

FedCSIS_2023_paper_3409.pdf

Developing Field Theory in Mizar

¹
Christoph Schwarzweller

Institute of Informatics, Faculty of Mathematics, Physics and Informatics,
University of Gdańsk,
Wita Stwosza 57, 80-952 Gdańsk, Poland
christoph.schwarzweller@inf.ugl

³⁵

Abstract—As part of our ongoing project to prove Artin's solution of Hilbert's 17th problem ¹ in Mizar we are formalizing a great deal of basic field – and Galois – theory ¹⁶. In this paper we report on our formalization so far: we present basic mathematical structures and our Mizar definitions enriched with some main results. We also discuss some of our design decisions as well as subtleties – in particular connected with Mizar types.

¹

I. INTRODUCTION

INTERACTIVE theorem proving aims at developing systems to be used to formalize, that is both formulate and prove, mathematical theorems and theories in an accurate and comfortable way. The ultimate dream is a system containing all mathematical knowledge in which also mathematicians develop and prove new theorems. To come at least a little closer to this goal much effort has been spent building large repositories of computer-verified theorems such as the Coq library ⁷, the Isabelle2017 library ¹⁵, and the Mizar Mathematical Library ¹⁷. A number of important mathematical theorems have been proven to illustrate the capability of interactive theorem proving, the most prominent examples being the proof of Kepler's conjecture in HOL Light ¹³, the Feit-Thompson theorem in Coq, and the Jordan curve theorem in Mizar.

Mizar ², ¹¹ is one of the pioneering systems for formalizing mathematics, after 50 years Mizar's proof checker still is actively developed and its library maintained and extended. One of the latest achievements in Mizar is the proof of the MRDP theorem solving Hilbert's 10th ⁵ problem in the negative ¹⁹. Another challenging problem is Hilbert's 17th problem: Given a multivariate polynomial that takes only non-negative values over the reals, can it be represented as a sum of squares of rational functions? Artin's positive solution ¹ is a highlight in abstract algebra, introducing what today is known as formally real fields and initiated the development of real algebra.

Soon after starting the formalization of formally real fields it became clear that much more field theory is necessary than expected: not only field extensions and algebraically closed fields, but also basic Galois theory. Therefore we decided to formalize what usually appears in a on ¹³ semester graduate course on higher algebra ²⁰, ⁹, ²¹. The main results of our formalization so far are

- 1) existence and uniqueness of splitting fields

- 2) existence and uniqueness of algebraic closures
- 3) simple extensions (characterization by intermediate fields, finite field extensions of characteristic 0 are simple)
- 4) normal extensions (characterization by minimal polynomials, splitting fields, and fixing monomorphisms, counter example $\mathbb{Q}(\sqrt[3]{2})$)
- 5) separable extensions (finite field extensions of characteristic 0 are separable, counter examples $X^p - a$ for characteristic p , finite ⁴² fields are perfect)
- 6) formally and maximal formally real fields (formally real fields are exactly the ordered fields, sums of squares are exactly the total positive elements, real closed fields are maximal formally real)

¹³

The complete formalization with entire proofs can be found in the Mizar Mathematical Library in the article series FIELD_xx and REALALG_xx.

⁵

Related Work Formalizations of both field and Galois theory have been performed in different proof assistants: In Coq Galois theory has been ¹⁷ developed to prove the Abel-Ruffini theorem ⁴ and also real closed ⁵ fields can be found in ⁶. Lean provides the theory up to the fundamental theorem of Galois theory ⁵. General field ⁵ theory also has been formalized in Isabelle - in particular the existence of algebraic closures of fields has been proved ⁸.

