

Characterization of Finite Galois Extensions

Christoph Schwarzweller 
 Institute of Informatics
 University of Gdańsk
 Poland

Summary. In this article we prove the well-known characterization of finite Galois extensions: a finite extension E of F is a Galois extension of F iff E is both normal and separable iff E is the splitting field of a separable polynomial $p \in F[X]$. We also prove some applications of the characterization, so for example that $F(a_1, \dots, a_n)$ is a separable extension of F if and only if all the a_i are separable, or that every finite separable extension of F is contained in a Galois extension of F .

MSC: 12F10 68V20 68V35

Keywords: finite Galois extension; minimal polynomial; separable extension

MML identifier: GALOIS_2, version: 8.1.15 5.98.1507

INTRODUCTION

This article is the third (after [9]) in a series of five articles formalizing the Fundamental Theorem of Galois Theory [1], [5], using the Mizar formalism [3], [4], [8]. Here we prove the well-known characterization of finite Galois extensions [10], [11]: a finite extension E of F is a Galois extension of F if and only if E is both normal and separable if and only if E is the splitting field of a separable polynomial $p \in F[X]$ [7], [5]. The key of the proof are two observations concerning minimal polynomials [6], [2].

Firstly, that if E is a Galois extension of F , the minimal polynomial $\mu_a(X)$ of an algebraic element $a \in E$ is just the product

$$\mu_a(X) = (X - a_1) \cdot \dots \cdot (X - a_n),$$

where $a_1, \dots, a_n$ are exactly the conjugates of a . From this easily follows that in a Galois extension E all minimal polynomials are separable, and of course split in E .

Secondly, that for algebraic elements $a_1, \dots, a_n$ the extension $F(a_1, \dots, a_n)$ is generated by the roots of

$$p(X) = \mu_{a_1}(X) \cdot \dots \cdot \mu_{a_n}(X),$$

where $\mu_{a_i}(X)$ is the minimal polynomial of a_i . In particular, for a separable extension $F(a_1, \dots, a_n)$ the polynomial $p(X)$ is separable.

In the last section we also prove some applications of the characterization, so for example that $F(a_1, \dots, a_n)$ is a separable extension of F if and only if all the a_i are separable, or that every finite separable extension of F is contained in a Galois extension of F .

1. PRELIMINARIES

Let X, Y be non empty sets, f be a function from X into Y , and S be a non empty, finite subset of X . Let us observe that the functor $f^\circ S$ yields a non empty, finite subset of Y . Now we state the propositions:

- (1) Let us consider a field F , elements g_1, g_2 of $\text{Aut}(F)$, and automorphisms f_1, f_2 of F . If $g_1 = f_1$ and $g_2 = f_2$, then $g_1 \cdot g_2 = f_1 \cdot f_2$.
- (2) Let us consider a field F , an element g of $\text{Aut}(F)$, and an automorphism f of F . If $g = f$, then $g^{-1} = f^{-1}$.
- (3) Let us consider a field F , an extension E of F , elements g_1, g_2 of $\text{Aut}(E, F)$, and F -fixing automorphisms f_1, f_2 of E . If $g_1 = f_1$ and $g_2 = f_2$, then $g_1 \cdot g_2 = f_1 \cdot f_2$.
- (4) Let us consider a field F , an extension E of F , an element g of $\text{Aut}(E, F)$, and an F -fixing automorphism f of E . If $g = f$, then $g^{-1} = f^{-1}$. The theorem is a consequence of (3).
- (5) Let us consider a commutative ring R , a commutative ring extension S of R , and elements p, q of the carrier of Polynom-Ring R . If $q \mid p$, then $\text{Roots}(S, q) \subseteq \text{Roots}(S, p)$.

Let R be an integral domain, p be a non zero polynomial over R , and q be a non constant polynomial over R . Note that $p * q$ is non constant. Let p be a non zero element of the carrier of Polynom-Ring R and q be a non constant element of the carrier of Polynom-Ring R . Note that $p \cdot q$ is non constant. Now we state the propositions:

- (6) Let us consider a ring R , a ring extension S of R , an element a of R , and an element b of S . Then $\text{ExtEval}(a \upharpoonright R, b) = a$.

