FORMALIZED MATHEMATICS
Vol. 27, No. 2, Pages 93–100, 2019
DOI: 10.2478/forma-2019-0010

sciendo
https://www.sciendo.com/

On Roots of Polynomials over $F[X]/\langle p\rangle$

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Summary. This is the first 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 $p \in F[X]\backslash F$ 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 [9], [4], [6].

In this 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 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)

$\phi : F \longrightarrow F[X]/{<}p{>}$. 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_1`, version: `8.1.09 5.57.1355`

1. Preliminaries

From now on n denotes a natural number.

Let L be a non empty zero structure and p be a polynomial over L. We introduce the notation $\mathrm{LM}(p)$ as a synonym of Leading-Monomial p.

Now we state the proposition:

(1) Let us consider a non empty zero structure L, and a polynomial p over L. Then $\deg p$ is an element of $\mathbb{N}$ if and only if $p \neq \mathbf{0}.L$.

Let R be a non degenerated ring and p be a non zero polynomial over R. Note that the functor $\deg p$ yields an element of $\mathbb{N}$. Let R be an add-associative, right zeroed, right complementable, right distributive, non empty double loop structure and f be an additive function from R into R. One can check that $f(0_R)$ reduces to 0_R.

Now we state the proposition:

(2) Let us consider a ring R, an ideal I of R, an element x of ${}^{R}/_{I}$, and an element a of R. Suppose $x = [a]_{\mathrm{EqRel}(R,I)}$. Let us consider a natural number n. Then $x^n = [a^n]_{\mathrm{EqRel}(R,I)}$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv x^{\$_1} = [a^{\$_1}]_{\mathrm{EqRel}(R,I)}$. For every natural number i, $\mathcal{P}[i]$. $\square$

Let R be a ring and a, b be elements of R. We say that b is an irreducible factor of a if and only if

(Def. 1) $b \mid a$ and b is irreducible.

Observe that there exists an integral domain which is non almost left invertible and factorial.

Now we state the proposition:

(3) Let us consider a non almost left invertible, factorial integral domain R, and a non zero non-unit a of R. Then there exists an element b of R such that b is an irreducible factor of a.

2. The Polynomials $a \cdot x^n$

Let R be a ring, a be an element of R, and n be a natural number. We introduce the notation anpoly(a, n) as a synonym of seq(n, a).

Let R be a non degenerated ring and a be a non zero element of R. One can check that anpoly(a, n) is non zero.

Let R be a ring and a be a zero element of R. Observe that anpoly(a, n) is zero.

Now we state the propositions:

(4) Let us consider a non degenerated ring R, and a non zero element a of R. Then $\deg \text{anpoly}(a, n) = n$.

(5) Let us consider a non degenerated ring R, and an element a of R. Then $\text{LC}\,\text{anpoly}(a, n) = a$.

(6) Let us consider a non degenerated ring R, a non zero natural number n, and elements a, x of R. Then $\text{eval}(\text{anpoly}(a, n), x) = a \cdot (x^n)$.

(7) Let us consider a non degenerated ring R, and an element a of R. Then $\text{anpoly}(a, 0) = a \restriction R$.

(8) Let us consider a non degenerated ring R, and a non zero element n of $\mathbb{N}$. Then $\text{anpoly}(1_R, n) = \text{rpoly}(n, 0_R)$.

(9) Let us consider a non degenerated commutative ring R, and non zero elements a, b of R. Then $b \cdot (\text{anpoly}(a, n)) = \text{anpoly}(a \cdot b, n)$.

(10) Let us consider a non degenerated commutative ring R, non zero elements a, b of R, and natural numbers n, m. Then $\text{anpoly}(a, n) * \text{anpoly}(b, m) = \text{anpoly}(a \cdot b, n + m)$. The theorem is a consequence of (9).

(11) Let us consider a non degenerated ring R, and a non zero polynomial p over R. Then $\text{LM}(p) = \text{anpoly}(p(\deg p), \deg p)$.

(12) Let us consider a non degenerated commutative ring R. Then $\langle 0_R, 1_R\rangle^n = \text{anpoly}(1_R, n)$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv \langle 0_R, 1_R\rangle^{\$_1} = \text{anpoly}(1_R, \$_1)$. $\mathcal{P}[0]$ by [8, (15)]. For every natural number k, $\mathcal{P}[k]$. □

3. More on Homomorphisms

Now we state the propositions:

(13) Let us consider a ring R, an R-homomorphic ring S, a homomorphism h from R to S, an element a of R, and a natural number n. Then $h(a^n) = h(a)^n$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv h(a^{\$_1}) = h(a)^{\$_1}$. $\mathcal{P}[0]$ by [10, (8)]. For every natural number n, $\mathcal{P}[n]$. □

(14) Let us consider a ring R, an R-homomorphic ring S, and a homomorphism h from R to S. Then $h(\sum \varepsilon_\alpha) = 0_S$, where α is the carrier of R.

Let us consider a ring R, an R-homomorphic ring S, a homomorphism h from R to S, a finite sequence F of elements of R, and an element a of R. Now we state the propositions:

(15) $h(\sum(\langle a\rangle \frown F)) = h(a) + h(\sum F)$.

