FORMALIZED MATHEMATICS
Vol. 34, No. 1, pp. 23–30, 2026
DOI: 10.2478/forma-2026-0003
e-ISSN: 1898–9934

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

MSC: 68V20

Keywords:

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

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

1. the functions φ mapping intermediate fields K to $\mathrm{Aut}(E,K)$ and ϕ mapping subgroups G of $\mathrm{Aut}(E,F)$ to $\mathrm{Fix}(E,G)$ 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 $\mathrm{Aut}(E,K)$ and the degree of K over F equals the index of $\mathrm{Aut}(E,K)$ in $\mathrm{Aut}(E,F)$.

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 $\mathrm{Aut}(E, K_1)$ and $\mathrm{Aut}(E, K_2)$ are conjugated in $\mathrm{Aut}(E, F)$.

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 $f \in \mathrm{Aut}(E, F)$ we have $f(K) = K$ if and only if $\mathrm{Aut}(E, K)$ is a normal subgroup of $\mathrm{Aut}(E, F)$. In this case $\mathrm{Aut}(K, F)$ and $\mathrm{Aut}(E, F)/\mathrm{Aut}(E, K)$ are isomorphic.

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

6. $\mathrm{Aut}(E, \bigvee M) = \bigwedge\{\, \varphi(K) \mid K \in M\} = \bigwedge\{\mathrm{Aut}(E, K) \mid K \in M\}$ and $\mathrm{Aut}(E, \bigwedge M) = \bigvee\{\, \varphi(K) \mid K \in M\} = \bigvee\{\mathrm{Aut}(E, K) \mid K \in M\}$.

7. $\mathrm{Fix}(E, \bigvee N) = \bigwedge\{\, \phi(G) \mid G \in N\} = \bigwedge\{\mathrm{Fix}(E, G) \mid G \in N\}$ and $\mathrm{Fix}(E, \bigwedge N) = \bigvee\{\, \phi(G) \mid G \in N\} = \bigvee\{\mathrm{Fix}(E, G) \mid G \in N\}$.

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 $\mathrm{Ker}\, f = H$.

Let G, H be groups. Assume H is a subgroup of G. The functor $\mathrm{Index}(H, G)$ 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 $\mathrm{rng}(h, K)$ yielding a subset of E is defined by the term

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

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

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

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

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 $f \restriction (\text{the carrier of } K)$ 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 $f_1 \cdot f_2 \restriction (\text{the carrier of } K) = (f_1 \restriction (\text{the carrier of } K)) \cdot (f_2 \restriction (\text{the carrier of } K))$. 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 $\mathrm{Aut}(E, F)$. 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 $\mathrm{Fix}(K, \mathrm{Aut}(K, F))$ is a subfield of $\mathrm{Fix}(E, \mathrm{Aut}(E, F))$. The theorem is a consequence of (4).

(8) Let us consider a field F, a F-normal extension E of F, and an F-algebraic element a of E. Suppose $E \approx \mathrm{FAdj}(F, \{a\})$. Then E is a splitting field of $\mathrm{MinPoly}(a, F)$.

(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 $f \restriction K_1 = h$.

PROOF: Consider a being an element of E such that $E \approx \mathrm{FAdj}(F, \{a\})$. Set $p = \mathrm{MinPoly}(a, F)$. Reconsider $p_1 = p$ as an element of the carrier of 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 an 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 [9, (4)], [7, (7)], (8), [8, (29)]. Consider f being a function from L into L such that f is h_1-extending and isomorphism. □

(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 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 $\text{IntermediateFields}(E, F)$, $\text{SubGr}\,\text{Aut}(E, F)$.

(15) $\Phi(E)$ is a bijection of $\text{SubGr}\,\text{Aut}(E, F)$, $\text{IntermediateFields}(E, F)$.

(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 $(\text{SubGr}\,\text{Aut}(E, F))$-bijective and $\text{SubGr}\,\text{Aut}(E, F)$ 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 $\mathrm{Aut}(E, K_2)$ is a subgroup of $\mathrm{Aut}(E, K_1)$. 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 $\mathrm{Aut}(E, F)$. Then G_1 is a subgroup of G_2 if and only if $\mathrm{Fix}(E, G_2)$ is a subfield of $\mathrm{Fix}(E, G_1)$. 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) $\deg(E, K) = \mathrm{order}\,\mathrm{Aut}(E, K)$, and

(ii) $\deg(K, F) = \mathrm{Index}(\mathrm{Aut}(E, K), \mathrm{Aut}(E, F))$.

(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 $\mathrm{Aut}(E, K_1)$, $\mathrm{Aut}(E, K_2)$ are conjugated in $\mathrm{Aut}(E, F)$. 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 $\mathrm{Aut}(E, F)$, $f^{\circ}K = K$. The theorem is a consequence of (6).