- (7) Let us consider a field F , an extension E of F , a non empty finite sequence f of elements of the carrier of Polynom-Ring F , and a polynomial q over F . Suppose $q = \prod f$. Let us consider an element a of E . Then $\text{ExtEval}(q, a) = 0_E$ if and only if there exists an element i of $\text{dom } f$ and there exists a polynomial p over F such that $p = f(i)$ and $\text{ExtEval}(p, a) = 0_E$.
- (8) Let us consider a field F , a finite sequence f of elements of Polynom-Ring F , and elements p, q of the carrier of Polynom-Ring F . Suppose $p = \prod f$ and there exists a natural number i such that $1 \leq i \leq \text{len } f$ and $f(i) = q$. Then $q \mid p$.
- (9) Let us consider a field F , a finite sequence f of elements of Polynom-Ring F , and elements p, q_1, q_2 of the carrier of Polynom-Ring F . Suppose $p = \prod f$ and there exist natural numbers i, j such that $j \neq i$ and $1 \leq i \leq \text{len } f$ and $f(i) = q_1$ and $1 \leq j \leq \text{len } f$ and $f(j) = q_2$. Then $q_1 * q_2 \mid p$.
 PROOF: Consider i, j being natural numbers such that $j \neq i$ and $1 \leq i \leq \text{len } f$ and $f(i) = q_1$ and $1 \leq j \leq \text{len } f$ and $f(j) = q_2$. Reconsider $i_1 = i - 1$ as an element of $\mathbb{N}$. Set $g = (f \upharpoonright i_1) \hat{\ } f \upharpoonright i$. Reconsider $r = \prod g, r_1 = \prod (f \upharpoonright i_1), r_2 = \prod f \upharpoonright i$ as an element of the carrier of Polynom-Ring F . There exists a natural number k such that $1 \leq k \leq \text{len } g$ and $g(k) = q_2$. Consider s being a polynomial over F such that $q_2 * s = r$. $\square$
- (10) Let us consider a field F , and a finite sequence f of elements of the carrier of Polynom-Ring F . Suppose for every element i of $\text{dom } f$ for every polynomial q over F such that $q = f(i)$ holds q is monic. Let us consider a polynomial p over F . If $p = \prod f$, then p is monic.
 PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite sequence f of elements of the carrier of Polynom-Ring F such that $\text{len } f = \$_1$ and for every element i of $\text{dom } f$ and for every polynomial q over F such that $q = f(i)$ holds q is monic for every polynomial p over F such that $p = \prod f$ holds p is monic. $\mathcal{P}[0]$. For every natural number $k, \mathcal{P}[k]$. Consider k being a natural number such that $\text{len } f = k$. $\square$
- (11) Let us consider a field F , an extension E of F , a non constant polynomial p over F , and a non zero polynomial q over F . If $p * q$ splits in E , then p splits in E .

Let us consider a field F and extensions E_1, E_2 of F . Now we state the propositions:

- (12) If $E_1 \approx E_2$, then $\text{Aut}(E_1) = \text{Aut}(E_2)$.
- (13) If $E_1 \approx E_2$, then $\text{Aut}(E_1, F) = \text{Aut}(E_2, F)$. The theorem is a consequence of (12).
- (14) If $E_1 \approx E_2$, then $\text{Fix}(E_1, \text{Aut}(E_1, F)) = \text{Fix}(E_2, \text{Aut}(E_2, F))$. The theorem is a consequence of (13).

- (15) Let us consider a field F , a Galois extension E_1 of F , and an extension E_2 of F . If $E_2 \approx E_1$, then E_2 is a Galois extension of F . The theorem is a consequence of (14).

2. MORE ON SEPARABILITY

Let F be a field, E be an extension of F , and T be a subset of E . We say that T is F -separable if and only if

- (Def. 1) for every element a of E such that $a \in T$ holds a is F -separable.

One can verify that there exists a subset of E which is finite, F -separable, and non empty and every F -separable subset of E is F -algebraic.

Let E be an F -separable extension of F . Observe that every subset of E is F -separable. Now we state the proposition:

- (16) Let us consider a field F , and a non constant element p of the carrier of Polynom-Ring F . Then p is separable if and only if for every extension E of F such that p splits in E holds $\overline{\text{Roots}(E, p)} = \deg(p)$.

Let F be a field and p, q be elements of the carrier of Polynom-Ring F . We say that p, q have common roots in some extension if and only if

- (Def. 2) there exists an extension E of F such that $\text{Roots}(E, p) \cap \text{Roots}(E, q) \neq \emptyset$.