¹

II. THE MIZAR SYSTEM

Mizar has often been described ¹ in the literature, for example in ¹⁸, ¹², ¹¹ and ³. In this paper we will present only theorems, not proofs; therefore we give only a very rough description of Mizar. Mizar's logical basis is classical ¹ first-order logic, extended with so-called schemes. Schemes introduce free second-order variables enabling the definition of induction schemes among others. In addition, Mizar objects are typed, the types forming a hierarchy with the fundamental type *set*. The user can introduce new (sub)types describing mathematical objects such as groups, fields, vector spaces, or polynomials over rings or fields. The development of the Mizar Mathematical Library relies on Tarski-Grothendieck set theory – a variant of Zermelo-Fraenkel set theory using Tarski's axiom about arbitrarily large, strongly inaccessible cardinals which can be used to prove the axiom of choice. Mizar proofs

are written in natural deduction style. The rules of the calculus are connected with corresponding (English) natural language phrases so that the Mizar language is close to the one used in mathematical textbooks.

To define algebraic domains Mizar provides so-called structure modes fixing the domain's sets of elements and operations. So, for example (Throughout the paper Mizar code is written in verbatim style.)

```
definition
  struct (addLoopStr,multLoopStr_0) doubleLoopStr
  (# carrier -> set,
    addF, multF -> BinOp of the carrier,
    OneF, ZeroF -> Element of the carrier #);
end;
```

defines the necessary backbone of rings and fields. Note that doubleLoopStr inherits from both addLoopStr and multLoopStr_0, that is it joins the operations of additive and multiplicative groups. Properties such as commutativity or the existence of inverse elements are described by attribute definitions such as

```
definition
  let R be addLoopStr;
  attr R is right_zeroed means
    for a being Element of R holds a + 0.R = a;
end;
```

Here for elements a and b of (the carrier) of R $a+b$ is a shortcut for (the addF of R). (a,b) . A field then is defined as a doubleLoopStr with the appropriate collection of attributes (compare [10]).

```
definition
  mode Field is
    Abelian add-associative right_zeroed
    right_complementable associative commutative
    well-unital almost_left_invertible
    distributive non empty doubleLoopStr;
end;
```

As a consequence a Mizar object of type Field obtains all properties described by the defining attributes. We note here, that Mizar types have to be non-empty, so that each mode definition requires an existence proof.

Concrete algebraic domains are built by instantiation of structures. The field of rational numbers $\mathbb{Q}$, for example, is given by the set RAT of rational numbers and operations addrat and multirat defining addition and multiplication for elements of RAT. These are then glued together by the following

```
definition
  func F_Rat -> Field equals
    doubleLoopStr (#RAT,addrat,multirat,1,0#);
end;
```

Note, that using the set RAT in defining the field F_Rat gives a particular representation of the rational numbers $\mathbb{Q}$ to be used when arguing about the rational numbers using the field F_Rat. Of course there are other fields, that is fields with a different set of elements, isomorphic to $\mathbb{Q}$. In fact any field of characteristic 0 contains a subfield isomorphic to $\mathbb{Q}$.

so that every field of characteristic 0 can be considered as a field extension of $\mathbb{Q}$.

III. FIELD EXTENSIONS AND FIELD ADJUNCTIONS

If F is a subfield of E then E is called a (field) extension of F . Note that this definition in particular means that the elements of F are a subset of the elements of E . Subfields (and subrings) already have been defined in Mizar, so we get

```
definition
  let R,S be Ring;
  attr S is R-extending means
    R is Subring of S;
end;

definition
  let F be Field;
  mode FieldExtension of F is F-extending Field;
end;
```

Note that in the definition instead of postulating that F is a subfield of E we demand that a ring R is a subring of another ring S . In this way our definition gets more flexible. For example, this allows to show that $\mathbb{Q}$ extends $\mathbb{Z}$. For a fields, however, our definition is equivalent to the one from the literature given above, as stated by the following

```
theorem
  for F,E being Field
  holds E is FieldExtension of F iff
    F is Subfield of E;
```

There is an alternative equivalent definition saying that F embeds into E . In human mathematics it's obvious to switch between these two – ignoring usually the embedding. We decided to use the first option as it makes it easier to consider polynomials of F as polynomials of E (and also makes it more straightforward to define F -fixing morphisms needed later): In Mizar a polynomial of E must have coefficients of type E . Thus the second option would require to take care of the embedding φ : not p , but $\varphi(p)$ then is a polynomial of E .

