FORMALIZED MATHEMATICS
Vol. 27, No. 2, Pages 133–137, 2019
DOI: 10.2478/forma-2019-0014

sciendo
https://www.sciendo.com/

# On Monomorphisms and Subfields

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

**Summary.** This is the second part of a four-article series containing a Mizar [2], [1] formalization of Kronecker's construction about roots of polynomials in field extensions, i.e. that for every field $F$ and every polynomial $p \in F[X] \backslash F$ there exists a field extension $E$ of $F$ such that $p$ has a root over $E$. The formalization follows Kronecker's classical proof using $F[X]/{<}p{>}$ as the desired field extension $E$ [5], [3], [4].

In the first part we show that an irreducible polynomial $p \in F[X] \backslash F$ has a root over $F[X]/{<}p{>}$. Note, however, that this statement cannot be true in a rigid formal sense: We do not have $F \subseteq F[X]/<p>$ as sets, so $F$ is not a subfield of $F[X]/{<}p{>}$, and hence formally $p$ is not even a polynomial over $F[X]/{<}p{>}$. Consequently, we translate $p$ along the canonical monomorphism $\phi : F \longrightarrow F[X]/{<}p{>}$ and show that the translated polynomial $\phi(p)$ has a root over $F[X]/{<}p{>}$.

Because $F$ is not a subfield of $F[X]/{<}p{>}$ we construct in this second part the field $(E \setminus \phi F) \cup F$ for a given monomorphism $\phi : F \longrightarrow E$ and show that this field both is isomorphic to $F$ and includes $F$ as a subfield. In the literature this part of the proof usually consists of saying that "one can identify $F$ with its image $\phi F$ in $F[X]/{<}p{>}$ and therefore consider $F$ as a subfield of $F[X]/{<}p{>}$". Interestingly, to do so we need to assume that $F \cap E = \emptyset$, in particular Kronecker's construction can be formalized for fields $F$ with $F \cap F[X] = \emptyset$.

Surprisingly, as we show in the third part, this condition is not automatically true for arbitray fields $F$: With the exception of $\mathbb{Z}_2$ we construct for every field $F$ an isomorphic copy $F'$ of $F$ with $F' \cap F'[X] \neq \emptyset$. We also prove that for Mizar's representations of $\mathbb{Z}_n$, $\mathbb{Q}$ and $\mathbb{R}$ we have $\mathbb{Z}_n \cap \mathbb{Z}_n[X] = \emptyset$, $\mathbb{Q} \cap \mathbb{Q}[X] = \emptyset$ and $\mathbb{R} \cap \mathbb{R}[X] = \emptyset$, respectively.

In the fourth part we finally define field extensions: $E$ is a field extension of $F$ iff $F$ is a subfield of $E$. Note, that in this case we have $F \subseteq E$ as sets, and thus a polynomial $p$ over $F$ is also a polynomial over $E$. We then apply the construction of the second part to $F[X]/{<}p{>}$ with the canonical monomorphism




ISSN 1426–2630(Print), 1898-9934(Online)

$\phi : F \longrightarrow F[X]/\langle p\rangle$. Together with the first part this gives - for fields $F$ with $F \cap F[X] = \emptyset$ - a field extension $E$ of $F$ in which $p \in F[X] \setminus F$ has a root.

MSC: 12E05 12F05 68T99 03B35

Keywords: roots of polynomials; field extensions; Kronecker's construction

MML identifier: FIELD_2, version: 8.1.09 5.57.1355

From now on $R$ denotes a ring, $S$ denotes an $R$-monomorphic ring, $K$ denotes a field, $F$ denotes a $K$-monomorphic field, and $T$ denotes a $K$-monomorphic commutative ring.

Let us consider $R$ and $S$. Let $f$ be a monomorphism of $R$ and $S$. Let us observe that the functor $f^{-1}$ yields a function from $\operatorname{rng} f$ into $R$. Now we state the propositions:

(1) Let us consider a monomorphism $f$ of $R$ and $S$, and elements $a$, $b$ of $\operatorname{rng} f$. Then

  (i) $(f^{-1})(a + b) = (f^{-1})(a) + (f^{-1})(b)$, and

  (ii) $(f^{-1})(a \cdot b) = (f^{-1})(a) \cdot (f^{-1})(b)$.