Now we state the propositions:

- (17) Let us consider a field F , and monic, irreducible elements p, q of the carrier of Polynom-Ring F . If p, q have common roots in some extension, then $p = q$.
- (18) Let us consider a field F , and non constant elements p, q of the carrier of Polynom-Ring F . Suppose p is separable and q is separable. Then $p \cdot q$ is separable if and only if p, q have nowhere common roots.
- (19) Let us consider a field F , and monic, irreducible elements p, q of the carrier of Polynom-Ring F . Suppose p is separable and q is separable. Then $p \cdot q$ is separable if and only if $p \neq q$. The theorem is a consequence of (17) and (18).
- (20) Let us consider a field F , an extension E of F , and a non empty finite sequence f of elements of Polynom-Ring F . Suppose for every natural number i such that $1 \leq i \leq \text{len } f$ there exists a monic, irreducible element q of the carrier of Polynom-Ring F such that $f(i) = q$ and q is separable. Let us consider a non constant element p of the carrier of Polynom-Ring F . If $p = \prod f$, then p is separable iff f is one-to-one. The theorem is a consequence of (9), (19), (8), and (17).

3. THE PRODUCT OF MINIMAL POLYNOMIALS OF A GIVEN FINITE ALGEBRAIC SET

Let F be a field, E be an extension of F , and T be an F -algebraic subset of E . The functor $\text{MinPolys}(T)$ yielding a subset of the carrier of $\text{Polynom-Ring } F$ is defined by the term

(Def. 3) $\{\text{MinPoly}(a, F), \text{ where } a \text{ is an } F\text{-algebraic element of } E : a \in T\}$.

Let T be a non empty, F -algebraic subset of E .

Let us observe that $\text{MinPolys}(T)$ is non empty. Let T be a finite, F -algebraic subset of E . Let us note that $\text{MinPolys}(T)$ is finite. The functor $\text{MinPolys}_{\text{FS}}(T)$ yielding a finite sequence of elements of the carrier of $\text{Polynom-Ring } F$ is defined by the term

(Def. 4) $\text{CFS}(\text{MinPolys}(T))$.

Let T be a non empty, finite, F -algebraic subset of E .

Observe that $\text{MinPolys}_{\text{FS}}(T)$ is non empty. Let T be a finite, F -algebraic subset of E . The functor $\text{ProdMinPolys}(T)$ yielding an element of the carrier of $\text{Polynom-Ring } F$ is defined by the term

(Def. 5) $\prod \text{MinPolys}_{\text{FS}}(T)$.

Let T be a non empty, finite, F -algebraic subset of E .

Note that $\text{ProdMinPolys}(T)$ is non constant and monic and $\text{Roots}(E, \text{ProdMinPolys}(T))$ is non empty. Let T be a non empty, finite, F -separable subset of E . One can verify that $\text{ProdMinPolys}(T)$ is separable. Now we state the propositions:

- (21) Let us consider a field F , an extension E of F , and a non empty, finite, F -algebraic subset T of E . Suppose $E \approx \text{FAdj}(F, T)$. Then $E \approx \text{FAdj}(F, \text{Roots}(E, \text{ProdMinPolys}(T)))$.
- (22) Let us consider a field F , a non constant element p of the carrier of $\text{Polynom-Ring } F$, and an extension E of F . Then E is a splitting field of p if and only if p splits in E and $E \approx \text{FAdj}(F, \text{Roots}(E, p))$.

4. MINIMAL POLYNOMIALS IN GALOIS EXTENSIONS

Now we state the propositions:

- (23) Let us consider a field F , an extension E of F , and a subgroup G of $\text{Aut}(E)$. If $\text{Fix}(E, G) \approx F$, then G is a subgroup of $\text{Aut}(E, F)$.
- (24) Let us consider a field F , an extension E of F , and a subgroup G of $\text{Aut}(E)$. Suppose $\text{Fix}(E, G) \approx F$. Let us consider a polynomial p over E . Suppose for every element g of the carrier of G , $(\text{PolyHom}(g))(p) = p$. Then p is a polynomial over F .

- (25) Let us consider a field F , an extension E of F , and a subgroup G of $\text{Aut}(E)$. Suppose $\text{Fix}(E, G) \approx F$. Let us consider an element g of the carrier of G , and an element a of E . Suppose $\text{Conj}(a, G)$ is finite. Then $g^\circ(\text{Conj}(a, G)) = \text{Conj}(a, G)$. The theorem is a consequence of (23), (4), and (3).
- (26) Let us consider a field F , an extension E of F , and a subgroup G of $\text{Aut}(E)$. Suppose $\text{Fix}(E, G) \approx F$. Let us consider an F -algebraic element a of E , and a non empty, finite subset Z of E . Suppose $Z = \text{Conj}(a, G)$. Let us consider a product of linear polynomials p of E and Z . Then $p = \text{MinPoly}(a, F)$. The theorem is a consequence of (25), (24), and (23).
- (27) Let us consider a field F , an extension E of F , and a subgroup G of $\text{Aut}(E)$. Suppose $\text{Fix}(E, G) \approx F$. Let us consider an F -algebraic element a of E . Suppose $\text{Conj}(a, G)$ is finite. Then
- (i) $\text{MinPoly}(a, F)$ is separable, and
 - (ii) $\text{MinPoly}(a, F)$ splits in E , and
 - (iii) $\text{Roots}(E, \text{MinPoly}(a, F)) = \text{Conj}(a, G)$, and
 - (iv) $\deg(\text{MinPoly}(a, F)) = \overline{\overline{\overline{\text{Conj}(a, G)}}}$.

