FORMALIZED MATHEMATICS
Vol. 33, No. 1, pp. 175–183, 2025
DOI: 10.2478/forma-2025-0014
e-ISSN: 1898–9934

Paradigm
reference-global.com

Introduction to Galois Theory

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Agnieszka Rowińska-Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Summary. This article continues a series devoted to the formalization of the Fundamental Theorem of Galois Theory using the Mizar proof assistant. We define groups of automorphisms and fixed fields and establish their fundamental properties. We also introduce an encoding of conjugates for groups of automorphisms and Galois extensions, and present the classical example demonstrating that the field of complex numbers is a Galois extension of the field of real numbers.

MSC: 12F10 68V20 68V35

Keywords: Galois theory; conjugates; field of complex numbers; finite field

MML identifier: GALOIS_1, version: 8.1.15 5.97.1503

Introduction

This article is the second (after [10]) in a series of five articles formalizing the Fundamental Theorem of Galois Theory [1], [5] using the Mizar formalism [3], [8].

We start the actual formalization defining groups of automorphisms and fixed fields and proving some of their basic properties [7]. We also define conjugates for a group of automorphisms and prove that for algebraic elements $a \in E$, there is a bijection between $\mathrm{Aut}(F(a), F)$ and the roots of a's minimal polynomial in $F(a)$ [2]. Finally we define Galois extensions as extensions E over F with $\mathrm{Fix}(E, \mathrm{Aut}(E, F)) = F$ and show that the field of complex numbers is a Galois extension of the field of real numbers (Th. 29). We also consider finite fields [9] and prove that a field E of order p^n is a Galois extension of $\mathbb{Z}_p$

of degree n and that $\mathrm{Aut}(E, \mathbb{Z}_p)$ is generated by the Frobenius morphism [6]. Actually, the last theorem in this article is automatically justified by means of the formal apparatus of clusters' registrations, making further development of Galois theory [11], [12] more efficient [4].

1. Preliminaries

Let X be a non empty set and x be an element of X. Observe that the functor $\{x\}$ yields a subset of X. Let F be a non quadratic complete field and a be a non square element of F. One can check that $\mathrm{X}^2 - a$ is irreducible and there exists an extension of F which is F-quadratic.

Let F be a field. Note that every extension of F which is F-quadratic is also F-simple.

Let E be an extension of F and a be an F-algebraic element of E. One can verify that $\mathrm{Roots}(\mathrm{FAdj}(F, \{a\}), \mathrm{MinPoly}(a, F))$ is non empty and finite.

Now we state the proposition:

(1) Let us consider an element z of $\mathbb{C}_{\mathrm{F}}$. Then z is an element of $\mathbb{R}_{\mathrm{F}}$ if and only if $\overline{z} = z$.

One can check that $\mathbb{C}_{\mathrm{F}}$ has not characteristic 2. One can check that the functor i yields a non zero, $\mathbb{R}_{\mathrm{F}}$-algebraic element of $\mathbb{C}_{\mathrm{F}}$. Let us note that $\mathrm{X}^2 + 1_{\mathbb{R}_{\mathrm{F}}}$ is irreducible. Now we state the propositions:

(2) $\mathrm{Roots}(\mathbb{C}_{\mathrm{F}}, \mathrm{X}^2 + 1_{\mathbb{R}_{\mathrm{F}}}) = \{i, -i\}$.

(3) $\mathrm{MinPoly}(i, \mathbb{R}_{\mathrm{F}}) = \mathrm{X}^2 + 1_{\mathbb{R}_{\mathrm{F}}}$. The theorem is a consequence of (2).

(4) $\mathbb{C}_{\mathrm{F}}$ is a splitting field of $\mathrm{X}^2 + 1_{\mathbb{R}_{\mathrm{F}}}$. The theorem is a consequence of (2).

(5) $\mathbb{C}_{\mathrm{F}} = \mathrm{FAdj}(\mathbb{R}_{\mathrm{F}}, \{i\})$. The theorem is a consequence of (4) and (2).

