FORMALIZED MATHEMATICS
Vol. 27, No. 3, Pages 229–235, 2019
DOI: 10.2478/forma-2019-0022

sciendo
https://www.sciendo.com/

Field Extensions and Kronecker's Construction

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Summary. This is the fourth part of a four-article series containing a Mizar [3], [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 [6], [4], [5].

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 the 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 ϕF 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 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 this 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

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

construction of the second part to $F[X]/{<}p{>}$ with the canonical monomorphism $\phi : F \longrightarrow F[X]/{<}p{>}$. 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_4`, version: `8.1.09 5.59.1363`

1. Preliminaries

From now on K, F, E denote fields and R, S denote rings.

Now we state the proposition:

(1) K is a subfield of K.

Let R be a non degenerated ring. One can verify that every subring of R is non degenerated.

Let R be a commutative ring. Note that every subring of R is commutative.

Let R be an integral domain. Let us observe that every subring of R is integral domain-like.

Now we state the proposition:

(2) Let us consider a subring S of R, a finite sequence F of elements of R, and a finite sequence G of elements of S. If $F = G$, then $\sum F = \sum G$.

2. Ring and Field Extensions

Let R, S be rings. We say that S is R-extending if and only if

(Def. 1) R is a subring of S.

Let R be a ring. Note that there exists a ring which is R-extending.

Let R be a commutative ring. One can check that there exists a commutative ring which is R-extending.

Let R be an integral domain. One can verify that there exists an integral domain which is R-extending.

Let F be a field. Let us observe that there exists a field which is F-extending.

Let R be a ring.

A ring extension of R is an R-extending ring. Let R be a commutative ring.

A commutative ring extension of R is an R-extending commutative ring. Let R be an integral domain.

A domain ring extension of R is an R-extending integral domain. Let F be a field.

An extension of F is an F-extending field. Now we state the propositions:

(3) R is a ring extension of R.

(4) Every commutative ring is a commutative ring extension of R.

(5) Every integral domain is a domain ring extension of R.

(6) F is an extension of F.

(7) E is an extension of F if and only if F is a subfield of E.

One can check that $\mathbb{C}_{\rm F}$ is $(\mathbb{R}_{\rm F})$-extending and $\mathbb{R}_{\rm F}$ is $(\mathbb{F}_{\mathbb{Q}})$-extending and $\mathbb{F}_{\mathbb{Q}}$ is $(\mathbb{Z}^{\rm R})$-extending.

Let R be a ring and S be a ring extension of R. One can check that every ring extension of S is R-extending.

Let R be a commutative ring and S be a commutative ring extension of R. One can verify that every commutative ring extension of S is R-extending.

Let R be an integral domain and S be a domain ring extension of R. Let us observe that every domain ring extension of S is R-extending.

Let F be a field and E be an extension of F. Observe that every extension of E is F-extending.

Let R be a non degenerated ring. Observe that every ring extension of R is non degenerated.

3. Extensions of Polynomial Rings

Now we state the propositions:

(8) Let us consider a ring extension S of R. Then every polynomial over R is a polynomial over S.

(9) Let us consider a subring R of S. Then every polynomial over R is a polynomial over S.

(10) Let us consider a ring extension S of R. Then the carrier of $\mathrm{PolyRing}(R) \subseteq$ the carrier of $\mathrm{PolyRing}(S)$. The theorem is a consequence of (8).

(11) If S is a ring extension of R, then $0_{\mathrm{PolyRing}(S)} = 0_{\mathrm{PolyRing}(R)}$.

(12) If S is a ring extension of R, then $\mathbf{0}.S = \mathbf{0}.R$. The theorem is a consequence of (11).

(13) If S is a ring extension of R, then $1_{\mathrm{PolyRing}(S)} = 1_{\mathrm{PolyRing}(R)}$. The theorem is a consequence of (12).

(14) Let us consider a ring extension S of R. Then $\mathbf{1}.S = \mathbf{1}.R$. The theorem is a consequence of (13).

(15) Let us consider a ring extension S of R, polynomials p, q over R, and polynomials p_1, q_1 over S. If $p = p_1$ and $q = q_1$, then $p + q = p_1 + q_1$.

(16) Let us consider a ring extension S of R. Then the addition of PolyRing

(R) = (the addition of PolyRing(S)) $\restriction$ (the carrier of PolyRing(R)). The theorem is a consequence of (10) and (15).

(17) Let us consider a ring extension S of R, polynomials p, q over R, and polynomials p_1, q_1 over S. If $p = p_1$ and $q = q_1$, then $p * q = p_1 * q_1$. The theorem is a consequence of (2).

(18) Suppose S is a ring extension of R. Then the multiplication of PolyRing (R) = (the multiplication of PolyRing(S)) $\restriction$ (the carrier of PolyRing(R)). The theorem is a consequence of (10) and (17).

Let R be a ring and S be a ring extension of R. One can verify that PolyRing(S) is (PolyRing(R))-extending. Now we state the propositions:

(19) Let us consider a ring R, and a ring extension S of R. Then PolyRing(S) is a ring extension of PolyRing(R).

(20) Let us consider a ring extension S of R, an element p of the carrier of PolyRing(R), and an element q of the carrier of PolyRing(S). If $p = q$, then $\deg p = \deg q$. The theorem is a consequence of (11).

(21) Let us consider a non degenerated ring R, a ring extension S of R, an element a of R, and an element b of S. If $a = b$, then $\mathrm{rpoly}(1, a) = \mathrm{rpoly}(1, b)$. The theorem is a consequence of (10).