(16) $h(\sum(F \frown \langle a\rangle)) = h(\sum F) + h(a)$.

(17) Let us consider a ring R, an R-homomorphic ring S, a homomorphism h from R to S, and finite sequences F, G of elements of R. Then $h(\sum(F \frown G)) = h(\sum F) + h(\sum G)$.

(18) Let us consider a ring R, an R-homomorphic ring S, and a homomorphism h from R to S. Then $h(\prod \varepsilon_\alpha) = 1_S$, where α is the carrier of R.

Let us consider a ring R, an R-homomorphic ring S, a homomorphism h from R to S, a finite sequence F of elements of R, and an element a of R. Now we state the propositions:

(19) $h(\prod(\langle a\rangle \frown F)) = h(a) \cdot h(\prod F)$.

(20) $h(\prod(F \frown \langle a\rangle)) = h(\prod F) \cdot h(a)$.

(21) Let us consider a ring R, an R-homomorphic ring S, a homomorphism h from R to S, and finite sequences F, G of elements of R. Then $h(\prod(F \frown G)) = h(\prod F) \cdot h(\prod G)$.

4. Lifting Homomorphisms from R to $R[X]$

Let R, S be rings, f be a function from PolyRing(R) into PolyRing(S), and p be an element of the carrier of PolyRing(R). Observe that the functor $f(p)$ yields an element of the carrier of PolyRing(S). Let R be a ring, S be an R-homomorphic ring, and h be an additive function from R into S. The functor PolyHom(h) yielding a function from PolyRing(R) into PolyRing(S) is defined by

(Def. 2) for every element f of the carrier of PolyRing(R) and for every natural number i, $(it(f))(i) = h(f(i))$.

Let h be a homomorphism from R to S. Observe that PolyHom(h) is additive, multiplicative, and unity-preserving.

Let us consider a ring R, an R-homomorphic ring S, and a homomorphism h from R to S. Now we state the propositions:

(22) $(\mathrm{PolyHom}(h))(\mathbf{0}.R) = \mathbf{0}.S$.

(23) $(\mathrm{PolyHom}(h))(\mathbf{1}.R) = \mathbf{1}.S$.

Let us consider a ring R, an R-homomorphic ring S, a homomorphism h from R to S, and elements p, q of the carrier of PolyRing(R). Now we state the propositions:

(24) $(\mathrm{PolyHom}(h))(p+q) = (\mathrm{PolyHom}(h))(p) + (\mathrm{PolyHom}(h))(q)$.

(25) $(\mathrm{PolyHom}(h))(p \cdot q) = (\mathrm{PolyHom}(h))(p) \cdot (\mathrm{PolyHom}(h))(q)$.

(26) Let us consider a ring R, an R-homomorphic ring S, a homomorphism h from R to S, an element p of the carrier of PolyRing(R), and an element b of R. Then $(\mathrm{PolyHom}(h))(b \cdot p) = h(b) \cdot (\mathrm{PolyHom}(h))(p)$.

(27) Let us consider a ring R, an R-homomorphic ring S, a homomorphism h from R to S, an element p of the carrier of PolyRing(R), and an element a of R. Then $h(\mathrm{eval}(p, a)) = \mathrm{eval}((\mathrm{PolyHom}(h))(p), h(a))$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every element p of the carrier of PolyRing(R) for every element a of R such that $\mathrm{len}\, p = \$_1$ holds $h(\mathrm{eval}(p, a)) = \mathrm{eval}((\mathrm{PolyHom}(h))(p), h(a))$. $\mathcal{P}[0]$ by [7, (5), (17)], [5, (6)], (22). For every natural number k, $\mathcal{P}[k]$. □

(28) Let us consider an integral domain R, an R-homomorphic integral domain S, a homomorphism h from R to S, an element p of the carrier of PolyRing(R), and elements b, x of R. Then $h(\mathrm{eval}(b \cdot p, x)) = h(b) \cdot (\mathrm{eval}((\mathrm{PolyHom}(h))(p), h(x)))$. The theorem is a consequence of (27) and (26).

Let R be a ring. One can check that there exists a ring which is R-homomorphic and R-monomorphic and there exists a ring which is R-homomorphic and R-isomorphic and every ring which is R-monomorphic is also R-homomorphic.

Let S be an R-homomorphic, R-monomorphic ring and h be a monomorphism of R and S. Note that PolyHom(h) is monomorphic.

Let S be an R-isomorphic, R-homomorphic ring and h be an isomorphism between R and S. Let us note that PolyHom(h) is isomorphism.

Now we state the propositions:

(29) Let us consider a ring R, an R-homomorphic ring S, a homomorphism h from R to S, and an element p of the carrier of PolyRing(R). Then $\deg(\mathrm{PolyHom}(h))(p) \leqslant \deg p$.

(30) Let us consider a non degenerated ring R, an R-homomorphic ring S, a homomorphism h from R to S, and a non zero element p of the carrier of PolyRing(R). Then $\deg(\mathrm{PolyHom}(h))(p) = \deg p$ if and only if $h(\mathrm{LC}\, p) \neq 0_S$.

