Proceedings of the Federated Conference on Computer Science and Information Systems pp. 67–72
DOI: 10.15439/2018F88
ISSN 2300-5963 ACSIS, Vol. 15

Representation Matters: An Unexpected Property of Polynomial Rings and its Consequences for Formalizing Abstract Field Theory

This paper is dedicated to Grzegorz Bancerek.

Christoph Schwarzweller
Intstitute of Informatics, Faculty of Mathematics, Physics and Informatics,
University of Gdańsk,
Wita Stwosza 57, 80-952 Gdańsk, Poland
Email: schwarzw@inf.ug.edu.pl

***Abstract*—In this paper we develop a Mizar formalization of Kronecker's construction, which states that for every field F and irreducible polynomial $p \in F[X]$ there exists a field extension E of F such that p has a root over E. It turns out that to prove the correctness of the construction the field F needs to provide a disjointness condition, namely $F \cap F[X] = \emptyset$. Surprisingly this property does not hold for arbitrary representations of a field F: We construct for almost every field F another representation F', i.e. an isomorphic copy F' of F, not satisfying this condition. As a consequence to F' our formalization of Kronecker's construction cannot be applied.**
All proofs have been carried out in the Mizar system. Based on Mizar's representation of the fields $\mathbb{Z}_p, \mathbb{Q}$ and $\mathbb{R}$ we also have proven that $\mathbb{Z}_p \cap \mathbb{Z}_p[X] = \emptyset$, $\mathbb{Q} \cap \mathbb{Q}[X] = \emptyset$, and $\mathbb{R} \cap \mathbb{R}[X] = \emptyset$ respectively.

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 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 [4], 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 (see also [25]).

Another interesting challenge in this context is Artin's solution of Hilbert's 17th problem, which asks whether a (multivariate) polynomial taking only non-negative values over the real numbers can be represented as a sum of squares of rational functions. Its formalization requires the development of real algebra: the theory of ordered fields and in particular the notion of field extensions and field adjunctions [23]. A key tool in field theory is Kronecker's construction which states that for every field F and every non-constant polynomial $p \in F[X]$ there exists a field extension E of F in which p has a root. The Mizar formalization of Kronecker's construction is the topic of this paper.

One dominating subject in abstract field theory is the construction of new larger fields containing the field (or ring) one has started with, for example constructing $\mathbb{C}$ from $\mathbb{R}$ or $F(X)$ from $F[X]$. Here only the general structure of the field, not the individual representation of the field's elements, is of interest; isomorphic fields are just considered to be the same field. For example, when constructing the complex numbers by $\mathbb{R}[X]/(X^2+1)$ the result is not the usual field $\mathbb{C}$ of complex numbers, yet we have $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$. Also $\mathbb{R}[X]/(X^2+1)$ does not contain $\mathbb{R}$ as a subfield, but an isomorphic copy of it. From a mathematician's point of view this of course does not matter, because you can get what you want by exchanging the isomorphic fields. This kind of argument is omnipresent in abstract field theory. In fact, Kronecker's construction contains a similar argument and we will see that exactly this is the hardest part in the formalization: to carry it out, we need the disjointness condition $F \cap F[X] = \emptyset$ already mentioned in the abstract.

The plan of the paper is as follows. In the next section we give a brief overview of the Mizar system and illustrate how algebraic domains are constructed. In section III we discuss our Mizar formalization of Kronecker's construction placing emphasis on the disjointness condition. In the subsequent section we present the construction of fields which do not fulfill our disjointness condition. It turns out that our construction works for every field except $\mathbb{Z}_2$. In section V and VI we provide an intuitive, though not really helpful, condition implying $F \cap F[X] = \emptyset$ and finally prove the disjointness condition for Mizar's representation of the fields $\mathbb{Z}_p, \mathbb{Q}$, and $\mathbb{R}$. In the conclusion we discuss how a formalization of Kronecker's construction without a disjointness condition might look like.

II. The Mizar System

Mizar has often been described in the literature, for example in [3], [18], [12], [9], [8] and [11]. 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 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 [10].