One can verify that $\mathbb{C}_{\mathrm{F}}$ is $\mathbb{R}_{\mathrm{F}}$-quadratic.

2. Groups of Automorphims

Let F be a field. The functor $\mathrm{Auts}(F)$ yielding a non empty set is defined by the term

(Def. 1) the set of all f where f is an automorphism of F.

One can check that $\mathrm{Auts}(F)$ is F-functional and every element of $\mathrm{Auts}(F)$ is additive, multiplicative, unity-preserving, and isomorphism.

The functor $\mathrm{AutComp}(F)$ yielding a binary operation on $\mathrm{Auts}(F)$ is defined by

(Def. 2) for every automorphisms f, g of F, $it(f, g) = f \cdot g$.

The functor $\mathrm{Aut}(F)$ yielding a strict, non empty multiplicative magma is defined by the term

(Def. 3) $\langle \mathrm{Auts}(F), \mathrm{AutComp}(F)\rangle$.

Let us note that $\mathrm{Aut}(F)$ is group-like and associative. Now we state the proposition:

(6) Let us consider a field F. Then $\mathbf{1}_{\mathrm{Aut}(F)} = \mathrm{id}_F$.

Let F be a field. Note that $\mathrm{Aut}(F)$ is F-functional and the carrier of $\mathrm{Aut}(F)$ is F-functional and every subset of $\mathrm{Aut}(F)$ is F-functional.

Let G be a subgroup of $\mathrm{Aut}(F)$. Observe that the carrier of G is F-functional and every element of the carrier of $\mathrm{Aut}(F)$ is additive, multiplicative, unity-preserving, and isomorphism.

Let G be a non empty subset of $\mathrm{Aut}(F)$. Let us note that every element of G is additive, multiplicative, unity-preserving, and isomorphism.

Let G be a non empty subgroup of $\mathrm{Aut}(F)$. Note that every element of the carrier of G is additive, multiplicative, unity-preserving, and isomorphism.

Let E be an extension of F. The functor $\mathrm{Auts}(E, F)$ yielding a non empty subset of $\mathrm{Auts}(E)$ is defined by the term

(Def. 4) the set of all f where f is an F-fixing automorphism of E.

One can verify that $\mathrm{Auts}(E, F)$ is E-functional and every element of $\mathrm{Auts}(E, F)$ is F-fixing, additive, multiplicative, unity-preserving, and isomorphism.

The functor $\mathrm{AutComp}(E, F)$ yielding a binary operation on $\mathrm{Auts}(E, F)$ is defined by the term

(Def. 5) $\mathrm{AutComp}(E) \restriction \mathrm{Auts}(E, F)$.

The functor $\mathrm{Aut}(E, F)$ yielding a strict multiplicative magma is defined by the term

(Def. 6) $\langle \mathrm{Auts}(E, F), \mathrm{AutComp}(E, F)\rangle$.

Let us note that $\mathrm{Aut}(E, F)$ is non empty and $\mathrm{Aut}(E, F)$ is group-like and associative.

One can verify that the functor $\mathrm{Aut}(E, F)$ yields a strict subgroup of $\mathrm{Aut}(E)$. Let us observe that $\mathrm{Aut}(E, F)$ is E-functional and the carrier of $\mathrm{Aut}(E, F)$ is E-functional and every subset of $\mathrm{Aut}(E, F)$ is E-functional and every element of the carrier of $\mathrm{Aut}(E, F)$ is F-fixing, additive, multiplicative, unity-preserving, and isomorphism.

Let G be a non empty subset of $\mathrm{Aut}(E, F)$. Let us observe that every element of G is F-fixing, additive, multiplicative, unity-preserving, and isomorphism.

Let G be a subgroup of $\mathrm{Aut}(E, F)$. One can check that every element of the carrier of G is F-fixing, additive, multiplicative, unity-preserving, and isomorphism.

Let E be a field and F be a subfield of E. The functor $\mathrm{Aut}(E, F)$ yielding a strict subgroup of $\mathrm{Aut}(E)$ is defined by the term

(Def. 7) $\mathrm{Aut}(\mathrm{FieldExt}(E, F), F)$.