However, even though an element $a \in F$ can naturally be considered as an element of E , this has to be made explicit in a typed system like Mizar: for a being an element of F and b an element of E the term $a+b$ is not defined as a and b must have the same type. This type can be element of E or element of F , if b turns out to be in F . In Mizar type casts are realized with the help of the reconsider-statement for changing types of objects, or one defines a functor for changing types, usually denoted by $@$. In both cases the result is independent of the field, that is for $a,b \in F$ we get

```
a + b = @(a,E) + @(b,E);
reconsider a1 = a, b1 = b as Element of E;
a + b = a1 + b1;
```

Both versions now allow to shift from one field to another. Note that this also works in powers of fields. For $T \subseteq E$ the adjunction of F with T is the smallest extension of F containing T . Thus $F(T)$ is both an extension of F and E

is an extension of $F(T)$. To "attach" both types to $F(T)$ we defined the type of $\text{FAdj}(F, T)$ as subfield of E :

```

3 definition
  let F be Field, E be FieldExtension of F;
  let T be Subset of E;
  func FAdj(F,T) -> Subfield of E means ...;
end;

```

Then the type of the field E can be easily changed into $\text{FieldExtension of FAdj}(F, T)$, if necessary. Because Mizar's typing mechanism allows to enrich types with further attributes the type of $\text{FAdj}(F, T)$ can be "extended" with F -extending, hence then is $\text{FieldExtension of F}$. Note that this typing is necessary to prove $F(T_1 \cup T_2) = F(T_1)(T_2)$ for $T_1, T_2 \subseteq E$, because then E must have type $\text{FieldExtension of F}(T_1)$ on the right-hand side – in contrast to $\text{FieldExtension of F}$ on the left-hand side.

IV. SPLITTING FIELDS

21 A splitting field of a polynomial $p \in F[X]$ is an extension E in which p splits into linear factors and is generated by p 's roots, e.g. $E = F(\alpha_1 \dots \alpha_n)$ where the α_i are the roots of p – or equivalently a smallest field extension of F in which p splits:

```

3 definition
  let F be Field;
  let p be non constant Polynomial of F;
  mode SplittingField of p
  3 -> FieldExtension of F means
    p splits in it &
    for E being FieldExtension of F
      st p splits in E & E is Subfield of it
      holds E == it;

```

Note again that in Mizar a mode definition requires an existence (but no uniqueness) proof, because the introduced type – here $\text{SplittingField of p}$ – is not allowed to be empty. Our proof follows [20] and does not use algebraic closures: Iterating Kronecker's construction [22] ensures that there exists an extension of F in which p splits, so one easily shows that there is a smallest one – of course this then is the extension of F generated by p 's roots. Consequently, that a splitting field of p is generated by the roots of p now follows as a theorem.

```

3 theorem
  for F being Field
  for p being non constant Polynomial of F
  for E being SplittingField of p
  holds E = FAdj(E, Roots(E, p));
43

```

To prove uniqueness of splitting fields we introduced the notion of being isomorphic over a field F , e.g. there is an isomorphism that fixes the elements of F . Note that such an isomorphism also fixes polynomials $p \in F[X]$. We then lifted isomorphisms from $F_1 \rightarrow F_2$ to $F_1(\{a\}) \rightarrow F_2(\{b\})$ where a and b are algebraic elements of F_1 and F_2 respectively.

Because splitting fields are generated by roots of a polynomial, hence by algebraic elements, then follows

```

3 theorem
  for F being Field
  for p being non constant Polynomial of F
  for E1, E2 being SplittingField of p
  holds E1, E2 are_isomorphic_over F;
29

```

so a splitting field of a non-constant polynomial is unique up to isomorphism.

V. ALGEBRAIC CLOSURES

2 An algebraic closure A of F is an extension of F which is both algebraic closed and algebraic over F , that is every non-constant polynomial of A has a root and every element $a \in A$ is the root of a non-zero polynomial of F .

