FORMALIZED MATHEMATICS
Vol. 33, No. 1, pp. 165–174, 2025
DOI: 10.2478/forma-2025-0013
e-ISSN: 1898–9934

The Lattice of Intermediate Fields and Other Preliminaries 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 initiates a series devoted to the formalization of the Fundamental Theorem of Galois Theory. It presents several preliminaries required for the formal development of Galois theory. In particular, as a main result, we define the lattice of intermediate fields of an extension E/F; we also treat sets of functions, groups, and intermediate fields in order to provide the necessary cluster registrations that enable effective Mizar automation.

MSC: 12F10 68V20 68V35

Keywords: Galois theory; lattice of intermediate fields; Galois connection

MML identifier: GALOIS_0, version: 8.1.15 5.97.1503

Introduction

This article lays the groundwork for a formalized treatment of the Fundamental Theorem of Galois Theory [3], [8] within the Mizar Mathematical Library [5]. It introduces the encoding of basic notions needed for the lattice structure [2], [7] of intermediate fields in a field extension E of F [11] (for a discussion on the development of lattice theory in Mizar, see [4] or [1] for more order-oriented approach, including the formalization of Galois connection, which is a subject of Sect. 4).

We deal with sets of functions, groups, and intermediate fields [9], [10]: a series of clusters adapting the type of elements of such sets provides more efficient work with these sets (compare [6]). In order to enable Mizar automation, we use several Mizar attributes, e.g. `G-subgroup-membered` or `F-subfield-membered`, characterize subfields and intermediate fields within a field extension, and prove foundational lemmas that make manipulating these structures feasible in the Mizar proof assistant. In Sect. 5 we prove some missing properties of the lattice of subgroups, while Section 6 proves that the collection of intermediate fields forms a complete lattice with well-defined join and meet operations.

Beyond lattice theory, the paper covers auxiliary results needed later in the series on Galois theory [12], [13]: in Sect. 8, we add several theorems about homomorphisms from $R[X]$ to $R[X]$, where R is a ring; it is instrumental for later formalized proofs involving field automorphisms and polynomial evaluation.

1. Preliminaries

Let A, B be sets. We say that B is A-bijective if and only if

(Def. 1) there exists a function f from A into B such that f is bijective.

Let A, B be non empty sets. Assume B is A-bijective.

A bijection of A, B is a function from A into B defined by

(Def. 2) *it* is bijective.

Now we state the proposition:

(1) Let us consider a field E, and subfields F_1, F_2 of E. Suppose the carrier of $F_1 \subseteq$ the carrier of F_2. Then F_1 is a subfield of F_2.

Let F be a finite field. One can check that SubFields(F) is finite.

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

(Def. 3) E.

The functor $\deg(E, F)$ yielding an integer is defined by the term

(Def. 4) $\deg(\mathrm{FieldExt}(E, F), F)$.

Let F be a finite field and E be an F-finite extension of F. One can verify that $\mathrm{IntermediateFields}(E, F)$ is finite.

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

An intermediate field of E, F is a field defined by

(Def. 5) $it \in \mathrm{IntermediateFields}(E, F)$.

Observe that every intermediate field of E, F is strict and F-extending.

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

(Def. 6) E.

The functor $\deg(E, K)$ yielding an integer is defined by the term

(Def. 7) $\deg(\mathrm{FieldExt}(E, K), K)$.

Let E be an F-finite extension of F. One can check that $\mathrm{FieldExt}(E, K)$ is K-finite and every intermediate field of E, F is F-finite.

2. Sets of Groups

Let X be a set. We say that X is group-membered if and only if

(Def. 8) for every object x such that $x \in X$ holds x is a group.

Let G be a group. We say that X is G-subgroup-membered if and only if

(Def. 9) for every object x such that $x \in X$ holds x is a subgroup of G.

Note that there exists a set which is group-membered and non empty.

Let G be a group. Observe that there exists a set which is G-subgroup-membered and non empty and every set which is G-subgroup-membered is also group-membered and $\mathrm{SubGr}\, G$ is G-subgroup-membered and every subset of $\mathrm{SubGr}\, G$ is G-subgroup-membered.

Let X be a non empty, group-membered set.

One can verify that an element of X is a group. Let G be a group and X be a non empty, G-subgroup-membered set.

Let us observe that an element of X is a subgroup of G. Let H be a subgroup of G. Observe that $\{H\}$ is G-subgroup-membered.