(2) Let us consider a monomorphism $f$ of $R$ and $S$, and an element $a$ of $\operatorname{rng} f$. Then $(f^{-1})(a) = 0_R$ if and only if $a = 0_S$.

Let us consider a monomorphism $f$ of $R$ and $S$. Now we state the propositions:

(3) (i) $(f^{-1})(1_S) = 1_R$, and

  (ii) $(f^{-1})(0_S) = 0_R$.

  The theorem is a consequence of (1).

(4) $f^{-1}$ is one-to-one and onto.

(5) Let us consider a monomorphism $f$ of $R$ and $S$, and an element $a$ of $R$. Then $f(a) = 0_S$ if and only if $a = 0_R$.

(6) Let us consider a monomorphism $f$ of $K$ and $F$, and an element $a$ of $K$. If $a \neq 0_K$, then $f(a^{-1}) = f(a)^{-1}$. The theorem is a consequence of (5).

Let $R$, $S$ be rings. We introduce the notation $R$ and $S$ are disjoint as a synonym of $R$ misses $S$.

One can check that $R$ and $S$ are disjoint if and only if the condition (Def. 1) is satisfied.

(Def. 1) $\Omega_R \cap \Omega_S = \emptyset$.

Let us consider $R$ and $S$. Let $f$ be a monomorphism of $R$ and $S$. The functor $\overline{f}$ yielding a non empty set is defined by the term

(Def. 2) $(\Omega_S \setminus \operatorname{rng} f) \cup \Omega_R$.

Let $R$ be a ring, $S$ be an $R$-monomorphic ring, and $a$, $b$ be elements of $\overline{f}$. The functor addemb$(f, a, b)$ yielding an element of $\overline{f}$ is defined by the term

(Def. 3) $$\begin{cases} (\text{the addition of } R)(a, b), & \textbf{if } a, b \in \Omega_R, \\ (\text{the addition of } S)(f(a), b), & \textbf{if } a \in \Omega_R \text{ and } b \notin \Omega_R, \\ (\text{the addition of } S)(a, f(b)), & \textbf{if } b \in \Omega_R \text{ and } a \notin \Omega_R, \\ (f^{-1})((\text{the addition of } S)(a, b)), & \textbf{if } a \notin \Omega_R \text{ and } b \notin \Omega_R \text{ and} \\ & \quad (\text{the addition of } S)(a, b) \in \operatorname{rng} f, \\ (\text{the addition of } S)(a, b), & \textbf{otherwise}. \end{cases}$$

The functor addemb$(f)$ yielding a binary operation on $\overline{f}$ is defined by

(Def. 4) for every elements $a$, $b$ of $\overline{f}$, $it(a, b) = \text{addemb}(f, a, b)$.

Let $K$ be a field, $T$ be a $K$-monomorphic commutative ring, $f$ be a monomorphism of $K$ and $T$, and $a$, $b$ be elements of $\overline{f}$. The functor multemb$(f, a, b)$ yielding an element of $\overline{f}$ is defined by the term

(Def. 5) $$\begin{cases} (\text{the multiplication of } K)(a, b), & \textbf{if } a, b \in \Omega_K, \\ 0_K, & \textbf{if } a = 0_K \text{ or } b = 0_K, \\ (\text{the multiplication of } T)(f(a), b), & \textbf{if } a \in \Omega_K \text{ and } a \neq 0_K \text{ and} \\ & \quad b \notin \Omega_K, \\ (\text{the multiplication of } T)(a, f(b)), & \textbf{if } b \in \Omega_K \text{ and } b \neq 0_K \text{ and} \\ & \quad a \notin \Omega_K, \\ (f^{-1})((\text{the multiplication of } T)(a, b)), & \textbf{if } a \notin \Omega_K \text{ and } b \notin \Omega_K \text{ and} \\ & \quad (\text{the multiplication of } T) \\ & \quad (a, b) \in \operatorname{rng} f, \\ (\text{the multiplication of } T)(a, b), & \textbf{otherwise}. \end{cases}$$

The functor multemb$(f)$ yielding a binary operation on $\overline{f}$ is defined by

(Def. 6) for every elements $a$, $b$ of $\overline{f}$, $it(a, b) = \text{multemb}(f, a, b)$.