Our proof follows Artin's classical one as presented by Lang in [16]: Kronecker's construction is applied to each polynomial $p \in F[X] \setminus F$ simultaneously to get an extension E of F in which every non-constant polynomial $p \in F[X]$ has a root in E . For that we need the polynomial ring $F[X_1, X_2, \dots]$ with infinitely many variables, one for each polynomial $p \in F[X] \setminus F$. The sought-after field extension E then is (isomorphic to) $F[X_1, X_2, \dots]/I$, where I is a maximal ideal generated by all non-constant polynomials $p \in F[X]$. Note that to show that I is maximal Zorn's lemma is necessary.

Iterating this construction gives an infinite sequence of fields, whose union defines an extension A of F , in which every non-constant polynomial $p \in A[X]$ has a root. The field of algebraic elements of A then is an algebraic closure of F . With this existence proof we can define

```

1 definition
  let F be Field;
  mode AlgebraicClosure of F
  -> FieldExtension of F means
    it is F-algebraic &
    it is algebraic-closed;
45

```

To prove uniqueness of algebraic closures again the technique of lifting morphisms is applied: a monomorphism $F \rightarrow A$, where A is an algebraic closure of F can be extended to a monomorphism $E \rightarrow A$, where E is any algebraic extension of F . In case that E is algebraically closed this monomorphism is an isomorphism.

```

3 theorem
  for F being Field
  for A1, A2 being AlgebraicClosure of F
  holds A1, A2 are_isomorphic_over F;
2

```

Note that the existence of the lifted monomorphism again relies on Zorn's lemma.

VI. SIMPLE EXTENSIONS

8 An extension E of a field F is simple if E is generated over F by a single element $a \in E$, e.g. $E = F(\{a\})$. The element a then is a primitive element.

```

definition
  let F be Field, E be FieldExtension of F;
  attr E is F-simple means
    ex a being Element of E st E == FAdj(F, {a});
end;

```

For finite fields F we proved that a finite extension E of F is simple if and only if the number of intermediate fields between E and F is finite. In Mizar the intermediate fields of given fields E and F can be defined as a functor giving the appropriate set: because the elements of such a field must be a subset of the elements of E , one can pick up the subsets of the elements of E which constitute a field using Mizar's replacement-scheme.

```

theorem
  for F being infinite Field
  for E being F-finite FieldExtension of F
  holds E is F-simple iff
    IntermediateFields(E, F) is finite;

```

The theorem holds for finite fields. The proof, however, follows easily from group theory, in particular every finite extension of a finite field is simple.

For fields with characteristic zero we also proved that a linear combination of a and b generates $F(a, b)$ – in fact in doing so we already showed that in fields with characteristic 0 irreducible polynomials are separable.

```

theorem
  for F being 0-characteristic Field
  for E being FieldExtension of F
  for a, b being F-algebraic Element of E
  ex x being Element of F
  st FAdj(F, {a, b}) = FAdj(F, {a + @ (x, E) * b});

```

Note that to take the element x from F we again have to shift x into E using the functor $@$.

VII. NORMAL EXTENSIONS

An extension E of F is normal, if every polynomial over F that has a root in E – or equivalently every minimal polynomial – already splits in E . There is a number of equivalent characterizations of (finite) normal extensions (usually shown in a ring proof), for example, that normal extensions are given by splitting fields of polynomial $p \in F[X]$:

```

theorem
  for F being Field,
  E being F-finite FieldExtension of F
  holds E is F-normal iff
    ex p being non constant Polynomial of F
    st E is SplittingField of p;

```

One direction of this theorem can now be described using types (and therefore be automated) by using Mizar's cluster mechanism:

```

registration
  let F be Field;
  let p be non constant Polynomial of F;
  cluster -> F-normal for SplittingField of p;
end;

```

Then the type SplittingField of p is extended to F -normal FieldExtension of F instead of only FieldExtension of F , so all theorems about normal can be automatically applied.