Let F be a field, E be an extension of F, and K be an intermediate field of E, F. The functor $\mathrm{Aut}(E, K)$ yielding a strict subgroup of $\mathrm{Aut}(E)$ is defined by the term

(Def. 8) $\mathrm{Aut}(\mathrm{FieldExt}(E, K), K)$.

Now we state the proposition:

(7) Let us consider a field F, an extension E of F, an intermediate field K_1 of E, F, and a subfield K_2 of E. If $K_2 = K_1$, then $\mathrm{Aut}(E, K_2) = \mathrm{Aut}(E, K_1)$.

3. Conjugates

Let F be a field, G be a subgroup of $\mathrm{Aut}(F)$, and a be an element of F. The functor $\mathrm{Conjugates}(a, G)$ yielding a non empty subset of F is defined by the term

(Def. 9) the set of all $f(a)$ where f is an element of the carrier of G.

Let E be an extension of F and a be an element of E.

The functor $\mathrm{Conjugates}(a)$ yielding a non empty subset of E is defined by the term

(Def. 10) $\mathrm{Conjugates}(a, \mathrm{Aut}(E, F))$.

Let G be a subgroup of $\mathrm{Aut}(F)$ and a be an element of F. We introduce the notation $\mathrm{Conj}(a, G)$ as a synonym of $\mathrm{Conjugates}(a, G)$.

Let E be an extension of F and a be an element of E. We introduce the notation $\mathrm{Conj}(a)$ as a synonym of $\mathrm{Conjugates}(a)$.

Let us consider a field F, an extension E of F, an F-algebraic element a of E, and an element b of E. Now we state the propositions:

(8) Suppose $E \approx \mathrm{FAdj}(F, \{a\})$. Then if $b \in \mathrm{Roots}(\mathrm{FAdj}(F, \{a\}), \mathrm{MinPoly}(a, F))$, then $\mathrm{FAdj}(F, \{b\}) = \mathrm{FAdj}(F, \{a\})$.

(9) Suppose $b \in \mathrm{Roots}(\mathrm{FAdj}(F, \{a\}), \mathrm{MinPoly}(a, F))$. Then there exists an F-fixing automorphism f of $\mathrm{FAdj}(F, \{a\})$ such that $f(a) = b$. The theorem is a consequence of (8).

(10) Let us consider a field F, an extension E of F, a subgroup G of $\mathrm{Aut}(E, F)$, and an F-algebraic element a of E. Then $\mathrm{Conj}(a, G) \subseteq \mathrm{Roots}(E, \mathrm{MinPoly}(a, F))$.

Let F be a field, E be an extension of F, G be a subgroup of $\mathrm{Aut}(E, F)$, and a be an F-algebraic element of E. Note that $\mathrm{Conj}(a, G)$ is finite and $\mathrm{Conj}(a)$ is finite.

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

(11) If $E \approx \mathrm{FAdj}(F, \{a\})$, then $\mathrm{Conj}(a) = \mathrm{Roots}(E, \mathrm{MinPoly}(a, F))$. The theorem is a consequence of (10) and (9).

(12) There exists a function f from $\mathrm{Auts}(\mathrm{FAdj}(F, \{a\}), F)$ into $\mathrm{Roots}(\mathrm{FAdj}(F, \{a\}), \mathrm{MinPoly}(a, F))$ such that f is bijective.
PROOF: Set $G = \mathrm{Auts}(\mathrm{FAdj}(F, \{a\}), F)$. Set $R = \mathrm{Roots}(\mathrm{FAdj}(F, \{a\}), \mathrm{MinPoly}(a, F))$. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists an element f of G such that $\$_1 = f$ and $\$_2 = f(a)$. Consider h being a function from G into R such that for every object x such that $x \in G$ holds $\mathcal{P}[x, h(x)]$. $\square$

Let F be a field, E be an extension of F, and a be an F-algebraic element of E. Observe that $\mathrm{Aut}(\mathrm{FAdj}(F, \{a\}), F)$ is finite.

