FORMALIZED MATHEMATICS
Vol. **28**, No. **2**, Pages 129–135, **2020**
DOI: 10.2478/forma-2020-0012

sciendo
https://www.sciendo.com/

Renamings and a Condition-free Formalization of Kronecker's Construction

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Summary. In [7], [9], [10] we presented a formalization of Kronecker's construction of a field extension E for a field F in which a given polynomial $p \in F[X]\backslash F$ has a root [5], [6], [3]. A drawback of our formalization was that it works only for polynomial-disjoint fields, that is for fields F with $F \cap F[X] = \emptyset$. The main purpose of Kronecker's construction is that by induction one gets a field extension of F in which p splits into linear factors. For our formalization this means that the constructed field extension E again has to be polynomial-disjoint.

In this article, by means of Mizar system [2], [1], we first analyze whether our formalization can be extended that way. Using the field of polynomials over F with degree smaller than the degree of p to construct the field extension E does not work: In this case E is polynomial-disjoint if and only if p is linear. Using $F[X]/{<}p{>}$ one can show that for $F = \mathbb{Q}$ and $F = \mathbb{Z}_n$ the constructed field extension E is again polynomial-disjoint, so that in particular algebraic number fields can be handled.

For the general case we then introduce renamings of sets X as injective functions f with $\mathrm{dom}(f) = X$ and $\mathrm{rng}(f) \cap (X \cup Z) = \emptyset$ for an arbitrary set Z. This, finally, allows to construct a field extension E of an arbitrary field F in which a given polynomial $p \in F[X]\backslash F$ splits into linear factors. Note, however, that to prove the existence of renamings we had to rely on the axiom of choice.

MSC: 12E05 12F05 68V20

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

MML identifier: `FIELD_5`, version: `8.1.10 5.63.1382`

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

1. Preliminaries

Now we state the proposition:

(1) Let us consider sets X, Y. If $Y \subseteq X$, then $X \setminus Y \cup Y = X$.

Let us consider natural numbers n, m. Now we state the propositions:

(2) (i) $n + m = n + m$, and

(ii) $n \cdot m = n \cdot m$.

(3) (i) $n \subseteq m$ iff $n \leqslant m$, and

(ii) $n \in m$ iff $n < m$.

Let us consider a natural number n. Now we state the propositions:

(4) $2^n = 2^n$.

(5) If $n \geqslant 3$, then $n + n < 2^n$.

(6) If $n \geqslant 3$, then $n + n \in 2^n$. The theorem is a consequence of (2), (5), (3), and (4).

(7) $\mathbb{N}$ meets $2^{\mathbb{N}}$.

Let us consider a set X. Now we state the propositions:

(8) There exists an object o such that $o \notin X$.

(9) There exists a set Y such that

(i) $\overline{\overline{X}} \subseteq \overline{\overline{Y}}$, and

(ii) $X \cap Y = \emptyset$.

(10) Let us consider sets X, Y. Suppose $\overline{\overline{X}} \subseteq \overline{\overline{Y}}$. Then there exists a set Z such that

(i) $Z \subseteq Y$, and

(ii) $\overline{\overline{Z}} = \overline{\overline{X}}$.

(11) Let us consider a set X. Then there exists a set Y such that

(i) $\overline{\overline{X}} = \overline{\overline{Y}}$, and

(ii) $X \cap Y = \emptyset$.

The theorem is a consequence of (9) and (10).

(12) Let us consider a field E. Then every subfield of E is a subring of E.

(13) Let us consider a field F, and a subring R of F. Then R is a subfield of F if and only if R is a field.

Let F be a field and E be an extension of F. Note that there exists an extension of F which is E-extending. We introduce the notation E is F-infinite as an antonym for E is F-finite. Let us consider a field F, an extension E of F, and an E-extending extension K of F.

(14) $\mathrm{VecSp}(E, F)$ is a subspace of $\mathrm{VecSp}(K, F)$.

(15) (i) K is F-infinite, or

(ii) E is F-finite and $\deg(E, F) \leqslant \deg(K, F)$.

The theorem is a consequence of (14).

(16) Let us consider a field F, a polynomial p over F, and a non zero polynomial q over F. Then $\deg(p \bmod q) < \deg q$.

2. Linear Polynomials

Let R be a ring and p be a polynomial over R. We say that p is linear if and only if

(Def. 1) $\deg p = 1$.

Let R be a non degenerated ring. One can check that there exists a polynomial over R which is linear and there exists a polynomial over R which is non linear and there exists an element of the carrier of $\mathrm{PolyRing}(R)$ which is linear and there exists an element of the carrier of $\mathrm{PolyRing}(R)$ which is non linear and every polynomial over R which is zero is also non linear and every polynomial over R which is constant is also non linear.

Let F be a field. Let us note that every polynomial over F which is linear has also roots and every element of the carrier of $\mathrm{PolyRing}(F)$ which is linear is also irreducible and every element of the carrier of $\mathrm{PolyRing}(F)$ which is non linear and has roots is also reducible.