Let H_1, H_2 be subgroups of G. Observe that $\{H_1, H_2\}$ is G-subgroup-membered.

A SubGroup of G is a subgroup of G defined by

(Def. 10) $it \in \mathrm{SubGr}\, G$.

Note that every SubGroup of G is strict and there exists a SubGroup of G which is finite. Let G be a finite group. Note that every SubGroup of G is finite. Let G be a group. We introduce the notation $\mathrm{order}\, G$ as a synonym of $\overline{\overline{G}}$.

3. Sets of Subfields and Intermediate Fields

Let F be a field and X be a set. We say that X is F-subfield-membered if and only if

(Def. 11) for every object x such that $x \in X$ holds x is a subfield of F.

Let E be an extension of F. We say that X is E-intermediate-membered if and only if

(Def. 12) for every object x such that $x \in X$ holds x is an intermediate field of E, F.

One can verify that there exists a set which is F-subfield-membered and non empty and every set which is F-subfield-membered is also field-membered and SubFields(F) is F-subfield-membered and every subset of SubFields(F) is F-subfield-membered.

Let E be an extension of F. One can verify that there exists a set which is E-intermediate-membered and non empty and every set which is E-intermediate-membered is also E-subfield-membered and IntermediateFields(E, F) is non empty and E-intermediate-membered and every subset of IntermediateFields(E, F) is E-intermediate-membered.

Let X be a non empty, F-subfield-membered set.

Let us note that an element of X is a subfield of F. Let E be an extension of F and X be a non empty, E-intermediate-membered set.

Note that an element of X is an intermediate field of E, F. Let E be a field and F be a subfield of E. Let us observe that $\{F\}$ is E-subfield-membered.

Let F_1, F_2 be subfields of E. Let us observe that $\{F_1, F_2\}$ is E-subfield-membered.

Let F be a field, E be an extension of F, and K be an intermediate field of E, F. One can check that $\{K\}$ is E-intermediate-membered.

Let K_1, K_2 be intermediate fields of E, F. Observe that $\{K_1, K_2\}$ is E-intermediate-membered.

Let L be a lattice. One can check that the functor LattRel(L) yields a binary relation on the carrier of L.

4. On Galois Connections

Let S, T be non empty relational structures, g be a function from S into T, and d be a function from T into S. Note that the functor $\langle g, d\rangle$ yields a connection between S and T. The functor Closed(g) yielding a non empty subset of T is defined by the term

(Def. 13) the set of all $g(o)$ where o is an element of S.

Let d be a function from T into S. The functor Restr(g, d) yielding a function from Closed(d) into Closed(g) is defined by the term

(Def. 14) $g\restriction$Closed(d).

The functor Restr(d, g) yielding a function from Closed(g) into Closed(d) is defined by the term

(Def. 15) $d\restriction$Closed(g).

Let us consider non empty posets S, T, a function g from S into T, and a function d from T into S. Now we state the propositions:

(2) Suppose $\langle g, d\rangle$ is co-Galois. Then

(i) $\mathrm{Restr}(g, d)$ is a bijection of $\mathrm{Closed}(d)$, $\mathrm{Closed}(g)$, and

(ii) $(\mathrm{Restr}(g, d))^{-1} = \mathrm{Restr}(d, g)$.

(3) Suppose $\langle g, d\rangle$ is co-Galois. Then

(i) $\mathrm{Restr}(d, g)$ is a bijection of $\mathrm{Closed}(g)$, $\mathrm{Closed}(d)$, and

(ii) $(\mathrm{Restr}(d, g))^{-1} = \mathrm{Restr}(g, d)$.

(4) Let us consider non empty posets S, T, a function g from S into T, and a function d from T into S. Suppose $\langle g, d\rangle$ is co-Galois. Let us consider an element s of S. Then $s \in \mathrm{Closed}(d)$ if and only if $d(g(s)) = s$.

(5) Let us consider non empty posets S, T, a function g from S into T, and a function d from T into S. Suppose $\langle g, d\rangle$ is co-Galois. Let us consider an element t of T. Then $t \in \mathrm{Closed}(g)$ if and only if $g(d(t)) = t$.

5. On the Lattice of Subgroups

Now we state the propositions:

(6) Let us consider a group G_1, a subgroup G_2 of G_1, subsets H_1, H_2 of G_1, and subsets H_3, H_4 of G_2. If $H_1 = H_3$ and $H_2 = H_4$, then $H_1 \cdot H_2 = H_3 \cdot H_4$.