Let S be a subset of E. The functor $\mathrm{Auts}(S)$ yielding a non empty subset of $\mathrm{Auts}(E, F)$ is defined by the term

(Def. 11) $\{f$, where f is an F-fixing automorphism of $E : f^{\circ}S = S\}$.

Let a be an element of E. The functor $\mathrm{Auts}(a)$ yielding a non empty subset of $\mathrm{Auts}(E, F)$ is defined by the term

(Def. 12) $\mathrm{Auts}(\{a\})$.

Now we state the proposition:

(13) Let us consider a field F, an extension E of F, and an element a of E. Then $\mathrm{Auts}(a) = \{f$, where f is an F-fixing automorphism of $E : f(a) = a\}$.

Let F be a field, E be an extension of F, and S be a subset of E. The functor $\mathrm{AutComp}(S)$ yielding a binary operation on $\mathrm{Auts}(S)$ is defined by the term

(Def. 13) $\mathrm{AutComp}(E, F) \restriction \mathrm{Auts}(S)$.

The functor $\mathrm{Aut}(S)$ yielding a strict, non empty multiplicative magma is defined by the term

(Def. 14) $\langle \mathrm{Auts}(S), \mathrm{AutComp}(S) \rangle$.

Let S be a non empty subset of E. One can check that $\mathrm{Aut}(S)$ is group-like and associative.

Let us observe that the functor $\mathrm{Aut}(S)$ yields a strict subgroup of $\mathrm{Aut}(E, F)$. Let a be an element of E. The functor $\mathrm{Aut}(a)$ yielding a strict subgroup of $\mathrm{Aut}(E, F)$ is defined by the term

(Def. 15) $\mathrm{Aut}(\{a\})$.

Now we state the proposition:

(14) Let us consider a field F, an extension E of F, and an element a of E. Then $\overline{\overline{\mathrm{Conj}(a)}} = |\bullet : \mathrm{Aut}(a)|$.

PROOF: Set $H = \mathrm{Aut}(a)$. Set $G = \mathrm{Aut}(E, F)$. $\mathrm{Auts}(a) = \{f$, where f is an F-fixing automorphism of $E : f(a) = a\}$ and the carrier of $H = \mathrm{Auts}(a)$. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ for every element f of the carrier of G such that $\$_1 = f(a)$ holds $\$_2 = f \cdot H$. Consider h being a function from $\mathrm{Conj}(a)$ into the left cosets of H such that for every object x such that $x \in \mathrm{Conj}(a)$ holds $\mathcal{P}[x, h(x)]$. $\mathrm{rng}\, h =$ the left cosets of H. $\square$

4. Fixed Fields

Let F be a field and G be a subgroup of $\mathrm{Aut}(F)$. The functor FixedElements (F, G) yielding a non empty subset of F is defined by the term

(Def. 16) $\{a$, where a is an element of F : for every function f from F into F such that $f \in G$ holds $f(a) = a\}$.

We introduce the notation $\mathrm{FixEl}(F, G)$ as a synonym of $\mathrm{FixedElements}(F, G)$. One can check that $\mathrm{FixEl}(F, G)$ is inducing subfield.

The functor $\mathrm{Fix}(F, G)$ yielding a strict double loop structure is defined by

(Def. 17) the carrier of *it* $= \mathrm{FixEl}(F, G)$ and the addition of *it* $=$ (the addition of F) $\restriction \mathrm{FixEl}(F, G)$ and the multiplication of *it* $=$ (the multiplication of F) $\restriction \mathrm{FixEl}(F, G)$ and $1_{it} = 1_F$ and $0_{it} = 0_F$.

One can check that $\mathrm{Fix}(F, G)$ is non degenerated and $\mathrm{Fix}(F, G)$ is Abelian, add-associative, right zeroed, and right complementable and $\mathrm{Fix}(F, G)$ is commutative, associative, well unital, distributive, and almost left invertible.

Let us note that the functor $\mathrm{Fix}(F, G)$ yields a strict subfield of F. Let E be an extension of F and G be a subgroup of $\mathrm{Aut}(E, F)$. Let us note that the functor $\mathrm{Fix}(E, G)$ yields an intermediate field of E, F.