Another important characterization deals with fixing morphisms. It states that for (finite) normal extensions E an F -fixing monomorphism $h : E \rightarrow K$ into a bigger field K actually maps to E only, and therefore is an isomorphism.

```

theorem
  for F being Field
  for E being F-finite FieldExtension of F
  holds E is F-normal iff
    for K being FieldExtension of E
    for h being F-fixing Monomorphism of E, K
    holds h is Automorphism of E;

```

The proof turned out to be quite technical because one needs to show $h(E) = h(F(\{a_1, \dots, a_n\})) \subseteq F(\{h(a_1), \dots, h(a_n)\})$. In human mathematics this is almost obvious just because every element $a \in F(\{a_1, \dots, a_n\})$ is given by $p(a_1, \dots, a_n)$ for some polynomial $p \in F[X_1, \dots, X_n]$. The formal proof in Mizar is by induction on the degree of multivariate polynomials and hence needs to reduce the degree of a multivariate polynomial in order to apply the induction hypothesis.

VIII. SEPARABLE EXTENSIONS

A polynomial $p \in F[X]$ is separable, if p has no multiple roots in the (any) splitting field of p . This is equivalent to p being coprime with its formal derivative. An algebraic extension E of F is separable, if for all $a \in E$ the minimal polynomial μ_a is separable.

```

definition
  let F be Field
  let p be non constant
  Element of the carrier of Polynom-Ring F;
  attr p is separable means
    for a being
      Element of the SplittingField of p
    st a is_a_root_of p, (the SplittingField of p)
    holds multiplicity(p, a) = 1;
end;

```

Note the use of the the-operator in the following definition which nicely puts into mind the fact that a splitting field is unique up to isomorphism. This, unfortunately, is not expressed by the definition as the just takes an arbitrary element of the non-empty type SplittingField of p . All the obvious properties about polynomials over isomorphic fields nevertheless have to be proved. In particular the fact that separability indeed is independent of the splitting field is established not until the following

```

theorem
  for F being Field,
  p being non constant Polynomial of F
  holds p is separable iff
    ex E being FieldExtension of F
    st p splits_in E &

```

```

for a being Element of E
  holds multiplicity(p,a) <= 1;

```

In fields with characteristic 0 every irreducible polynomial p is separable (such fields are called perfect), because p must be square-free to be relatively prime with its formal derivation. In fields with prime characteristic p , however, the polynomial $X^p - a$ is irreducible only if a has a p -th root and then equals $(X - a)^p$. In the other case $X^p - a$ is irreducible and because $\sqrt[p]{a}$ is a p -fold root of $X^p - a = (X - \sqrt[p]{a})^p$ in its splitting field we get

```

theorem
  for p being Prime
  for F being p-characteristic Field
  for a being Element of F
  st not a in F^p
  holds X^p - a is irreducible inseparable;

```

where F^p denotes the subfield F^p of all p -th roots in F . Indeed, $F^p = F$ if and only all irreducible polynomials of F are separable, which we applied to finally prove that every finite field is perfect. On the other hand the field $F_p(X)$ of rational functions over a field F_p with characteristic $p \neq 0$ is not perfect.

IX. FORMALLY REAL FIELDS

Finally we return to our original motivation of formalizing formally real fields and Artin's solution of Hilbert's 17th problem. A field F is formally real, if -1 is not a sum of squares. In this – and only this – case F can be ordered. Here, orders are usually defined as positive cones – the set of positive elements [21]. Note that formally real fields have characteristic 0. A first main result from [1] we proved states, that the elements of F that can be described as sums of squares are exactly the total positive ones:

```

theorem
  for F being formally_real Field
  for a being Element of F
  holds a in Quadratic_Sums_of F iff
    for P being Ordering of F holds a in P;

```

So, to solve Hilbert's 17th problem it's crucial to identify the total positive elements of the real numbers. In general fields all for different orderings. Maximal formally real fields F – in the sense that there is no proper extension of F which again is formally real – however, have only one ordering – the set of squares $SQ F$:

```

definition
  let F be Field;
  attr F is maximal_formally_real means
    F is formally_real &
    for E being F-algebraic FieldExtension of F
    st E is formally_real holds E == F;
end;

```

```

theorem
  for F being maximal_formally_real Field holds
    SQ F is Ordering of F &
    for P being Ordering of F holds P = SQ F;