(7) Let us consider a group G_1, a subgroup G_2 of G_1, a subset H_1 of G_1, and a subset H_2 of G_2. If $H_1 = H_2$, then $\mathrm{gr}(H_1) = \mathrm{gr}(H_2)$.

(8) Let us consider a group G_1, a subgroup G_2 of G_1, subgroups H_1, H_2 of G_1, and subgroups H_3, H_4 of G_2. Suppose $H_1 = H_3$ and $H_2 = H_4$. Then

(i) $H_3 \sqcup H_4 = H_1 \sqcup H_2$, and

(ii) $H_3 \cap H_4 = H_1 \cap H_2$.

The theorem is a consequence of (6) and (7).

Let G be a group. Observe that the carrier of $\mathbb{L}_G$ is G-subgroup-membered and the carrier of $\mathrm{Poset}(\mathbb{L}_G)$ is G-subgroup-membered.

Let M be a non empty, G-subgroup-membered set. The functors: $\bigcap M$ and $\bigcup M$ yielding strict subgroups of G are defined by conditions

(Def. 16) the carrier of $\bigcap M = \bigcap$ the set of all the carrier of H where H is an element of M,

(Def. 17) the carrier of $\bigcup M = \bigcap\{$the carrier of H, where H is an element of $\mathrm{SubGr}\, G$: for every group K such that $K \in M$ holds K is a subgroup of $H\}$,

respectively. Now we state the propositions:

(9) Let us consider a group G, a non empty, G-subgroup-membered set M, and an element H of M. Then $\bigcap M$ is a subgroup of H.

(10) Let us consider a group G, a non empty, G-subgroup-membered set M, and a subgroup K of G. Suppose for every element H of M, K is a subgroup of H. Then K is a subgroup of $\bigcap M$.

(11) Let us consider a group G, and a non empty, G-subgroup-membered set M. Then every element of M is a subgroup of $\bigcup M$.

(12) Let us consider a group G, a non empty, G-subgroup-membered set M, and an element K of $\mathrm{SubGr}\, G$. Suppose every element of M is a subgroup of K. Then $\bigcup M$ is a subgroup of K.

Let us consider a group G and subgroups H_1, H_2 of G. Now we state the propositions:

(13) $\bigcap\{H_1, H_2\} = H_1 \cap H_2$.

(14) $\bigcup\{H_1, H_2\} = H_1 \sqcup H_2$. The theorem is a consequence of (12) and (11).

Let G be a group. Observe that $\mathbb{L}_G$ is complete. Now we state the proposition:

(15) Let us consider a group G, and elements G_1, G_2 of the carrier of $\mathrm{Poset}(\mathbb{L}_G)$. Then $G_1 \leqslant G_2$ if and only if G_1 is a subgroup of G_2.

6. The Lattice of Intermediate Fields

Let E be a field and M be a non empty, E-subfield-membered set. The functors: $\bigcap M$ and $\bigcup M$ yielding strict subfields of E are defined by conditions

(Def. 18) the carrier of $\bigcap M = \bigcap$ the set of all the carrier of K where K is an element of M,

(Def. 19) the carrier of $\bigcup M = \bigcap\{$the carrier of K, where K is an element of SubFields(E) : for every field F such that $F \in M$ holds F is a subfield of $K\}$,

respectively. Now we state the propositions:

(16) Let us consider a field E, a non empty, E-subfield-membered set M, and an element F of M. Then $\bigcap M$ is a subfield of F.

(17) Let us consider a field E, a non empty, E-subfield-membered set M, and a subfield K of E. Suppose for every element F of M, K is a subfield of F. Then K is a subfield of $\bigcap M$.

(18) Let us consider a field E, and a non empty, E-subfield-membered set M. Then every element of M is a subfield of $\bigcup M$.

(19) Let us consider a field E, a non empty, E-subfield-membered set M, and an element K of SubFields(E). Suppose every element of M is a subfield of K. Then $\bigcup M$ is a subfield of K.

Let us consider a field F, an extension E of F, and a non empty subset M of IntermediateFields(E, F). Now we state the propositions:

(20) $\bigcap M$ is an intermediate field of E, F.

(21) $\bigcup M$ is an intermediate field of E, F. The theorem is a consequence of (18).

Let F be a field, E be an extension of F, and K_1, K_2 be intermediate fields of E, F. The functor $K_1 \sqcap K_2$ yielding an intermediate field of E, F is defined by the term

(Def. 20) $\bigcap\{K_1, K_2\}$.

