


On the Intersection of Fields F with $F[X]$

Christoph Schwarzweller 
Institute of Informatics
University of Gdańsk
Poland

Summary. This is the third part of a four-article series containing a Mizar [3], [1], [2] formalization of Kronecker’s construction about roots of polynomials in field extensions, i.e. that for every field F and every polynomial $p \in F[X] \setminus F$ there exists a field extension E of F such that p has a root over E . The formalization follows Kronecker’s classical proof using $F[X]/\langle p \rangle$ as the desired field extension E [6], [4], [5].

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

Because F is not a subfield of $F[X]/\langle p \rangle$ we construct in the second part the field $(E \setminus \phi F) \cup F$ for a given monomorphism $\phi : F \rightarrow E$ 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 ϕF in $F[X]/\langle p \rangle$ and therefore consider F as a subfield of $F[X]/\langle p \rangle$ ”. 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 this third part, this condition is not automatically true for arbitrary 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 $F[X]/\langle p \rangle$ with the canonical monomorphism

$\phi : F \longrightarrow F[X]/\langle p \rangle$. 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_3, version: 8.1.09 5.59.1363

1. PRELIMINARIES

Now we state the propositions:

- (1) Let us consider a natural number n , and an object x . If $n = \{x\}$, then $x = 0$.
- (2) Let us consider a natural number n , and objects x, y . If $n = \{x, y\}$ and $x \neq y$, then $x = 0$ and $y = 1$ or $x = 1$ and $y = 0$.
- (3) Let us consider a natural number n . If $1 < n$, then $0_{\mathbb{Z}/n} = 0$.
- (4) $1_{\mathbb{Z}/2} + 1_{\mathbb{Z}/2} = 0_{\mathbb{Z}/2}$. The theorem is a consequence of (3).
- (5) Let us consider a ring R , and a non zero natural number n . Then $\text{power}_R(0_R, n) = 0_R$.

One can verify that $\mathbb{Z}/3$ is non degenerated and almost left invertible and there exists a field which is finite and there exists a field which is infinite.

Let L be a non empty double loop structure. We say that L is almost trivial if and only if

(Def. 1) for every element a of L , $a = 1_L$ or $a = 0_L$.

Observe that every ring which is degenerated is also almost trivial and there exists a field which is non almost trivial.

Now we state the proposition:

- (6) Let us consider a ring R . Then R is almost trivial if and only if R is degenerated or R and $\mathbb{Z}/2$ are isomorphic. The theorem is a consequence of (4).

Let R be a ring and a be an element of R . We say that a is trivial if and only if

(Def. 2) $a = 1_R$ or $a = 0_R$.

Let R be a non almost trivial ring. One can verify that there exists an element of R which is non trivial.

Let R be a ring. We say that R is polynomial-disjoint if and only if

(Def. 3) $\Omega_R \cap \Omega_{\text{PolyRing}(R)} = \emptyset$.

2. SOME NEGATIVE RESULTS

Let R be a non almost trivial ring, x be a non trivial element of R , and o be an object. The functor $\text{carr}(x, o)$ yielding a non empty set is defined by the term

(Def. 4) $\Omega_R \setminus \{x\} \cup \{o\}$.

Let a, b be elements of $\text{carr}(x, o)$. The functor $\text{addR}(a, b)$ yielding an element of $\text{carr}(x, o)$ is defined by the term

(Def. 5) $\left\{ \begin{array}{ll} \text{(the addition of } R)(x, x), & \text{if } a = o \text{ and } b = o \text{ and} \\ & \text{(the addition of } R)(x, x) \neq x, \\ \text{(the addition of } R)(a, x), & \text{if } a \neq o \text{ and } b = o \text{ and} \\ & \text{(the addition of } R)(a, x) \neq x, \\ \text{(the addition of } R)(x, b), & \text{if } a = o \text{ and } b \neq o \text{ and} \\ & \text{(the addition of } R)(x, b) \neq x, \\ \text{(the addition of } R)(a, b), & \text{if } a \neq o \text{ and } b \neq o \text{ and} \\ & \text{(the addition of } R)(a, b) \neq x, \\ o, & \text{otherwise.} \end{array} \right.$

The functor $\text{addR}(x, o)$ yielding a binary operation on $\text{carr}(x, o)$ is defined by

(Def. 6) for every elements a, b of $\text{carr}(x, o)$, $it(a, b) = \text{addR}(a, b)$.