To define algebraic domains Mizar provides so-called structure modes fixing the domain's sets of elements and operations. So, for example[1]

```
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 a `doubleLoopStr` with the appropriate collection of attributes (compare [21], [19]).

```
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.

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 `multrat` defining addition and multiplication for elements of `RAT`. These are then glued together by the following

[1]Throughout the paper Mizar code is written in verbatim style.

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

Note, that the definition of the set `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`. 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 $\mathbb{Q}$.

III. Kronecker's Construction

In this section we discuss our Mizar formalization of Kronecker's construction, sometimes also called the main theorem of field theory. It can be stated as follows [24], [23]:

Theorem
Let F be a field and $p \in F[X]$ irreducible. Then there exists a field extension E of F such that p has a root over E.

Note that from this theorem easily follows the existence of such an extension for every non-constant $p \in F[X]$.

A. Field Extensions

We begin with the Mizar definition of field extensions: A field E is a field extension of a field F, if F is a subfield of E [24], or equivalently if F is a subset of E, which itself is a field. It is understood that the operations $+$ and $*$ in F are the restrictions of $+$ and $*$ in E. In Mizar this is stated as follows (see [6]).

```
definition
let F be Field;
mode Subfield of F -> Field means
  the carrier of it c= the carrier of F &
  the addF of it = (the addF of F)
                        || the carrier of it &
  the multF of it = (the multF of F)
                        || the carrier of it &
  1.it = 1.F & 0.it = 0.F;
end;
```

The mode `Subring of R`, where `R` is a ring is defined analogously. Based on this definition we can introduce field extensions as follows.

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

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

Note that instead of postulating that F is a subfield of E we demand that a ring R is a subring of E. This way our definition gets more flexible. For example, this allows to show that $\mathbb{Q}$ extends $\mathbb{Z}$. For a field F, however, our definition is equivalent

to the one from the literature given above, in particular one proves that

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

In any case the definition implies that a field E in order to be a field extension of a field F in particular must contain the elements of F, e.g. we must have `the carrier of` $F \subseteq$ `the carrier of` E as sets.

B. The Construction

Kronecker's proof is constructive [24] and consists of two parts: The first one observes is that if p is irreducible then $<p>$ is a maximal ideal in $F[X]$, and hence $E := F[X]/<p>$ is a field. The second step consists of showing that $[X]_{<p>}$ is a root of p in $E[X]$: If $p = a_0 + a_1 * X + \ldots a_n * X^n$ we get

$$\begin{aligned} p([X]) &= a_0 + a_1 * [X] + \ldots a_n * [X]^n \\ &= a_0 + a_1 * [X] + \ldots a_n * [X^n] \\ &= a_0 + [a_1 * X] + \ldots [a_n * X^n] \\ &= [a_0 + a_1 * X + \ldots a_n * X^n] \\ &= [p] \\ &= 0. \end{aligned}$$

Between these two steps one usually finds a remark that $F[X]/<p>$ is a field extension of F. Note that formally F is no subfield of $F[X]/<p>$ just because $F \not\subseteq F[X]/<p>$ as sets; and therefore $p \in F[X]$ is not even a polynomial over $F[X]/<p>$. However, $\varphi : F \longrightarrow F[X]/<p>$ given by $a \mapsto [a()]_{<p>}$ is a monomorphism, the so-called canonical monomorphism, and gives rise to the embedding of F into $F[X]/<p>$. The remark mentioned above then reads

> *We can identify φF with F in $F[X]/<p>$ and thus consider F as a subfield of $F[X]/<p>$.*

The Mizar formalization of the two steps is quite straightforward. The quotient field $F[X]/<p>$ has been defined in [16], [20] and $p([X]) = [p]$ can be easily shown by induction on the degree of p.

The main task is to formalize the aforementioned remark: Formally, identifying φF with F in a field E if $\varphi : F \longrightarrow E$ is a monomorphism means defining a new carrier $K := (E \setminus \varphi F) \cup F$ and modifying addition and multiplication of F appropriately. For example, $a + b$ for two elements a and b of K where $a \in F$ and $b \in E \setminus \varphi F$ actually means adding $\varphi a + b$ in E. The result $a + b$ then either is $\varphi a + b$ if this is not in φF or $\varphi^{-1}(\varphi a + b)$ if this is in φF. In this way we get a new field K isomorphic to E with $F \subseteq E$:

Theorem
Let F, E be fields and $\varphi : F \longrightarrow E$ a monomorphism. Then $K := (E \setminus \varphi F) \cup F$ is a field isomorphic to E. Moreover F is a subfield of K.