Note that the functor is commutative.

The functor $K_1 \sqcup K_2$ yielding an intermediate field of E, F is defined by the term

(Def. 21) $\bigcup\{K_1, K_2\}$.

Let us note that the functor is commutative.

Let K be an intermediate field of E, F. One can verify that $K \sqcap K$ reduces to K and $K \sqcup K$ reduces to K.

Let us consider a field F, an extension E of F, and intermediate fields K_1, K_2 of E, F. Now we state the propositions:

(22) $K_1 \sqcap (K_1 \sqcup K_2) = K_1$. The theorem is a consequence of (18).

(23) $(K_1 \sqcap K_2) \sqcup K_2 = K_2$. The theorem is a consequence of (16).

(24) $K_1 \sqcap K_2 = K_2 \sqcap K_1$.

(25) $K_1 \sqcup K_2 = K_2 \sqcup K_1$.

Let us consider a field F, an extension E of F, and intermediate fields K_1, K_2, K_3 of E, F. Now we state the propositions:

(26) $(K_1 \sqcap K_2) \sqcap K_3 = K_1 \sqcap (K_2 \sqcap K_3)$.

(27) $(K_1 \sqcup K_2) \sqcup K_3 = K_1 \sqcup (K_2 \sqcup K_3)$. The theorem is a consequence of (18) and (19).

Let us consider a field F, an extension E of F, and intermediate fields K_1, K_2 of E, F. Now we state the propositions:

(28) $K_1 \sqcap K_2 = K_1$ if and only if K_1 is a subfield of K_2. The theorem is a consequence of (17) and (16).

(29) $K_1 \sqcup K_2 = K_2$ if and only if K_1 is a subfield of K_2. The theorem is a consequence of (19) and (18).

Let F be a field and E be an extension of F. The functors: SubMeet E and SubJoin E yielding binary operations on IntermediateFields(E, F) are defined by conditions

(Def. 22) for every intermediate fields K_1, K_2 of E, F, SubMeet $E(K_1, K_2) = K_1 \sqcap K_2$, (Def. 23) for every intermediate fields K_1, K_2 of E, F, SubJoin $E(K_1, K_2) = K_1 \sqcup K_2$,

respectively. The functor IntermediateFields(E) yielding a lattice is defined by the term

(Def. 24) $\langle$IntermediateFields(E, F), SubJoin E, SubMeet $E\rangle$.

One can check that the carrier of IntermediateFields(E) is non empty and E-intermediate-membered.

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

(30) $\top_{\text{IntermediateFields}(E)}$ = the double loop structure of E. The theorem is a consequence of (18).

(31) $\perp_{\text{IntermediateFields}(E)}$ = the double loop structure of F. The theorem is a consequence of (16) and (17).

Let F be a field and E be an extension of F. One can verify that IntermediateFields(E) is complete and the carrier of Poset(IntermediateFields(E)) is non empty and E-intermediate-membered. Now we state the proposition:

(32) Let us consider a field F, an extension E of F, and elements K_1, K_2 of the carrier of Poset(IntermediateFields(E)). Then $K_1 \leqslant K_2$ if and only if K_1 is a subfield of K_2. The theorem is a consequence of (28).

7. Sets of Functions of Rings

Let R be a ring and X be a set. We say that X is R-functional if and only if

(Def. 25) for every object o such that $o \in X$ holds o is a function from R into R.

Let L be a 1-sorted structure. We say that L is R-functional if and only if

(Def. 26) the carrier of L is R-functional.

Observe that there exists a set which is non empty and R-functional.

Let X be an R-functional set. Note that every subset of X is R-functional.

Let X be a non empty, R-functional set.

One can check that an element of X is a function from R into R. Let us observe that there exists a 1-sorted structure which is non empty and R-functional.

Let L be an R-functional 1-sorted structure. Let us note that every subset of L is R-functional.

Let L be a non empty, R-functional 1-sorted structure. One can check that the carrier of L is R-functional.

Let S be a ring extension of R. Note that there exists a function from S into S which is R-fixing and id_S is R-fixing.

Let f, g be R-fixing functions from S into S. Let us note that $f \cdot g$ is R-fixing as a function from S into S.

Let f be an R-fixing function from S into S and n be a natural number. Let us observe that f^n is R-fixing as a function from S into S.