Let a, b be elements of $\text{carr}(x, o)$. The functor $\text{multR}(a, b)$ yielding an element of $\text{carr}(x, o)$ is defined by the term

(Def. 7) $\left\{ \begin{array}{ll} \text{(the multiplication of } R)(x, x), & \text{if } a = o \text{ and } b = o \text{ and} \\ & \text{(the multiplication of } R)(x, x) \neq x, \\ \text{(the multiplication of } R)(a, x), & \text{if } a \neq o \text{ and } b = o \text{ and} \\ & \text{(the multiplication of } R)(a, x) \neq x, \\ \text{(the multiplication of } R)(x, b), & \text{if } a = o \text{ and } b \neq o \text{ and} \\ & \text{(the multiplication of } R)(x, b) \neq x, \\ \text{(the multiplication of } R)(a, b), & \text{if } a \neq o \text{ and } b \neq o \text{ and} \\ & \text{(the multiplication of } R)(a, b) \neq x, \\ o, & \text{otherwise.} \end{array} \right.$

The functor $\text{multR}(x, o)$ yielding a binary operation on $\text{carr}(x, o)$ is defined by

(Def. 8) for every elements a, b of $\text{carr}(x, o)$, $it(a, b) = \text{multR}(a, b)$.

Let F be a non almost trivial field and x be a non trivial element of F . The functor $\text{ExField}(x, o)$ yielding a strict double loop structure is defined by

(Def. 9) the carrier of $it = \text{carr}(x, o)$ and the addition of $it = \text{addR}(x, o)$ and the multiplication of $it = \text{multR}(x, o)$ and the one of $it = 1_F$ and the zero of $it = 0_F$.

One can check that $\text{ExField}(x, o)$ is non degenerated and $\text{ExField}(x, o)$ is Abelian.

From now on o denotes an object, F denotes a non almost trivial field, and x, a denote elements of F .

Let us consider a non trivial element x of F and an object o . Now we state the propositions:

- (7) If $o \notin \Omega_F$, then $\text{ExField}(x, o)$ is right zeroed and right complementable.
- (8) If $o \notin \Omega_F$, then $\text{ExField}(x, o)$ is add-associative.

Let F be a non almost trivial field, x be a non trivial element of F , and o be an object. One can verify that $\text{ExField}(x, o)$ is commutative.

Let us consider a non trivial element x of F and an object o . Now we state the propositions:

- (9) If $o \notin \Omega_F$, then $\text{ExField}(x, o)$ is well unital.
- (10) If $o \notin \Omega_F$, then $\text{ExField}(x, o)$ is associative.
- (11) If $o \notin \Omega_F$, then $\text{ExField}(x, o)$ is distributive.
- (12) If $o \notin \Omega_F$, then $\text{ExField}(x, o)$ is almost left invertible.
- (13) Let us consider a non trivial element x of F , and a ring P . Suppose $P = \text{ExField}(x, \langle 0_F, 1_F \rangle)$. Then $\langle 0_F, 1_F \rangle \in \Omega_P \cap \Omega_{\text{PolyRing}(P)}$.
- (14) There exists a field K such that $\Omega_K \cap \Omega_{\text{PolyRing}(K)} \neq \emptyset$. The theorem is a consequence of (7), (8), (10), (9), (12), (11), and (13).

In the sequel n denotes a non zero natural number.

- (15) There exists a field K and there exists a polynomial p over K such that $\deg p = n$ and $p \in \Omega_K \cap \Omega_{\text{PolyRing}(K)}$. The theorem is a consequence of (7), (8), (10), (9), (12), (11), and (5).
- (16) There exists a field K and there exists an object x such that $x \notin \text{rng}(\text{the canonical homomorphism of } K \text{ into quotient field})$ and $x \in \Omega_K \cap \Omega_{\text{PolyRing}(K)}$. The theorem is a consequence of (7), (8), (10), (9), (12), (11), and (13).

Let us note that there exists a field which is non polynomial-disjoint.