```

So far we proved that in maximal formally real fields every polynomial of odd degree has a root and that the field of real numbers is maximal formally real. Maximal formally real fields F then are characterized as real closed fields: a field F is real closed iff the splitting field of the polynomial $X^2 + 1 \in F[X]$ – e.g. the field $F(i)$ – is an algebraic closure of F .

```

definition
  let F be Field;
  attr F is real_closed means
    not -1.F in SQ F &
    the SplittingField of X^2+1.F
      is algebraic-closed;
end;

```

Note that this definition does not make use of orderings. So far we proved that real closed fields are maximal formally real. The main part here was to show that for real closed fields the set of squares is an ordering – maximality is straightforward from the definition and the fact that algebraic complete fields are not formally real.

The other direction – that maximal formally real fields are real closed – is proved by showing that for fields F , in which both the set of squares is an ordering and every polynomial of odd degree has a root, the extension $F(i)$ is algebraic closed. This requires the development of Galois theory necessary in order to show that the splitting field of a non-constant polynomial $p \in F(i)[X]$ indeed must be $F(i)$ [16], [21].

X. CONCLUSION AND FURTHER WORK

We have presented the beginnings of formalizing field and Galois theory in Mizar. Three main lessons of our Mizar formalization so far we consider worth mentioning: Mathematical types such as rings, fields, vector spaces, topological spaces, and so forth are usually considered helpful in proof assistants as they automate applying theorems. However when it comes to field extensions where objects such as elements, subsets, and polynomials are shifted between different fields, it's often necessary to explicitly cast types in order to apply definitions or theorems.

Secondly, dealing with (multivariate) polynomials tends to cause much more work than expected: many properties considered as obvious by human mathematics require a step-by-step formalization resulting in a number of technical lemmas.

Thirdly, the omnipresent "uniqueness up to isomorphism" also increases the formalization's length: each property carrying over to isomorphic fields has to be explicitly stated and proved.

The next step of our formalization will be the combination of normal and separable extensions to establish Galois extensions. Developing Galois theory will enable to further extend the formalization of real algebra. In particular the fundamental theorem of Galois theory will allow to conclude the proof that maximal formally real fields are real closed as a main step towards Artin's solution of Hilbert's 17th problem.