4. Evaluation of Polynomials in Ring Extensions

Now we state the propositions:

(22) Let us consider an element a of S. Suppose S is a ring extension of R. Then $\mathrm{ExtEval}(\mathbf{0}.R, a) = 0_S$.

(23) Let us consider a non degenerated ring R, a ring extension S of R, and an element a of S. Then $\mathrm{ExtEval}(\mathbf{1}.R, a) = 1_S$.

(24) Let us consider a ring extension S of R, an element a of S, and polynomials p, q over R. Then $\mathrm{ExtEval}(p+q, a) = \mathrm{ExtEval}(p, a) + \mathrm{ExtEval}(q, a)$.

(25) Let us consider a commutative ring R, a commutative ring extension S of R, an element a of S, and polynomials p, q over R. Then $\mathrm{ExtEval}(p*q, a) = \mathrm{ExtEval}(p, a) \cdot \mathrm{ExtEval}(q, a)$.

(26) Let us consider a ring extension S of R, an element p of the carrier of PolyRing(R), an element q of the carrier of PolyRing(S), and an element a of S. If $p = q$, then $\mathrm{ExtEval}(p, a) = \mathrm{eval}(q, a)$. The theorem is a consequence of (11).

(27) Let us consider a ring extension S of R, an element p of the carrier of PolyRing(R), an element q of the carrier of PolyRing(S), an element a of

R, and an element b of S. If $q = p$ and $b = a$, then $\mathrm{eval}(q, b) = \mathrm{eval}(p, a)$. The theorem is a consequence of (26).

Let R be a ring, S be a ring extension of R, p be an element of the carrier of $\mathrm{PolyRing}(R)$, and a be an element of S. We say that a is a root of p in S if and only if

(Def. 2) $\mathrm{ExtEval}(p, a) = 0_S$.

We say that p has a root in S if and only if

(Def. 3) there exists an element a of S such that a is a root of p in S.

The functor $\mathrm{Roots}(S, p)$ yielding a subset of S is defined by the term

(Def. 4) $\{a$, where a is an element of $S : a$ is a root of p in $S\}$.

Now we state the proposition:

(28) Let us consider a ring extension S of R, and an element p of the carrier of $\mathrm{PolyRing}(R)$. Then $\mathrm{Roots}(p) \subseteq \mathrm{Roots}(S, p)$.

Let R be a ring, S be a non degenerated ring, and p be a polynomial over R. We say that p splits in S if and only if

(Def. 5) there exists a non zero element a of S and there exists a product of linear polynomials q of S such that $p = a \cdot q$.

Now we state the proposition:

(29) Let us consider a field F, and a polynomial p over F. If $\deg p = 1$, then p splits in F.

5. The Degree of Field Extensions

Let R be a ring and S be a ring extension of R. The functor $\mathrm{VecSp}(S, R)$ yielding a strict vector space structure over R is defined by

(Def. 6) the carrier of it = the carrier of S and the addition of it = the addition of S and the zero of $it = 0_S$ and the left multiplication of it = (the multiplication of S)$\restriction$((the carrier of R) $\times$ (the carrier of S)).

Observe that $\mathrm{VecSp}(S, R)$ is non empty and $\mathrm{VecSp}(S, R)$ is Abelian, add-associative, right zeroed, and right complementable and $\mathrm{VecSp}(S, R)$ is scalar distributive, scalar associative, scalar unital, and vector distributive.

Now we state the proposition:

(30) Let us consider a ring extension S of R. Then $\mathrm{VecSp}(S, R)$ is a vector space over R.

Let F be a field and E be an extension of F. The functor $\deg(E, F)$ yielding an integer is defined by the term

(Def. 7) $\begin{cases} \dim(\mathrm{VecSp}(E,F)), & \textbf{if } \mathrm{VecSp}(E,F) \text{ is finite dimensional,} \\ -1, & \textbf{otherwise}. \end{cases}$

Let us note that $\deg(E,F)$ is a dim-like.

We say that E is F-finite if and only if

(Def. 8) $\mathrm{VecSp}(E,F)$ is finite dimensional.

Observe that there exists an extension of F which is F-finite.

Let E be an F-finite extension of F. One can verify that $\deg(E,F)$ is natural.

6. Kronecker's Construction

Let F be a field and p be a non constant element of the carrier of PolyRing(F). Let us note that the carrier of PolyRing(p) is F-polynomial membered and PolyRing(p) is F-polynomial membered.

Let p be an irreducible element of the carrier of PolyRing(F). The functor KroneckerIso(p) yielding a function from the carrier of PolyRing(p) into the carrier of KroneckerField(F,p) is defined by

(Def. 9) for every element q of the carrier of PolyRing(p), $it(q) = [q]_{\mathrm{EqRel}(\mathrm{PolyRing}(F),\{p\}\text{–ideal})}$.

Observe that KroneckerIso(p) is additive, multiplicative, unity-preserving, one-to-one, and onto and KroneckerField(F,p) is (PolyRing(p))-homomorphic, (PolyRing(p))-monomorphic, and (PolyRing(p))-isomorphic.

PolyRing(p) is (KroneckerField(F,p))-homomorphic, (KroneckerField(F,p))-monomorphic, and (KroneckerField(F,p))-isomorphic and PolyRing(p) is F-homomorphic and F-monomorphic.

Now we state the proposition:

(31) Let us consider a polynomial-disjoint field F, and a non constant element f of the carrier of PolyRing(F). Then there exists an extension E of F such that f has a root in E.

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] 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.

[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