(26) K is F-normal if and only if $\mathrm{Aut}(E, K)$ is a normal subgroup of $\mathrm{Aut}(E, F)$. 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 Phi.(K) yielding a homomorphism from $\mathrm{Aut}(E, F)$ to $\mathrm{Aut}(K, F)$ is defined by

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

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 $\mathrm{Fix}(K, \mathrm{Im}\,\mathrm{Phi.}(K))$ is a subfield of $\mathrm{Fix}(E, \mathrm{Aut}(E, F))$. The theorem is a consequence of (4).

(28) If K is F-normal, then $\mathrm{Ker}\,\mathrm{Phi.}(K) = \mathrm{Aut}(E, K)$.

Now we state the propositions:

(29) Let us consider a field F, an F-finite Galois extension E of F, and an intermediate field K of E, F. Suppose K is F-normal. Then $\mathrm{Im}\,\mathrm{Phi.}(K) = \mathrm{Aut}(K, F)$. 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 $\mathrm{Aut}(E, F)$. Suppose

$H = \mathrm{Aut}(E, K)$. Then $\mathrm{Aut}(K, F)$ and ${}^{\mathrm{Aut}(E,F)}/_{H}$ 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) $\mathrm{Aut}(E, K_1) \sqcup \mathrm{Aut}(E, K_2)$ is a subgroup of $\mathrm{Aut}(E, (K_1 \sqcap K_2))$, and

(ii) $\mathrm{Aut}(E, (K_1 \sqcup K_2))$ is a subgroup of $\mathrm{Aut}(E, K_1) \cap \mathrm{Aut}(E, K_2)$.

(32) Let us consider a field F, an extension E of F, and subgroups G_1, G_2 of $\mathrm{Aut}(E, F)$. Then

(i) $\mathrm{Fix}(E, G_1) \sqcup \mathrm{Fix}(E, G_2)$ is a subfield of $\mathrm{Fix}(E, G_1 \cap G_2)$, and

(ii) $\mathrm{Fix}(E, G_1 \sqcup G_2)$ is a subfield of $\mathrm{Fix}(E, G_1) \sqcap \mathrm{Fix}(E, G_2)$.

(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) $\mathrm{Aut}(E, (K_1 \sqcap K_2)) = \mathrm{Aut}(E, K_1) \sqcup \mathrm{Aut}(E, K_2)$, and

(ii) $\mathrm{Aut}(E, (K_1 \sqcup K_2)) = \mathrm{Aut}(E, K_1) \cap \mathrm{Aut}(E, K_2)$.

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 $\mathrm{Aut}(E, F)$. Then

(i) $\mathrm{Fix}(E, G_1 \cap G_2) = \mathrm{Fix}(E, G_1) \sqcup \mathrm{Fix}(E, G_2)$, and

(ii) $\mathrm{Fix}(E, G_1 \sqcup G_2) = \mathrm{Fix}(E, G_1) \sqcap \mathrm{Fix}(E, G_2)$.

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

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

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

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

Now we state the propositions:

(35) Let us consider a field F, an extension E of F, and a non empty subset M of IntermediateFields(E, F). Then Psi.$(M) = \{$Aut(E, K), where K is an element of 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 SubGr Aut(E, F). Then the UNKNOWN of $M = \{$Fix(E, G), where G is an element of 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 IntermediateFields(E, F). Then the UNKNOWN of 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 SubGr Aut(E, F). Then Psi.(the UNKNOWN of $M) = M$. 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 IntermediateFields(E, F). Then

(i) Aut$(E, (\bigcup M))$ is a subgroup of $\bigcap$ Psi.(M), and

(ii) $\bigcup$ Psi.(M) is a subgroup of Aut$(E, (\bigcap M))$.

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 SubGr Aut(E, F). Then

(i) Fix$(E, \bigcup M)$ is a subfield of $\bigcap$(the UNKNOWN of M), and

(ii) $\bigcup$(the UNKNOWN of M) is a subfield of Fix$(E, \bigcap M)$.

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 IntermediateFields(E, F). Then

(i) Aut$(E, (\bigcup M)) = \bigcap$ Psi.(M), and

(ii) Aut$(E, (\bigcap M)) = \bigcup$ 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 SubGr Aut(E, F). Then

(i) Fix$(E, \bigcup M) = \bigcap$(the UNKNOWN of M), and

(ii) Fix$(E, \bigcap M) = \bigcup$(the UNKNOWN of M).

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

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. Splitting fields. *Formalized Mathematics*, 29(**3**):129–139, 2021. doi:10.2478/forma-2021-0013.

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

Received January 24, 2026