This field K then is the desired field extension for Kronecker's construction. Unfortunately we were not able to prove the theorem in this general setting: the problem is that there might be elements in E, more precisely in $E \setminus \varphi F$, already appearing in F, that is $F \cap (E \setminus \varphi F)$ might be non-empty. This leads to an identification of elements during the construction, which destroys the isomorphism between $(E \setminus \varphi F) \cup F$ and E. This has to be excluded, so we require a disjointness condition. We hence come up with two slightly weaker theorems in Mizar. Here E being a F-monomorphic field just means that there exists a monomorphism $\varphi : F \longrightarrow E$ and `emb f` is the field K defined above.

```
theorem
for F being Field,
    E being F-monomorphic Field
st F /\ E = {}
for f being Monomorphism of F,E
holds E,(emb f) are_isomorphic;

theorem
for F being Field,
    E being F-monomorphic Field
st F /\ E = {}
ex E' being Field st E',E are_isomorphic &
                     F is Subfield of E';
```

The Mizar proofs are straightforward, but quite tedious due to the number of different cases. Now our Mizar version of Kronecker's construction has to take into account the disjointness condition leading to the following theorem.

```
theorem
for F being Field,
    p being non constant
                  Element of Polynom-Ring F
st F /\ (Polynom-Ring F)/({p}-Ideal) = {}
ex E being FieldExtension of F
st p is_with_roots_in E;
```

The theorem's condition

```
F /\ (Polynom-Ring F)/({p}-Ideal) = {},
```

i.e. $F \cap F[X]/<p> = \emptyset$, is not really satisfying: it depends not only on the field F, but also on the given polynomial $p \in F[x]$. This can be improved by carrying out Kronecker's construction using another representation of $F[X]/<p>$: the isomorphic copy consisting of all polynomials $f \in F[X]$ with deg $f <$ deg p (see [24]). We denote this representation by $F[p]$. For $F[p]$ we have in particular $F[p] \subseteq F[X]$ as sets, so that the condition $F \cap F[X] = \emptyset$ suffices to apply the embedding theorems from above. With `polynomial_disjoint` denoting $F \cap F[X] = \emptyset$ we now get the following Mizar version of Kronecker's construction:

```
theorem
for F being polynomial_disjoint Field,
    p being non constant
                  Element of Polynom-Ring F
ex E being FieldExtension of F
st p is_with_roots_in E;
```

IV. Constructing Negative Examples

In the last section we discussed a Mizar formalization of Kronecker's construction and ended up with a version that does not hold for all fields in the first place: To apply Kronecker's construction to a given field F we have to ensure that $F \cap F[X] = \emptyset$.

At first glance this condition should be no restriction. Intuitively a polynomial $p \in F[X]$ is a more complex object than an element a of the underlying field F. In Mizar a polynomial $p \in F[X]$ is defined as a function $p : \mathbb{N} \longrightarrow F$, which returns the coefficients of p: for $n \in \mathbb{N}$ $p.n$ denotes the coefficient of X^n. Therefore it should be easy to show that $a \neq p$ and hence $F \cap F[X] = \emptyset$ for an arbitrary field F.

This, unfortunately, is not true in general. Of course it is easy to show $a \neq p$ if p includes a as a coefficient, that is $p.n = a$ for some $n \in \mathbb{N}$. This, however, does not exclude the existence of fields F with $F \cap F[X] \neq \emptyset$, and in the following we will construct for every field F, except for $\mathbb{Z}_2$, an isomorphic copy F' of F with $F' \cap F'[X] \neq \emptyset$.