5. Some Basic Properties

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

(15) F is a subfield of $\mathrm{Fix}(E, \mathrm{Aut}(E, F))$.

(16) Every intermediate field K of E, F is a subfield of $\mathrm{Fix}(E, \mathrm{Aut}(E, K))$.

(17) Let us consider a field F. Then every subgroup G of $\mathrm{Aut}(F)$ is a subgroup of $\mathrm{Aut}(F, \mathrm{Fix}(F, G))$.

(18) Let us consider a field F, an extension E of F, and an intermediate field K of E, F. Then $\mathrm{Aut}(E, K)$ is a subgroup of $\mathrm{Aut}(E, F)$.

(19) Let us consider a field F, an extension E of F, and intermediate fields K_1, K_2 of E, F. Suppose K_1 is a subfield of K_2. Then $\mathrm{Aut}(E, K_2)$ is a subgroup of $\mathrm{Aut}(E, K_1)$.

(20) Let us consider a field F, and subgroups G_1, G_2 of $\mathrm{Aut}(F)$. Suppose G_1 is a subgroup of G_2. Then $\mathrm{Fix}(F, G_2)$ is a subfield of $\mathrm{Fix}(F, G_1)$.

(21) Let us consider a field F, and an extension E of F. Then $\mathrm{Aut}(E, F) = \mathrm{Aut}(E, \mathrm{Fix}(E, \mathrm{Aut}(E, F)))$. The theorem is a consequence of (17) and (15).

(22) Let us consider a field F, and a subgroup G of $\mathrm{Aut}(F)$. Then $\mathrm{Fix}(F, G) = \mathrm{Fix}(F, \mathrm{Aut}(F, \mathrm{Fix}(F, G)))$. The theorem is a consequence of (17), (20), and (15).

6. Galois Extensions

Let F be a field and E be an extension of F. We say that E is F-Galois if and only if

(Def. 18) $\mathrm{Fix}(E, \mathrm{Aut}(E, F)) \approx F$.

One can check that there exists an extension of F which is F-Galois.

A Galois extension of F is an F-Galois extension of F. One can verify that there exists a Galois extension of F which is F-finite. Now we state the propositions:

(23) Let us consider a field F, and an extension E of F. Then E is F-Galois if and only if there exists a subgroup G of $\mathrm{Aut}(E)$ such that $\mathrm{Fix}(E, G) \approx F$. The theorem is a consequence of (20) and (15).

(24) Every field F is a Galois extension of F.

The functor $*'$ yielding a function from $\mathbb{C}_{\mathrm{F}}$ into $\mathbb{C}_{\mathrm{F}}$ is defined by

(Def. 19) for every element z of $\mathbb{C}_{\mathrm{F}}$, $it(z) = \overline{z}$.

Let us note that $*'$ is $(\mathbb{R}_{\mathrm{F}})$-fixing and isomorphism.

Let us note that the functor $*'$ yields an element of the carrier of $\mathrm{Aut}(\mathbb{C}_{\mathrm{F}}, \mathbb{R}_{\mathrm{F}})$. Now we state the propositions:

(25) $\mathrm{Auts}(\mathbb{C}_{\mathrm{F}}, \mathbb{R}_{\mathrm{F}}) = \{\mathrm{id}_{\mathbb{C}_{\mathrm{F}}}, *'\}$. The theorem is a consequence of (5), (2), and (3).

(26) $\mathrm{Aut}(\mathbb{C}_{\mathrm{F}}, \mathbb{R}_{\mathrm{F}}) = \mathrm{gr}(\{*'\})$. The theorem is a consequence of (25).

One can verify that $\mathrm{Aut}(\mathbb{C}_{\mathrm{F}}, \mathbb{R}_{\mathrm{F}})$ is finite and cyclic. Now we state the propositions:

(27) $\mathrm{order}\,\mathrm{Aut}(\mathbb{C}_{\mathrm{F}}, \mathbb{R}_{\mathrm{F}}) = 2$. The theorem is a consequence of (25).