Let F be a non almost trivial field, x be a non trivial element of F , and o be an object. The functor $\text{isoR}(x, o)$ yielding a function from F into $\text{ExField}(x, o)$ is defined by

(Def. 10) $it(x) = o$ and for every element a of F such that $a \neq x$ holds $it(a) = a$.

One can check that $\text{isoR}(x, o)$ is onto.

Now we state the propositions:

- (17) Let us consider a non trivial element x of F , and an object o . If $o \notin \Omega_F$, then $\text{isoR}(x, o)$ is one-to-one.

- (18) Let us consider a non trivial element x of F , and an object u . Suppose $u \notin \Omega_F$. Then $\text{isoR}(x, u)$ is additive, multiplicative, and unity-preserving. The theorem is a consequence of (7), (10), (8), (9), and (11).

Let us consider a non almost trivial field F . Now we state the propositions:

- (19) There exists a non polynomial-disjoint field K such that K and F are isomorphic. The theorem is a consequence of (7), (8), (9), (10), (11), (12), (13), and (18).
- (20) There exists a non polynomial-disjoint field K and there exists a polynomial p over K such that K and F are isomorphic and $\deg p = n$ and $p \in \Omega_K \cap \Omega_{\text{PolyRing}(K)}$. The theorem is a consequence of (7), (8), (10), (9), (12), (11), (5), and (18).

3. AN INTUITIVE "SOLUTION"

Let R be a ring. We say that R is flat if and only if

- (Def. 11) for every elements a, b of R , $\text{rk}(a) = \text{rk}(b)$.

One can check that there exists a ring which is flat.

Now we state the proposition:

- (21) Let us consider a flat ring R , and a polynomial p over R . Then $p \notin \Omega_R$. Note that every flat ring is polynomial-disjoint.
- (22) Let us consider a non degenerated ring R . Suppose $0 \in$ the carrier of R . Then R is not flat.

One can check that $\mathbb{Z}^{\mathbb{R}}$ is non flat and $\mathbb{F}_{\mathbb{Q}}$ is non flat and \mathbb{R}_F is non flat.

Let n be a non trivial natural number. One can verify that \mathbb{Z}/n is non flat.

4. SOME POSITIVE RESULTS

Now we state the proposition:

- (23) Let us consider a ring R , a polynomial p over R , and a natural number n . Then $p \neq n$.

Let n be a non trivial natural number. Let us observe that \mathbb{Z}/n is polynomial-disjoint and there exists a finite field which is polynomial-disjoint.

- (24) Let us consider a ring R , a polynomial p over R , and an integer i . Then $p \neq i$. The theorem is a consequence of (23).

One can verify that $\mathbb{Z}^{\mathbb{R}}$ is polynomial-disjoint.

- (25) Let us consider a ring R , a polynomial p over R , and a rational number r . Then $p \neq r$.

Observe that $\mathbb{F}_{\mathbb{Q}}$ is polynomial-disjoint. Now we state the proposition:

- (26) Let us consider a ring R , a polynomial p over R , and a real number r .
Then $p \neq r$.

Note that $\mathbb{R}_{\mathbb{F}}$ is polynomial-disjoint and there exists an infinite field which is polynomial-disjoint.

Let R be a polynomial-disjoint ring. Let us observe that $\text{PolyRing}(R)$ is polynomial-disjoint.

Let F be a field and p be an element of $\Omega_{\text{PolyRing}(F)}$. One can check that $\frac{\text{PolyRing}(F)}{\{p\}\text{-ideal}}$ is polynomial-disjoint.

Let F be a polynomial-disjoint field and p be a non constant element of the carrier of $\text{PolyRing}(F)$. One can check that $\text{PolyRing}(p)$ is polynomial-disjoint.

REFERENCES

- [1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Kornilowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.
- [2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Kornilowicz, 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.
- [3] Adam Grabowski, Artur Kornilowicz, 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.
- [4] Nathan Jacobson. *Basic Algebra I*. Dover Books on Mathematics, 1985.
- [5] Heinz Lüneburg. *Gruppen, Ringe, Körper: Die grundlegenden Strukturen der Algebra*. Oldenbourg Verlag, 1999.
- [6] Knut Radbruch. *Algebra I*. Lecture Notes, University of Kaiserslautern, Germany, 1991.

Accepted August 29, 2019