Let f be an R-fixing, one-to-one function from S into S. Note that f^{-1} is R-fixing and one-to-one as a function from S into S.

8. On Homomorphisms from $R[X]$ to $R[X]$

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. One can verify that the functor $f^{\circ}S$ yields a non empty, finite subset of Y. Let R be a ring and h be an additive function from R into R. The functor PolyHom(h) yielding a function from Polynom-Ring R into Polynom-Ring R is defined by

(Def. 27) for every element f of the carrier of Polynom-Ring R and for every natural number i, $(it(f))(i) = h(f(i))$.

Let h be a homomorphism of R. Let us observe that PolyHom(h) is additive, multiplicative, and unity-preserving.

Let us consider a ring R and a homomorphism h of R. Now we state the propositions:

(33) $(\mathrm{PolyHom}(h))(\mathbf{0}.R) = \mathbf{0}.R$.

(34) $(\mathrm{PolyHom}(h))(\mathbf{1}.R) = \mathbf{1}.R$.

Let us consider a ring R, a homomorphism h of R, and elements p, q of the carrier of Polynom-Ring R. Now we state the propositions:

(35) $(\mathrm{PolyHom}(h))(p+q) = (\mathrm{PolyHom}(h))(p) + (\mathrm{PolyHom}(h))(q)$.

(36) $(\mathrm{PolyHom}(h))(p \cdot q) = (\mathrm{PolyHom}(h))(p) \cdot (\mathrm{PolyHom}(h))(q)$.

(37) Let us consider a ring R, a homomorphism h of R, an element p of the carrier of Polynom-Ring R, and an element a of R. Then $(\mathrm{PolyHom}(h))(a \cdot p) = h(a) \cdot (\mathrm{PolyHom}(h))(p)$.

(38) Let us consider a ring R, a homomorphism h of R, an element p of the carrier of Polynom-Ring R, and an element x of R. Then $h(\mathrm{eval}(p,x)) = \mathrm{eval}((\mathrm{PolyHom}(h))(p), h(x))$.

(39) Let us consider an integral domain R, a homomorphism h of R, an element p of the carrier of Polynom-Ring R, and elements a, x of R. Then $h(\mathrm{eval}(a \cdot p, x)) = h(a) \cdot (\mathrm{eval}((\mathrm{PolyHom}(h))(p), h(x)))$.

(40) Let us consider a field F, an extension E of F, an element p of the carrier of Polynom-Ring F, an element a of E, and an F-fixing homomorphism h of E. Then $h(\mathrm{ExtEval}(p,a)) = \mathrm{ExtEval}(p, h(a))$.

Let us consider a ring R, a monomorphism h of R, and an element p of the carrier of Polynom-Ring R. Now we state the propositions:

(41) $\deg((\mathrm{PolyHom}(h))(p)) = \deg(p)$.

(42) $\mathrm{LM}((\mathrm{PolyHom}(h))(p)) = (\mathrm{PolyHom}(h))(\mathrm{LM}(p))$. The theorem is a consequence of (41).

(43) Let us consider a field F, a homomorphism h of F, and an element a of F. Then $(\mathrm{PolyHom}(h))(\mathrm{X}-a) = \mathrm{X}-h(a)$.

(44) Let us consider a field F, a non empty, finite subset S of F, a product of linear polynomials p of F and S, and a monomorphism h of F. Then $(\mathrm{PolyHom}(h))(p)$ is a product of linear polynomials of F and $h^\circ S$.

(45) Let us consider a field F, an extension E of F, a non empty subset S of E, and an automorphism h of E. Suppose $h^\circ S = S$. Then

  (i) $h \restriction S$ is a permutation of S, and

  (ii) $h^{-1} \restriction S$ is a permutation of S.

References

[1] Grzegorz Bancerek and Piotr Rudnicki. A Compendium of Continuous Lattices in Mizar. *Journal of Automated Reasoning*, 29(3–4):189–224, 2002. doi:10.1023/A:1021966832558.

[2] Garrett Birkhoff. *Lattice Theory.* Providence, Rhode Island, New York, 1967.

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

[4] Adam Grabowski. Mechanizing complemented lattices within Mizar system. *Journal of Automated Reasoning*, 55:211–221, 2015. doi:10.1007/s10817-015-9333-5.

[5] 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.

[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] George Grätzer. *Lattice Theory: Foundation.* Birkhäuser, 2011.

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

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

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

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

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

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

Received July 9, 2025, Accepted December 12, 2025