A. A First Example

Perhaps the easiest example is a three-element field isomorphic to $\mathbb{Z}_3$. One takes 0 and 1 and sets

$$F' := \{0,\ 1,\ X\}$$

where X is the identity polynomial. The idea is that the polynomial X as a function $\mathbb{N} \longrightarrow F'$ is

$$X.i = \begin{cases} 1; & i = 1 \\ 0; & i \neq 1 \end{cases}$$

Therefore, having $0 \in F'$ and $1 \in F'$ we can built this function (over F') and hence $X \in F' \cap F'[X]$. The operations $+$ and $*$ of F' are just defined to mimic the ones of $\mathbb{Z}_3$ with X playing the role of 2. As a result we have an isomorphic copy of $\mathbb{Z}_3$ our Mizar version of Kronecker's construction cannot be applied to.

B. A Class of Negative Examples

The idea of the first example can be generalized to almost arbitrary fields F by observing that we in fact changed the representation of $\mathbb{Z}_3$ by just exchanging 2 with the polynomial X. This works for almost every field F; $\mathbb{Z}_2$ is the only exception. One can exchange an arbitrary element $a \in F \backslash \{0, 1\}$ with another arbitrary object o by setting

$$F_{a,o} := (F \backslash \{a\}) \cup \{o\}.$$

Defining $+$ and $*$ appropriately $F_{a,o}$ then is an isomorphic copy of F for an arbitary object o. Substituting X for o now shows that $X \in F_{a,X} \cap F_{a,X}[X]$ and gives the Mizar

```
theorem
for F being non almost_trivial Field
ex F' being non polynomial_disjoint Field
st F',F are_isomorphic;
```

Here, the property `non almost trivial` excludes $\mathbb{Z}_2$. In other words, for every field F (except for $\mathbb{Z}_2$) we constructed a representation of F our Mizar version of Kronecker's construction cannot be applied to.

Note also that X is non-constant and hence $X \notin \varphi F$, so that identifying φF with F will not adjust the intersection. In fact - as o is arbitrary - one can substitute o with the polynomial X^n for $n \in \mathbb{N}^+$. X^n as a function is

$$(X^n).i = \begin{cases} 1; & i = n \\ 0; & i \neq n \end{cases}$$

so an analogous argument shows $X^n \in F_{a,X^n} \cap F_{a,X^n}[X]$. Hence, we get the following

```
theorem
for F being non almost_trivial Field
for n being non zero Nat
ex F' being non polynomial_disjoint Field,
   p being Polynomial of F'
st F',F are_isomorphic &
   deg p = n &
   p in (the carrier of F') /\
              (the carrier of Polynom-Ring F');
```

so that the degree of the polynomial p in the intersection $F' \cap F'[X]$ is not bounded.

As the main result from our counterexamples we get that $F' \cap F[X] = \emptyset$ is a property not invariant under isomorphisms (of fields). Consequently the application of Kronecker's theorem depends on the representation of the given field F.

V. An Intuitive "Solution"

In the last section it turned out that in order to apply Kronecker's construction with a given field F we have to ensure that $F \cap F[X] = \emptyset$, depending on the actual representation of F. This is in particular true for the basic fields $\mathbb{Q}, \mathbb{R}$, and $\mathbb{Z}_p$, where p is prime: it becomes important how these fields are represented in Mizar.

A first approach to solve this problem again relies on the intuitive feeling that a polynomial is a more complex object than an element of the underlying field. So, if all elements of a field F are of the same complexity, then $F \cap F[X]$ should be empty just because all polynomials $p \in F[X]$ are more complex than - and therefore are not equal to - all elements $a \in F$. Note, that our counterexamples from section IV do not fulfill this condition.

A possibility to measure the complexity of mathematical objects o is the so-called rank of o (see [5]). Here every object o is understood as a set and the rank of o is the least ordinal number greater than the rank of every member of the set o. In Mizar the notion of rank has been formalized as a function `the_rank_of` from objects into ordinal numbers [1]. Using this function we define

```
definition
let F be Field;
attr F is flat means
  for a,b being Element of F
  holds the_rank_of a = the_rank_of b;
end;
```

to express that all elements of a field F are of the same complexity. As already mentioned a Mizar polynomial over F is defined as a function $p : \mathbb{N} \longrightarrow F$, i.e. formally is a set of pairs $p = \{ [n, p.n] \mid n \in \mathbb{N}\}$.[2] From this immediately follows that if F is flat, then the rank of all polynomials $p \in F[X]$ is greater than the rank of all elements $a \in F$ and thus

```
theorem
for F being flat Field
              holds F is polynomial_disjoint;
```

Note that in particular the definition of functions in terms of set of pairs enabled the proof of this theorem.

