGr Aut}(E, F)$, $\text{IntermediateFields}(E, F)$.
- (16) (i) $(\Psi_E)^{-1} = \Phi_E$, and
(ii) $(\Phi_E)^{-1} = \Psi_E$.

Let F be a field and E be an F -finite Galois extension of F . Let us note that $\text{IntermediateFields}(E, F)$ is $\text{SubGr Aut}(E, F)$ -bijective and $\text{SubGr Aut}(E, F)$ is $\text{IntermediateFields}(E, F)$ -bijective. Now we state the propositions:

- (17) Let us consider a field F , an F -finite Galois extension E of F , and an intermediate field K of E , F . Then $K = \text{Fix}(E, \text{Aut}(E, K))$.
- (18) Let us consider a field F , an F -finite Galois extension E of F , and a SubGroup G of $\text{Aut}(E, F)$. Then $G = \text{Aut}(E, \text{Fix}(E, G))$.
- (19) Let us consider a field F , an F -finite Galois extension E of F , and intermediate fields K_1, K_2 of E , F . Then K_1 is a subfield of K_2 if and only if $\text{Aut}(E, K_2)$ is a subgroup of $\text{Aut}(E, K_1)$. The theorem is a consequence of (17).
- (20) Let us consider a field F , an F -finite Galois extension E of F , and SubGroups G_1, G_2 of $\text{Aut}(E, F)$. Then G_1 is a subgroup of G_2 if and only

if $\text{Fix}(E, G_2)$ is a subfield of $\text{Fix}(E, G_1)$. The theorem is a consequence of (18).

(21) Let us consider a field F , an F -finite Galois extension E of F , and an intermediate field K of E, F . Then

- (i) $\deg(E, K) = \text{order Aut}(E, K)$, and
- (ii) $\deg(K, F) = \text{Index}(\text{Aut}(E, K), \text{Aut}(E, F))$.

(22) Let us consider a field F , an F -finite Galois extension E of F , and intermediate fields K_1, K_2 of E, F . Then K_1 and K_2 are isomorphic over F if and only if $\text{Aut}(E, K_1), \text{Aut}(E, K_2)$ are conjugated in $\text{Aut}(E, F)$. The theorem is a consequence of (9), (17), and (11).

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

- (23) E is a Galois extension of K .
- (24) K is a Galois extension of F if and only if K is F -normal.
- (25) K is F -normal if and only if for every element f of the carrier of $\text{Aut}(E, F)$, $f^\circ K = K$. The theorem is a consequence of (6).
- (26) K is F -normal if and only if $\text{Aut}(E, K)$ is a normal subgroup of $\text{Aut}(E, F)$. The theorem is a consequence of (6), (10), (2), (14), and (25).

Let F be a field, E be an F -finite extension of F , and K be an intermediate field of E, F . Assume K is F -normal. The functor $\rho(K)$ yielding a homomorphism from $\text{Aut}(E, F)$ to $\text{Aut}(K, F)$ is defined by

(Def. 5) for every F -fixing automorphism f of E , $it(f) = f|_{\text{(the carrier of } K)}$.

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

- (27) If K is F -normal, then $\text{Fix}(K, \text{Im } \rho(K))$ is a subfield of $\text{Fix}(E, \text{Aut}(E, F))$. The theorem is a consequence of (4).
- (28) If K is F -normal, then $\text{Ker } \rho(K) = \text{Aut}(E, K)$.
- (29) Let us consider a field F , an F -finite Galois extension E of F , and an intermediate field K of E, F . If K is F -normal, then $\text{Im } \rho(K) = \text{Aut}(K, F)$. The theorem is a consequence of (24), (27), and (15).
- (30) Let us consider a field F , an F -finite Galois extension E of F , an intermediate field K of E, F , and a normal subgroup H of $\text{Aut}(E, F)$. Suppose $H = \text{Aut}(E, K)$. Then $\text{Aut}(K, F)$ and ${}^{\text{Aut}(E, F)}/_H$ are isomorphic. The theorem is a consequence of (26), (28), and (29).

4. SOME LATTICE PROPERTIES

Now we state the propositions:

- (31) Let us consider a field F , an extension E of F , and intermediate fields K_1, K_2 of E, F . Then
- (i) $\text{Aut}(E, K_1) \sqcup \text{Aut}(E, K_2)$ is a subgroup of $\text{Aut}(E, K_1 \sqcap K_2)$, and
 - (ii) $\text{Aut}(E, K_1 \sqcup K_2)$ is a subgroup of $\text{Aut}(E, K_1) \cap \text{Aut}(E, K_2)$.
- (32) Let us consider a field F , an extension E of F , and subgroups G_1, G_2 of $\text{Aut}(E, F)$. Then
- (i) $\text{Fix}(E, G_1) \sqcup \text{Fix}(E, G_2)$ is a subfield of $\text{Fix}(E, G_1 \cap G_2)$, and
 - (ii) $\text{Fix}(E, G_1 \sqcup G_2)$ is a subfield of $\text{Fix}(E, G_1) \sqcap \text{Fix}(E, G_2)$.
- (33) Let us consider a field F , an F -finite Galois extension E of F , and intermediate fields K_1, K_2 of E, F . Then
- (i) $\text{Aut}(E, K_1 \sqcap K_2) = \text{Aut}(E, K_1) \sqcup \text{Aut}(E, K_2)$, and
 - (ii) $\text{Aut}(E, K_1 \sqcup K_2) = \text{Aut}(E, K_1) \cap \text{Aut}(E, K_2)$.