Let R be an integral domain, p be a linear polynomial over R, and q be a non constant polynomial over R. Let us note that $p * q$ is non linear.

Let F be a field, p be a linear polynomial over F, and q be a non constant polynomial over F. Let us note that $p * q$ has roots.

3. More on PolyRing(p)

Let F be a field and p be a non constant element of the carrier of $\mathrm{PolyRing}(F)$. The functor $\mathrm{canHomP}(p)$ yielding a function from F into $\mathrm{PolyRing}(p)$ is defined by

(Def. 2) for every element a of F, $it(a) = a{\restriction}F$.

One can verify that $\mathrm{canHomP}(p)$ is additive, multiplicative, unity-preserving, and one-to-one and $\mathrm{PolyRing}(p)$ is F-homomorphic and F-monomorphic.

Let F be a polynomial-disjoint field and p be an irreducible element of the carrier of $\mathrm{PolyRing}(F)$. One can verify that $\mathrm{embField}(\mathrm{canHomP}(p))$ is add-associative, right complementable, associative, distributive, and almost left invertible and $\mathrm{embField}(\mathrm{canHomP}(p))$ is F-extending.

The functor KrRootP(p) yielding an element of embField(canHomP(p)) is defined by the term

(Def. 3) $((\text{emb-iso}(\text{canHomP}(p)))^{-1} \cdot ((\text{KroneckerIso}(p))^{-1}))(\text{KrRoot}(p))$.

Now we state the proposition:

(17) Let us consider a polynomial-disjoint field F, and an irreducible element p of the carrier of PolyRing(F). Then $\text{ExtEval}(p, \text{KrRootP}(p)) = 0_F$.
PROOF: Set $K = \text{KroneckerField}(F, p)$. Set $E = \text{embField}(\text{canHomP}(p))$. Set $h = (\text{KroneckerIso}(p)) \cdot (\text{emb-iso}(\text{canHomP}(p)))$. Reconsider $P = K$ as an E-isomorphic field. Reconsider $i_1 = h$ as an isomorphism between E and P. Reconsider $i_2 = {i_1}^{-1}$ as a homomorphism from P to E. Reconsider $t = p_p$ as an element of the carrier of PolyRing(P). $(\text{PolyHom}(i_2))(t) = p$ by [4, (12)], [8, (17)]. □

4. On Embedding F into $F[X]/\langle p \rangle$ and PolyRing(p)

Now we state the propositions:

(18) Let us consider a field F, and a linear element p of the carrier of PolyRing(F). Then

(i) PolyRing(p) and F are isomorphic, and

(ii) the carrier of embField(canHomP(p)) = the carrier of F.

(19) Let us consider a strict field F, and a linear element p of the carrier of PolyRing(F). Then embField(canHomP(p)) = F. The theorem is a consequence of (18).

(20) Let us consider a field F, and a linear element p of the carrier of PolyRing(F). Then

(i) $\frac{\text{PolyRing}(F)}{\{p\}\text{-ideal}}$ and F are isomorphic, and

(ii) the carrier of embField(embedding(p)) = the carrier of F.

The theorem is a consequence of (18) and (16).

(21) Let us consider a strict field F, and a linear element p of the carrier of PolyRing(F). Then embField(embedding(p)) = F. The theorem is a consequence of (20).

(22) Let us consider a polynomial-disjoint field F, and an irreducible element p of the carrier of PolyRing(F). Then embField(canHomP(p)) is polynomial-disjoint if and only if p is linear. The theorem is a consequence of (18).

(23) Let us consider a field F, an irreducible element p of the carrier of PolyRing(F), and a polynomial-disjoint field E.
Suppose $E = \mathrm{embField}(\mathrm{embedding}(p))$. Then F is polynomial-disjoint.

Let n be a prime number and p be an irreducible element of the carrier of PolyRing($\mathbb{Z}/n$). Let us observe that embField(embedding(p)) is add-associative, right complementable, associative, distributive, and almost left invertible.

Let p be an irreducible element of the carrier of PolyRing($\mathbb{F}_{\mathbb{Q}}$). Let us note that embField(embedding(p)) is add-associative, right complementable, associative, distributive, and almost left invertible.

(24) Let us consider a prime number n, and a non constant element p of the carrier of PolyRing($\mathbb{Z}/n$). Then $\mathbb{Z}/n$ and $\frac{\mathrm{PolyRing}(\mathbb{Z}/n)}{\{p\}\text{–ideal}}$ are disjoint.

(25) Let us consider a non constant element p of the carrier of PolyRing($\mathbb{F}_{\mathbb{Q}}$). Then $\mathbb{F}_{\mathbb{Q}}$ and $\frac{\mathrm{PolyRing}(\mathbb{F}_{\mathbb{Q}})}{\{p\}\text{–ideal}}$ are disjoint.

Let n be a prime number and p be an irreducible element of the carrier of PolyRing($\mathbb{Z}/n$). Let us note that embField(embedding(p)) is polynomial-disjoint.

Let p be an irreducible element of the carrier of PolyRing($\mathbb{F}_{\mathbb{Q}}$). One can check that embField(embedding(p)) is polynomial-disjoint.