Unfortunately the criterion of being flat is not really helpful, as it does not apply to standard representations of fields. The reason is that in Mizar 0 is defined as the empty set - and the empty set is the only mathematical object of rank 0. Consequently every field containing 0 is non-flat, so that in particular $\mathbb{Q}, \mathbb{R}$, and $\mathbb{Z}_p$ are non-flat.

VI. Some Positive Examples

To provide some examples our Mizar version of Kronecker's construction can be applied to, we prove $\mathbb{Z}_p \cap \mathbb{Z}_p[X] = \emptyset$, $\mathbb{Q} \cap \mathbb{Q}[X] = \emptyset$, and $\mathbb{R} \cap \mathbb{R}[X] = \emptyset$ by hand. To do so we have to rely on Mizar's representation of these fields: essentially we have to check the definitions. Note again, that for a field F the condition $F \cap F[X] = \emptyset$ suffices to apply our Mizar version of Kronecker's construction, because our formalization uses $F[p]$ instead of $F[X]/<p>$.

We already mentioned that a Mizar polynomial over F is a function $p : \mathbb{N} \longrightarrow F$, that is $p = \{[n, p.n] \mid n \in \mathbb{N}\}$ as a set. We now need to show that no Mizar polynomial p can equal any Mizar number $r \in \mathbb{R} \supseteq \mathbb{Q} \supseteq \mathbb{Z} \supseteq \mathbb{N}$. To be more precise, this has to be shown for the Mizar sets `REAL`, `RAT`, `INT`, and `NAT`, which have been used to define the fields `INT.Ring p`, `F_Rat`, and `F_Real`. To keep the following more readable we will, however, continue writing $\mathbb{N}$ for `NAT`, $\mathbb{Z}$ for `INT`, and so on.

In Mizar all numbers beginning with $\mathbb{N}$ are constructed from sets following the well-known set-theoretic approaches. So for $\mathbb{N}$ we find $0 = \emptyset,\ 1 = \{0\},\ 2 = \{0, 1\}, \ldots$ and in general $n = \{m \mid m < n\}$ for $n, m \in \mathbb{N}$.

Because the carrier of $\mathbb{Z}_n$ equals $\{0, 1, \ldots n-1\} \subset \mathbb{N}$ we already can show $\mathbb{Z}_n \cap \mathbb{Z}_n[X] = \emptyset$. For if we have $p = n$ for a polynomial p and a natural number n it follows that $\{[i, p.i] \mid i \in \mathbb{N}\} = \{m \mid m < n\}$, hence there is a $j \in \mathbb{N}$ smaller than n such that $j = [n, p.n] = \{\{n\}, \{n, p.n\}\}$. Then, because j is a natural number, j must equal $\{0, 1\} = \{\emptyset, 1\}$,[3] but neither $\{n\}$ nor $\{n, p.n\}$ equals $\emptyset$, a contradiction.

The proofs of polynomial disjointness for $\mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$ use similar set-based argumentations. To give an impression how Mizar's set-based definition of numbers is used, we briefly discuss the case of $\mathbb{Q}$. In Mizar first the non-negative rational numbers $\mathbb{Q}^+$ are introduced as pairs of natural numbers, i.e. elements of the set `NAT` (see [2]):

```
reserve i,j,k for Element of NAT;

definition
func RAT+ -> set equals
  ({[i,j]: i,j are_coprime & j <> {}}
                        \ the set of all [k,1])
  \/ NAT;
end;
```

Note that the embedding $\mathbb{N} \subseteq \mathbb{Q}^+$ is performed by hand substituting all pairs `[k,1]` for `k` $\in \mathbb{N}$. Then in a second step the rational numbers $\mathbb{Q}$ are defined as

```
definition
func RAT -> set equals
  RAT+ \/ [:{0},RAT+:] \ {[0,0]};
end;
```

that is a negative rational number r is represented as a pair $[0, r']$, where r' is a non-negative rational number.