The theorem is a consequence of (31), (18), (17), and (32).

- (34) Let us consider a field F , an F -finite Galois extension E of F , and SubGroups G_1, G_2 of $\text{Aut}(E, F)$. Then
- (i) $\text{Fix}(E, G_1 \cap G_2) = \text{Fix}(E, G_1) \sqcup \text{Fix}(E, G_2)$, and
 - (ii) $\text{Fix}(E, G_1 \sqcup G_2) = \text{Fix}(E, G_1) \sqcap \text{Fix}(E, G_2)$.

The theorem is a consequence of (17), (18), (31), and (32).

Let F be a field, E be an extension of F , and M be a non empty subset of $\text{IntermediateFields}(E, F)$. The functor Ψ_M yielding a non empty subset of $\text{SubGr Aut}(E, F)$ is defined by the term

(Def. 6) $\{(\Psi_E)(K), \text{ where } K \text{ is an element of } \text{IntermediateFields}(E, F) : K \in M\}$.

Let M be a non empty subset of $\text{SubGr Aut}(E, F)$. The functor Φ_M yielding a non empty subset of $\text{IntermediateFields}(E, F)$ is defined by the term

(Def. 7) $\{(\Phi_E)(G), \text{ where } G \text{ is an element of } \text{SubGr Aut}(E, F) : G \in M\}$.

Now we state the propositions:

- (35) Let us consider a field F , an extension E of F , and a non empty subset M of $\text{IntermediateFields}(E, F)$. Then $\Psi_M = \{\text{Aut}(E, K), \text{ where } K \text{ is an element of } \text{IntermediateFields}(E, F) : K \in M\}$.
- (36) Let us consider a field F , an extension E of F , and a non empty subset M of $\text{SubGr Aut}(E, F)$. Then $\Phi_M = \{\text{Fix}(E, G), \text{ where } G \text{ is an element of } \text{SubGr Aut}(E, F) : G \in M\}$.

- (37) Let us consider a field F , an F -finite Galois extension E of F , and a non empty subset M of $\text{IntermediateFields}(E, F)$. Then $\Phi_{\Psi_M} = M$. The theorem is a consequence of (35), (36), and (17).
- (38) Let us consider a field F , an F -finite Galois extension E of F , and a non empty subset M of $\text{SubGr Aut}(E, F)$. Then $\Psi_{\Phi_M} = M$. The theorem is a consequence of (36), (35), and (18).
- (39) Let us consider a field F , an extension E of F , and a non empty subset M of $\text{IntermediateFields}(E, F)$. Then
- (i) $\text{Aut}(E, \cup M)$ is a subgroup of $\cap \Psi_M$, and
 - (ii) $\cup \Psi_M$ is a subgroup of $\text{Aut}(E, \cap M)$.

The theorem is a consequence of (35).

- (40) Let us consider a field F , an extension E of F , and a non empty subset M of $\text{SubGr Aut}(E, F)$. Then
- (i) $\text{Fix}(E, \cup M)$ is a subfield of $\cap \Phi_M$, and
 - (ii) $\cup \Phi_M$ is a subfield of $\text{Fix}(E, \cap M)$.

The theorem is a consequence of (36).

- (41) Let us consider a field F , an F -finite Galois extension E of F , and a non empty subset M of $\text{IntermediateFields}(E, F)$. Then
- (i) $\text{Aut}(E, \cup M) = \cap \Psi_M$, and
 - (ii) $\text{Aut}(E, \cap M) = \cup \Psi_M$.

The theorem is a consequence of (39), (40), (37), and (18).

- (42) Let us consider a field F , an F -finite Galois extension E of F , and a non empty subset M of $\text{SubGr Aut}(E, F)$. Then
- (i) $\text{Fix}(E, \cup M) = \cap \Phi_M$, and
 - (ii) $\text{Fix}(E, \cap M) = \cup \Phi_M$.

The theorem is a consequence of (39), (38), (17), and (40).

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 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.
- [4] Thomas Browning and Patrick Lutz. Formalizing Galois theory. *Experimental Mathematics*, 31(2):413–424, 2022. doi:10.1080/10586458.2021.1986176.
- [5] 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.
- [6] 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.
- [7] David Hernandez and Yves Laszlo. *Introduction to Galois Theory*. Undergraduate Mathematics Series. Springer, 2024. doi:10.1007/978-3-031-66182-2.
- [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. Splitting fields. *Formalized Mathematics*, 29(3):129–139, 2021. doi:10.2478/forma-2021-0013.
- [14] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzweller. Simple extensions. *Formalized Mathematics*, 31(1):287–298, 2023. doi:10.2478/forma-2023-0023.
- [15] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzweller. Introduction to Galois theory. *Formalized Mathematics*, 33(1):175–183, 2025. doi:10.2478/forma-2025-0014.

Received July 9, 2025, Accepted January 24, 2026