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

(Def. 4) for every element a of R and for every ring S and for every element p of the carrier of PolyRing(S), $a \neq p$.

Observe that $\mathbb{Z}^{\mathrm{R}}$ is strong polynomial disjoint and $\mathbb{F}_{\mathbb{Q}}$ is strong polynomial disjoint and $\mathbb{R}_{\mathrm{F}}$ is strong polynomial disjoint.

Let n be a non trivial natural number. Note that $\mathbb{Z}/n$ is strong polynomial disjoint and every ring which is strong polynomial disjoint is also polynomial-disjoint and there exists a field which is strong polynomial disjoint and there exists a field which is non strong polynomial disjoint.

(26) Let us consider a strong polynomial disjoint field F, an irreducible element p of the carrier of PolyRing(F), and a field E.
Suppose $E = \mathrm{embField}(\mathrm{embedding}(p))$. Then E is strong polynomial disjoint.

5. Renamings

Let X be a non empty set and Z be a set.

A Renaming of X and Z is a function defined by

(Def. 5) $\mathrm{dom}\, it = X$ and it is one-to-one and $\mathrm{rng}\, it \cap (X \cup Z) = \emptyset$.

Let r be a Renaming of X and Z. Let us note that $\mathrm{dom}\, r$ is non empty and $\mathrm{rng}\, r$ is non empty and every Renaming of X and Z is X-defined and one-to-one.

Let r be a Renaming of X and Z. Observe that the functor r^{-1} yields a function from $\operatorname{rng} r$ into X. Now we state the proposition:

(27) Let us consider a non empty set X, a set Z, and a Renaming r of X and Z. Then r^{-1} is onto.

Let F be a field, Z be a set, and r be a Renaming of the carrier of F and Z. The functor ren-add(r) yielding a binary operation on $\operatorname{rng} r$ is defined by

(Def. 6) for every elements a, b of $\operatorname{rng} r$, $it(a,b) = r((r^{-1})(a) + (r^{-1})(b))$.

The functor ren-mult(r) yielding a binary operation on $\operatorname{rng} r$ is defined by

(Def. 7) for every elements a, b of $\operatorname{rng} r$, $it(a,b) = r((r^{-1})(a) \cdot (r^{-1})(b))$.

The functor RenField(r) yielding a strict double loop structure is defined by

(Def. 8) the carrier of $it = \operatorname{rng} r$ and the addition of $it =$ ren-add(r) and the multiplication of $it =$ ren-mult(r) and the one of $it = r(1_F)$ and the zero of $it = r(0_F)$.

One can check that RenField(r) is non degenerated and RenField(r) is Abelian, add-associative, right zeroed, and right complementable and RenField(r) is commutative, associative, well unital, distributive, and almost left invertible.

One can check that the functor r^{-1} yields a function from RenField(r) into F. Now we state the propositions:

(28) Let us consider a field F, a set Z, and a Renaming r of the carrier of F and Z. Then r^{-1} is additive, multiplicative, unity-preserving, one-to-one, and onto. The theorem is a consequence of (27).

(29) Let us consider a field F, and a set Z. Then there exists a field E such that

   (i) E and F are isomorphic, and

   (ii) (the carrier of E) $\cap$ ((the carrier of F) $\cup$ Z) $= \emptyset$.

The theorem is a consequence of (28).

6. Kronecker's Construction

Let us consider a field F and a non constant element f of the carrier of PolyRing(F). Now we state the propositions:

(30) There exists an extension E of F such that f has a root in E.

(31) There exists an extension E of F such that f splits in E.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every field F for every non constant element f of the carrier of PolyRing(F) such that $\deg f = \$_1$ there exists an extension E of F such that f splits in E. $\mathcal{P}[1]$. For every non zero natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $\deg f = n$. $\square$

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, 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 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.

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

[4] Artur Korniłowicz. Quotient rings. *Formalized Mathematics*, 13(**4**):573–576, 2005.

[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.

[7] Christoph Schwarzweller. On roots of polynomials over $F[X]/\langle p \rangle$. *Formalized Mathematics*, 27(**2**):93–100, 2019. doi:10.2478/forma-2019-0010.

[8] Christoph Schwarzweller. On monomorphisms and subfields. *Formalized Mathematics*, 27(**2**):133–137, 2019. doi:10.2478/forma-2019-0014.

[9] Christoph Schwarzweller. Field extensions and Kronecker's construction. *Formalized Mathematics*, 27(**3**):229–235, 2019. doi:10.2478/forma-2019-0022.

[10] Christoph Schwarzweller. Representation matters: An unexpected property of polynomial rings and its consequences for formalizing abstract field theory. In M. Ganzha, L. Maciaszek, and M. Paprzycki, editors, *Proceedings of the 2018 Federated Conference on Computer Science and Information Systems*, volume 15 of *Annals of Computer Science and Information Systems*, pages 67–72. IEEE, 2018. doi:10.15439/2018F88.

Accepted May 19, 2020