(28) $\mathrm{Aut}(\mathbb{C}_{\mathrm{F}}, \mathbb{R}_{\mathrm{F}})$ and $\mathbb{Z}_2^+$ are isomorphic.

Observe that $\mathbb{C}_{\mathrm{F}}$ is $(\mathbb{R}_{\mathrm{F}})$-Galois. Now we state the proposition:

(29) $\mathbb{C}_{\mathrm{F}}$ is a Galois extension of $\mathbb{R}_{\mathrm{F}}$.

Let p be a prime number, n be a non zero natural number, and F be a Galois field of p^n. Observe that the functor $\mathrm{Frob}(F)$ yields an element of the carrier of $\mathrm{Aut}(F, \mathbb{Z}/p)$. Let m be a natural number. One can verify that $(\mathrm{Frob}(F))^m$ is $(\mathbb{Z}/p)$-fixing and isomorphism.

Let us consider a prime number p, a non zero natural number n, and a Galois field F of p^n. Now we state the propositions:

(30) $\mathrm{Aut}(F, \mathbb{Z}/p) = \mathrm{Aut}(F)$.

(31) $\mathrm{Auts}(F, \mathbb{Z}/p) = \{(\mathrm{Frob}(F))^m$, where m is a natural number : $0 \leqslant m \leqslant n-1\}$. The theorem is a consequence of (30).

(32) $\mathrm{Aut}(F, \mathbb{Z}/p) = \mathrm{gr}(\{\mathrm{Frob}(F)\})$.

Let p be a prime number, n be a non zero natural number, and F be a Galois field of p^n. Observe that $\mathrm{Aut}(F, \mathbb{Z}/p)$ is finite and cyclic.

Let us consider a prime number p, a non zero natural number n, and a Galois field F of p^n. Now we state the propositions:

(33) $\mathrm{order}\,\mathrm{Aut}(F, \mathbb{Z}/p) = n$.

(34) $\mathrm{Aut}(F, \mathbb{Z}/p)$ and $\mathbb{Z}_n^+$ are isomorphic.

PROOF: Set $a = \mathrm{Frob}(F)$. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists a natural number m such that $\$_1 = m$ and $\$_2 = a^m$. Consider f being a function from the carrier of $\mathbb{Z}_n^+$ into the carrier of $\mathrm{Aut}(F, \mathbb{Z}/p)$ such that for every object x such that $x \in$ the carrier of $\mathbb{Z}_n^+$ holds $\mathcal{P}[x, f(x)]$. $\square$

Let p be a prime number and n be a non zero natural number. Let us note that every Galois field of p^n is $(\mathbb{Z}/p)$-Galois. Now we state the proposition:

(35) Let us consider a prime number p, and a non zero natural number n. Then every Galois field of p^n is a Galois extension of $\mathbb{Z}/p$.

References

[1] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Wiley and Sons, third edition, 2004.

[2] Andreas Gathmann. *Einführung in die Algebra*. Lecture Notes, University of Kaiserslautern, Germany, 2011.

[3] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[4] 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.

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

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

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

[8] Colin Rothgang, Artur Korniłowicz, and Florian Rabe. A new export of the Mizar Mathematical Library. In Fairouz Kamareddine and Claudio Sacerdoti Coen, editors, *Intelligent Computer Mathematics*, pages 205–210, Cham, 2021. Springer International Publishing. doi:10.1007/978-3-030-81097-9_17.

[9] Christoph Schwarzweller. Finite fields. *Formalized Mathematics*, 32(1):289–302, 2024. doi:10.2478/forma-2024-0024.

[10] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzweller. The lattice of intermediate fields and other preliminaries to Galois theory. *Formalized Mathematics*, 33(1): 165–174, 2025. doi:10.2478/forma-2025-0013.

[11] Ian Stewart. *Galois Theory*. Chapman and Hall/CRC, fourth edition, 2015.

[12] Steven H. Weintraub. *Galois Theory*. Springer-Verlag, second edition, 2009.

Received July 9, 2025, Accepted December 12, 2025