Now assuming that there is a polynomial p and a positive rational number r with $p = r$ we get $[i, j] = \{[n, p.n] \mid n \in \mathbb{N}\}$ for some $i, j \in \mathbb{N}$, $[i, j] \in \mathbb{Q}^+$ and hence that $[i, p.i] \in [i, j] = \{\{i\}, \{i, j\}\}$. Then both cases - $[i, p.i] = \{i\}$ and $[i, p.i] = \{i, j\}$ - lead to a contradiction. Here we just mention that in one (sub) case we even use that i and j are coprime.

With $\mathbb{Q}^+ \cap \mathbb{Q}^+[X] = \emptyset$ it is then straightforward to also show $\mathbb{Q} \cap \mathbb{Q}[X] = \emptyset$: For if $p = r$ for a polynomial p and a rational number r, then r must be negative, that is $r = [0, r']$ with $r' \in \mathbb{Q}^+$. But then because $[1, p.1] \in p = r = [0, r'] = \{\{0\}, \{0, r'\}\}$ we either get $[1, p.1] = \{0\} = 1$ or $[1, p.1] = \{0, r'\} = \{\emptyset, r'\}$ - in both cases a contradiction.

Summarizing, to show that our Mizar formalization of Kronecker's construction applies to $\mathbb{Z}_p, \mathbb{Q}$, and $\mathbb{R}$ we have to provide quite involved proofs using the set-based definition of numbers in Mizar.

VII. Conclusion

We have presented a Mizar formalization of Kronecker's construction. The main drawback is the necessary disjointness condition $F \cap F[X] = \emptyset$. This condition forbids the application of the construction with an arbitrary representation of the given field F.

Though the proofs have been carried out in Mizar, we claim that similar constructions should be possible in other proof assistants such as HOL [14] or Isabelle [15] as well: From a technical point of view all that was necessary to construct our counterexamples was the possibility to aggregate arbitrary objects in a set. In this way we defined the carrier of the fields by uniting elements of F with elements of $F[X]$. This should be possible in most proof assistants - if not some rank or typing argument forbids aggregating elements of different complexities.

Mathematicians solve our disjointness problem in a somewhat intuitive way:

[2] We already mention here, that Mizar uses Kuratowski's definition of pairs, that is $[x, y] := \{\{x\}, \{x, y\}\}$. This will be used in section VI.

[3] In fact, $j = \{0\}$ is possible if $n = p.n$; but in this case we get $j = \{\{n\}\}$, and hence $\{n\} = 0 = \emptyset$.

Of course $F \cap F[X]$, and also $F \cap F[X]/<p>$, can be considered non-empty, for if not just rename elements appropriately.

is their comment, and in fact for every field F there exists another representation $F' \cong F$ such that $F' \cap F'[X] = \emptyset$. It would be desirable to eliminate the disjointness condition in such a way. The comment can be stated as a theorem with F' denoting the renamed version of F:

```
theorem
for F being Field ex F' being Field
st F',F are_isomorphic &
   F' /\ (Polynom-Ring F') = {};
```

or more general for arbitrary fields

```
theorem
for F,E being Field ex F' being Field
st F',F are_isomorphic & F' /\ E = {};
```

These theorems would allow for formalizing Kronecker's construction without any condition. To prove them, it would be necessary to exchange a possibly infinite number of elements with new ones. The emphasize here is on "new", because one has to ensure that the adjoined elements are in fact new, that is appear neither in F nor in $F[X]$ (nor in E). Note also that the construction of our counterexamples uses precisely the technique of exchanging elements. So the key of the proof is the assumption that there is always an infinite stock of new objects which can be stated as a

```
theorem
for Y being set
ex Z being infinite set st Y /\ Z = {};
```

With such a theorem one could construct the required isomorphic copy F' by taking the elements of $F \cup F[X]$ (or $F \cup E$) as Y and then exchanging the elements of F that are in $F \cap F[X]$ (or in $F \cap E$) with elements from Z. Note, however, that one has to keep track of exactly which element of F is replaced with which element of Z. This is necessary to define the operations in F' appropriately.