The functor embField$(f)$ yielding a strict double loop structure is defined by

(Def. 7) the carrier of $it = \overline{f}$ and the addition of $it = \text{addemb}(f)$ and the multiplication of $it = \text{multemb}(f)$ and the one of $it = 1_K$ and the zero of $it = 0_K$.

One can verify that embField$(f)$ is non degenerated and embField$(f)$ is Abelian and right zeroed.

Let us consider a monomorphism $f$ of $K$ and $T$. Now we state the propositions:

(7) If $K$ and $T$ are disjoint, then embField$(f)$ is add-associative. The theorem is a consequence of (1).

(8) If $K$ and $T$ are disjoint, then embField$(f)$ is right complementable.

Let $K$ be a field, $T$ be a $K$-monomorphic commutative ring, and $f$ be a monomorphism of $K$ and $T$. Note that embField$(f)$ is commutative and well unital.

(9) Let us consider a monomorphism $f$ of $K$ and $F$. If $K$ and $F$ are disjoint, then embField($f$) is associative. The theorem is a consequence of (1), (2), and (6).

(10) Let us consider a monomorphism $f$ of $K$ and $T$. If $K$ and $T$ are disjoint, then embField($f$) is distributive. The theorem is a consequence of (3), (2), and (1).

Let us consider a monomorphism $f$ of $K$ and $F$. Now we state the propositions:

(11) If $K$ and $F$ are disjoint, then embField($f$) is almost left invertible. The theorem is a consequence of (3).

(12) If $K$ and $F$ are disjoint, then embField($f$) is a field.

Let $K$ be a field, $F$ be a $K$-monomorphic field, and $f$ be a monomorphism of $K$ and $F$. The functor emb-iso($f$) yielding a function from embField($f$) into $F$ is defined by

(Def. 8) for every element $a$ of embField($f$) such that $a \notin K$ holds $it(a) = a$ and for every element $a$ of embField($f$) such that $a \in K$ holds $it(a) = f(a)$.

One can verify that emb-iso($f$) is unity-preserving.

Let us consider a monomorphism $f$ of $K$ and $F$. Now we state the propositions:

(13) If $K$ and $F$ are disjoint, then emb-iso($f$) is additive.

(14) If $K$ and $F$ are disjoint, then emb-iso($f$) is multiplicative.

Let $K$ be a field, $F$ be a $K$-monomorphic field, and $f$ be a monomorphism of $K$ and $F$. Note that emb-iso($f$) is one-to-one.

Let us consider a monomorphism $f$ of $K$ and $F$. Now we state the propositions:

(15) If $K$ and $F$ are disjoint, then emb-iso($f$) is onto.

(16) If $K$ and $F$ are disjoint, then $F$ and embField($f$) are isomorphic. The theorem is a consequence of (13), (14), and (15).

(17) Let us consider a monomorphism $f$ of $K$ and $F$, and a field $E$. If $E =$ embField($f$), then $K$ is a subfield of $E$.

(18) If $K$ and $F$ are disjoint, then there exists a field $E$ such that $E$ and $F$ are isomorphic and $K$ is a subfield of $E$. The theorem is a consequence of (7), (9), (10), (8), (11), (16), and (17).

(19) Let us consider fields $K$, $F$. Suppose $K$ and $F$ are disjoint. Then $F$ is $K$-monomorphic if and only if there exists a field $E$ such that $E$ and $F$ are isomorphic and $K$ is a subfield of $E$. The theorem is a consequence of (18).

## References


[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[2] 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.

[3] Nathan Jacobson. *Basic Algebra I*. Dover Books on Mathematics, 1985.

[4] Heinz Lüneburg. *Gruppen, Ringe, Körper: Die grundlegenden Strukturen der Algebra*. Oldenbourg Verlag, 1999.

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


*Accepted May 27, 2019*