The theorem is a consequence of (26).

- (28) Let us consider a field F , an extension E of F , and a subgroup G of $\text{Aut}(E)$. Suppose $\text{Fix}(E, G) \approx F$. Let us consider an element a of E . If $\text{Conj}(a, G)$ is finite, then a is F -algebraic. The theorem is a consequence of (25) and (24).

Let F be a field, E be a Galois extension of F , and a be an F -algebraic element of E . Let us note that $\text{MinPoly}(a, F)$ is separable. Now we state the propositions:

- (29) Let us consider a field F , a Galois extension E of F , and an F -algebraic element a of E . Then
- (i) $\text{MinPoly}(a, F)$ splits in E , and
 - (ii) $\text{Roots}(E, \text{MinPoly}(a, F)) = \text{Conj}(a)$, and
 - (iii) $\deg(\text{MinPoly}(a, F)) = \overline{\overline{\overline{\text{Conj}(a)}}}$.

The theorem is a consequence of (27).

- (30) Let us consider a field F , a Galois extension E of F , and an element a of E . Then a is F -algebraic if and only if $\text{Conj}(a)$ is finite. The theorem is a consequence of (28).

5. CHARACTERIZATION OF FINITE GALOIS EXTENSIONS

Now we state the propositions:

- (31) Let us consider a field F , an irreducible element p of the carrier of Polynom-Ring F , a splitting field E of p , and elements a, b of E . Suppose $a, b \in \text{Roots}(E, p)$. Then there exists an F -fixing automorphism h of E such that $h(a) = b$.
- (32) Let us consider a field F , a non constant element p of the carrier of Polynom-Ring F , a splitting field E of p , and elements a, b of E . Suppose $a, b \in \text{Roots}(E, p)$ and $\text{MinPoly}(a, F) = \text{MinPoly}(b, F)$. Then there exists an F -fixing automorphism h of E such that $h(a) = b$.

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 E is F -normal and F -separable.
- (34) E is a Galois extension of F if and only if there exists a separable, non constant element p of Polynom-Ring F such that E is a splitting field of p .

Let F be a field. Observe that every F -finite Galois extension of F is F -normal and F -separable and every F -finite extension of F which is F -normal and F -separable is also F -Galois.

Let p be a separable, non constant element of the carrier of Polynom-Ring F . One can verify that every splitting field of p is F -Galois.

6. SOME COROLLARIES

Now we state the propositions:

- (35) Let us consider a field F , an F -finite Galois extension E of F , and an intermediate field K of E, F . Then E is a Galois extension of K .
- (36) Let us consider a field F , and an F -finite extension E of F . Then E is a Galois extension of F if and only if for every element a of E , $\overline{\text{Roots}(E, \text{MinPoly}(a, F))} = \text{deg}(\text{FAdj}(F, \{a\}), F)$. The theorem is a consequence of (16).
- (37) Let us consider a field F , an extension E of F , and a finite subset T of E . Then $\text{FAdj}(F, T)$ is F -separable if and only if for every element a of E such that $a \in T$ holds a is F -separable.
- (38) Let us consider a field F , and an F -finite extension E of F . Then there exists a non constant element p of the carrier of Polynom-Ring F and there exists a splitting field K of p such that K is E -extending.

Let F be a field and E be an F -finite extension of F . Observe that there exists an extension of F which is F -normal and E -extending. Now we state the proposition:

- (39) Let us consider a field F , and an F -finite, F -separable extension E of F . Then there exists a separable, non constant element p of the carrier of Polynom-Ring F and there exists a splitting field K of p such that K is E -extending.

Let F be a field and E be an F -finite, F -separable extension of F . Note that there exists a Galois extension of F which is F -finite and E -extending.

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 and Agnieszka Rowińska-Schwarzweller. Introduction to Galois theory. *Formalized Mathematics*, 33(1):175–183, 2025. doi:10.2478/forma-2025-0014.
- [10] Ian Stewart. *Galois Theory*. Chapman and Hall/CRC, fourth edition, 2015.
- [11] Steven H. Weintraub. *Galois Theory*. Springer-Verlag, second edition, 2009.

Received July 9, 2025, Accepted December 21, 2025