REFERENCES

- [1] E. Artin, *Über die Zerlegung definiter Funktionen in Quadrate*; Abh. Math. Sem. Univ. Hamburg 5(1), pp. 100–115, 1927.
- [2] G. Bancerek et al., *Mizar: State-of-the-art and Beyond*, in: M. Kerber et al. (eds.), *Proceedings of the 2015 International Conference on Intelligent Computer Mathematics*, Lecture Notes in Computer Science 10, pp. 261–279, 2015, http://dx.doi.org/10.1007/978-3-319-20615-8_17.
- [3] G. Bancerek, C. Bylinski, A. Grabowski, A. Kornilowicz, R. Matuszewski, A. Naumowicz, and K. Pak, *The Role of the Mizar Mathematical Library for Interactive Proof Development in Mizar*; Journal of Automated Reasoning, vol. 61(1-4), pp. 9–32, 2018.
- [4] S. Bernard, C. Cohen, and A. Mahboubi and P. Strub, *Unsolvability of the Quintic Formalized in Dependent Type Theory*, available at <https://hal.inria.fr/hal-03136002>, 2021.
- [5] T. Browning and P. Lutz, *Formalizing Galois Theory*; Experimental Mathematics, vol. 31(2), pp. 413–424 2022.
- [6] C. Cohen, *Construction of Real Algebraic Numbers in Coq*, in: ITP - 3rd International Conference on Interactive Theorem Proving, pp. 67–72, 2012.
- [7] *Coq Proof Assistant*, available at www.coc.inria.fr.
- [8] P.E. de Vilhena and L.C. Paulson, *Algebraically Closed Fields in Isabelle/HOL* in: *Automated Reasoning. IJCAR 2020*, Lecture Notes in Computer Science 12167, pp. 57–64, 2020.
- [9] A. Gathmann, *Einführung in die Algebra*; Lecture notes, University of Kaiserslautern, Germany, 2010.
- [10] A. Grabowski, A. Kornilowicz, and A. Naumowicz, *Mizar in a Nutshell*, Journal of Formalized Reasoning 3(2), 153–245, 2010, <https://doi.org/10.6092/issn.1972-5787/1980>.
- [11] A. Grabowski, A. Kornilowicz, and C. Schwarzweiller, *On Algebraic Hierarchies in Mathematical Repository of Mizar*, in: *Proceedings of the 2016 Federated Conference on Computer Science and Information Systems*, M. Ganzha, L. Maciaszek, M. Paprzycki (eds.), ACSIS, Vol. 8, pp. 363–371, 2016, <http://dx.doi.org/10.15439/2016F520>.
- [12] A. Grabowski, A. Kornilowicz, and A. Naumowicz, *Four Decades of Mizar*, Journal of Automated Reasoning, vol. 55(3), 191–198, 2015, <http://dx.doi.org/10.1007/s10817-015-9345-1>.
- [13] J. Harrison, *The HOL Light Theorem Prover*, available at www.cl.cam.ac.uk/~jrh13/hol-light.
- [14] *The HOL Interactive Theorem Prover*, available at hol-theorem-prover.org.
- [15] *Isabelle*, available at isabelle.in.tum.de.
- [16] H. Lang, *Algebra*, 3rd edition, Springer Verlag, 2002.
- [17] *Mizar Home Page*, available at www.mizar.org.
- [18] A. Naumowicz and A. Kornilowicz, *A Brief Overview of Mizar*, in: *Theorem Proving in Higher Order Logics 2009*, S. Berghofer, T. Nipkow, C. Urban, M. Wenzel (eds.), Lecture Notes in Computer Science, 5674, pp. 67–82, Springer Verlag, 2009.
- [19] K. Pak, *Formalization of the MRDP-Theorem in the Mizar System*, Formalized Mathematics, vol. 27(2), pp. 209–222, 2019.
- [20] K. Radbruch, *Algebra I*; Lecture notes, University of Kaiserslautern, Germany, 1990.
- [21] K. Radbruch, *Geometrie Körper*; Lecture notes, University of Kaiserslautern, Germany, 1991.
- [22] C. Schwarzweiller, *Representation Matters: An Unexpected Property of Polynomial Rings and its Consequences for Formalizing Abstract Field Theory*, in: M. Ganzha, L. Maciaszek, M. Paprzycki (eds.), *Proceedings of the 2018 Federated Conference on Computer Science and Information Systems*, ACSIS, vol. 15, pp. 67–72, 2018.

50%

SIMILARITY INDEX

PRIMARY SOURCES

1	annals-csis.org Internet	1067 words — 23%
2	repozytorium.uwb.edu.pl Internet	211 words — 4%
3	mizar.uwb.edu.pl Internet	200 words — 4%
4	mizar.org Internet	86 words — 2%
5	arxiv.org Internet	56 words — 1%
6	Dirk Hachenberger, Dieter Jungnickel. "Topics in Galois Fields", Springer Science and Business Media LLC, 2020 Crossref	48 words — 1%
7	inf.ug.edu.pl Internet	43 words — 1%
8	fm.mizar.org Internet	39 words — 1%
9	people.math.sc.edu Internet	37 words — 1%

10 Hirota Taniguchi, Kazuhisa Nakasho. "Visual Studio Code Extension and Auto-completion for Mizar Language", 2021 Ninth International Symposium on Computing and Networking (CANDAR), 2021

Crossref

35 words — 1%

11 www.researchgate.net

Internet

30 words — 1%

12 David A. Cox. "Galois Theory", Wiley, 2004

Crossref

27 words — 1%

13 ipfs.io

Internet

25 words — 1%

14 Nicolas Bourbaki. "Algebra II", Springer Science and Business Media LLC, 2003

Crossref

24 words — 1%

15 R. Kochendörffer. "Introduction to Algebra", Springer Science and Business Media LLC, 1981

Crossref

24 words — 1%

16 Adam Grabowski, Artur Kornilowicz, Christoph Schwarzweller. "On algebraic hierarchies in mathematical repository of Mizar", 'Polish Information Processing Society PTI', 2016