We believe that the above theorem follows from Zermelo's axioms of set theory, namely the axiom of power set. Carrying out these proofs would call for a non-trivial amount of additional work. Nevertheless it might be helpful when further developing abstract field theory - and in fact would give a formalization of Kronecker's construction as found in the literature. Again the proofs would make use of basics of set theory showing that field theory heavily relies on the (informally used) foundations of mathematics. Therefore the further development of abstract field theory will remain a challenge.

REFERENCES

[1] G. Bancerek, *Tarski's Classes and Ranks*. Formalized Mathematics 1(3), 563–567, 1990.

[2] G. Bancerek, *Arithmetic of Non Negative Rational Numbers*. Mizar Mathematical Library, 1998.

[3] 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 9150, 261–279, 2015. http://dx.doi.org/10.1007/978-3-319-20615-8_17

[4] *The Coq Proof Assistant*. available at www.coq.inria.fr.

[5] H.B. Enderton, *Elements of Set Theory*. Elsevier, 1977.

[6] Y. Futa, H. Okazaki, and Y. Shidama, *Set of Points on Elliptic Curve in Projective Coordinates*. Formalized Mathematics 19(3), 131–138, 2011. http://dx.doi.org/10.2478/v10037-011-0021-6

[7] A. Grabowski, A. Korniłowicz, 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

[8] A. Grabowski, A. Korniłowicz, and C. Schwarzweller, *Equality in Computer Proof-Assistants*. in: Proceedings of the 2015 Federated Conference on Computer Science and Information Systems, M. Ganzha, L. Maciaszek, M. Paprzycki (eds.), ACSIS, Vol. 5, 45–54, 2015. http://dx.doi.org/10.15439/2015F229

[9] A. Grabowski, A. Korniłowicz, and C. Schwarzweller, *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, 363–371, 2016. http://dx.doi.org/10.15439/2016F520

[10] A. Grabowski and C. Schwarzweller, *Translating Mathematical Vernacular into Knowledge Repositories*. in: M. Kohlhase (ed.), Proceedings of the 4th International Conference on Mathematical Knowledge Management, Lecture Notes in Artificial Intelligence, 3863, 49–64, Springer Verlag, 2006.

[11] A. Grabowski and C. Schwarzweller, *On Duplication in Mathematical Repositories*. in: S. Autexier et.al. (eds.), Intelligent Computer Mathematics, Lecture Notes in Artificial Intelligence, 6167, 300-314, Springer Verlag, 2010.

[12] A. Grabowski, A. Korniłowicz, 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] A. Korniłowicz, *Quotient Rings*. Formalized Mathematics 13(4), 573–576, 2005.

[17] *Mizar Home Page*. available at www.mizar.org.

[18] A. Naumowicz and A. Korniłowicz, *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, 67–72, *Springer Verlag*, 2009.

[19] P. Rudnicki, A. Trybulec, and C. Schwarzweller, *Commutative Algebra in the Mizar System*. Journal of Symbolic Computation, vol. 32(1/2), pp. 143–169, 2001. http://dx.doi.org/10.1006/jsco.2001.0456

[20] C. Schwarzweller, A. Korniłowicz, and A. Rowińska-Schwarzweller, *Some Algebraic Properties of Polynomial Rings*. Formalized Mathematics 24(3), 227–237, 2016. http://doi.org/10.1515/forma-2016-0019

[21] W.A. Trybulec, *Vectors in Real Linear Space*. Formalized Mathematics 1(2), 291–296, 1990.

[22] A. Trybulec, A. Korniłowicz, A. Naumowicz, and K. Kuperberg, *Formal Mathematics for Mathematicians*. Journal of Automated Reasoning 50(2), 119–121, 2013. http://dx.doi.org/10.1007/s10817-012-9268-z

[23] B.L. van der Waerden, *Algebra Vol. I*. 8th edition Springer Verlag 1990.

[24] S. Weintraub, *Galois Theory*. 2nd edition Springer Verlag, 2008.

[25] F. Wiedijk, *Formalizing 100 Theorems*. available at www.cs.ru.nl/~freek.