Internet

23 words — < 1%

17 Nathan Jacobson. "Lectures in Abstract Algebra", Springer Science and Business Media LLC, 1964

Crossref

22 words — < 1%

18 Antoine Chambert-Loir. "(Mostly) Commutative Algebra", Springer Science and Business Media LLC, 2021

Crossref

21 words — < 1%

19	Real Algebraic Geometry, 1998. Crossref	20 words — < 1%
20	radar.inria.fr Internet	19 words — < 1%
21	drops.dagstuhl.de Internet	18 words — < 1%
22	raweb.inria.fr Internet	18 words — < 1%
23	www.qucosa.de Internet	18 words — < 1%
24	"Algebra", Springer Nature, 2006 Crossref	17 words — < 1%
25	Thomas Browning, Patrick Lutz. "Formalizing Galois Theory", Experimental Mathematics, 2021 Crossref	17 words — < 1%
26	Todd K. Moon. "Error Correction Coding", Wiley, 2005 Crossref	17 words — < 1%
27	Christoph Schwarzweller, Agnieszka Rowińska- Schwarzweller. "Algebraic Extensions", Formalized Mathematics, 2021 Crossref	16 words — < 1%
28	Cornerstones, 2006. Crossref	15 words — < 1%
29	Eie, . "All About Roots", A Course On Abstract Algebra, 2010. Crossref	14 words — < 1%

- | | | |
|-------|---|-----------------|
| 30 | Grundlehren der mathematischen Wissenschaften, 1985.
<small>Crossref</small> | 12 words — < 1% |
| <hr/> | | |
| 31 | P. M. Cohn. "Basic Algebra", Springer Science and Business Media LLC, 2003
<small>Crossref</small> | 12 words — < 1% |
| <hr/> | | |
| 32 | alioth.uwb.edu.pl
<small>Internet</small> | 12 words — < 1% |
| <hr/> | | |
| 33 | Progress in Mathematics, 1993.
<small>Crossref</small> | 11 words — < 1% |
| <hr/> | | |
| 34 | vdoc.pub
<small>Internet</small> | 11 words — < 1% |
| <hr/> | | |
| 35 | Alexander Prestel, Charles N. Delzell. "Positive Polynomials", Springer Science and Business Media LLC, 2001
<small>Crossref</small> | 10 words — < 1% |
| <hr/> | | |
| 36 | Juliusz Brzeziński. "Galois Theory Through Exercises", Springer Science and Business Media LLC, 2018
<small>Crossref</small> | 10 words — < 1% |
| <hr/> | | |
| 37 | units.imamu.edu.sa
<small>Internet</small> | 10 words — < 1% |
| <hr/> | | |
| 38 | "Intelligent Computer Mathematics", Springer Science and Business Media LLC, 2020
<small>Crossref</small> | 9 words — < 1% |
| <hr/> | | |
| 39 | Christoph Schwarzweller. "Formally Real Fields", Formalized Mathematics, 2017
<small>Crossref</small> | 9 words — < 1% |

40	Graduate Texts in Mathematics, 2002. Crossref	9 words — < 1%
41	Lecture Notes in Computer Science, 2011. Crossref	8 words — < 1%
42	ir.lib.uwo.ca Internet	8 words — < 1%
43	Christoph Schwarzweller. "Splitting Fields", Formalized Mathematics, 2021 Crossref	7 words — < 1%
44	"Algebraic Examples", Graduate Texts in Mathematics, 2002 Crossref	6 words — < 1%
45	Christoph Schwarzweller. "Existence and Uniqueness of Algebraic Closures", Formalized Mathematics, 2022 Crossref	6 words — < 1%

EXCLUDE QUOTES OFF

EXCLUDE BIBLIOGRAPHY OFF

EXCLUDE SOURCES OFF

EXCLUDE MATCHES OFF