Let us consider a ring R, an R-monomorphic, R-homomorphic ring S, a monomorphism h of R and S, and an element p of the carrier of PolyRing(R). Now we state the propositions:

(31) $\deg(\mathrm{PolyHom}(h))(p) = \deg p$.

(32) $\mathrm{LM}((\mathrm{PolyHom}(h))(p)) = (\mathrm{PolyHom}(h))(\mathrm{LM}(p))$. The theorem is a consequence of (31).

(33) Let us consider a ring R, an R-homomorphic ring S, a homomorphism h from R to S, an element p of the carrier of PolyRing(R), and an element a of R. If a is a root of p, then $h(a)$ is a root of $(\mathrm{PolyHom}(h))(p)$. The theorem is a consequence of (27).

(34) Let us consider a ring R, an R-monomorphic, R-homomorphic ring S, a monomorphism h of R and S, an element p of the carrier of PolyRing(R), and an element a of R. Then a is a root of p if and only if $h(a)$ is a root of $(\mathrm{PolyHom}(h))(p)$. The theorem is a consequence of (27) and (33).

(35) Let us consider a ring R, an R-isomorphic, R-homomorphic ring S, an isomorphism h between R and S, an element p of the carrier of PolyRing (R), and an element b of S. Then b is a root of $(\mathrm{PolyHom}(h))(p)$ if and only if there exists an element a of R such that a is a root of p and $h(a) = b$. The theorem is a consequence of (27).

(36) Let us consider a ring R, an R-homomorphic ring S, a homomorphism h from R to S, and an element p of the carrier of PolyRing(R). Then $\mathrm{Roots}(p) \subseteq \{a$, where a is an element of $R : h(a) \in \mathrm{Roots}((\mathrm{PolyHom}(h))(p))\}$. The theorem is a consequence of (33).

(37) Let us consider a ring R, an R-monomorphic, R-homomorphic ring S, a monomorphism h of R and S, and an element p of the carrier of PolyRing(R). Then $\mathrm{Roots}(p) = \{a$, where a is an element of $R : h(a) \in \mathrm{Roots}((\mathrm{PolyHom}(h))(p))\}$. The theorem is a consequence of (36) and (34).

(38) Let us consider a ring R, an R-isomorphic, R-homomorphic ring S, an isomorphism h between R and S, and an element p of the carrier of PolyRing(R). Then $\mathrm{Roots}((\mathrm{PolyHom}(h))(p)) = \{h(a)$, where a is an element of $R : a \in \mathrm{Roots}(p)\}$. The theorem is a consequence of (35).

5. Kronecker's Construction

In the sequel F denotes a field, p denotes an irreducible element of the carrier of PolyRing(F), f denotes an element of the carrier of PolyRing(F), and a denotes an element of F.

Let us consider F and p. The functor KroneckerField(F, p) yielding a field is defined by the term

(Def. 3) $\mathrm{PolyRing}(F)/_{\{p\}\text{–ideal}}$.

The functor embedding(p) yielding a function from F into KroneckerField (F, p) is defined by the term

(Def. 4) (the canonical homomorphism of $\{p\}$–ideal into quotient field) $\cdot$ (the canonical homomorphism of F into quotient field).

Let us observe that embedding(p) is additive, multiplicative, and unity-preserving and embedding(p) is monomorphic and KroneckerField(F,p) is F-homomorphic and F-monomorphic.

Let us consider f. The functor f_p yielding an element of the carrier of PolyRing(KroneckerField(F,p)) is defined by the term

(Def. 5) (PolyHom(embedding(p)))(f).

The functor KrRoot(p) yielding an element of KroneckerField(F,p) is defined by the term

(Def. 6) $[\langle 0_F, 1_F\rangle]_{\mathrm{EqRel(PolyRing}(F),\{p\}\text{–ideal})}$.

Now we state the propositions:

(39) (embedding(p))$(a) = [a{\restriction}F]_{\mathrm{EqRel(PolyRing}(F),\{p\}\text{–ideal})}$.

(40) $(f_p)(n) = [f(n){\restriction}F]_{\mathrm{EqRel(PolyRing}(F),\{p\}\text{–ideal})}$. The theorem is a consequence of (39).

(41) eval$(f_p$, KrRoot$(p)) = [f]_{\mathrm{EqRel(PolyRing}(F),\{p\}\text{–ideal})}$.
PROOF: Set $z =$ KrRoot(p). Define $\mathcal{P}$[natural number] $\equiv$ for every f such that len $f = \$_1$ holds eval$(f_p, z) = [f]_{\mathrm{EqRel(PolyRing}(F),\{p\}\text{–ideal})}$. For every natural number k, $\mathcal{P}[k]$. $\square$

(42) KrRoot(p) is a root of p_p. The theorem is a consequence of (41).

(43) If f is not constant, then there exists an irreducible element p of the carrier of PolyRing(F) such that f_p has roots. The theorem is a consequence of (3) and (42).

(44) If embedding(p) is isomorphism, then p has roots. The theorem is a consequence of (38) and (42).

(45) If p has no roots, then embedding(p) is not isomorphism.

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] 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 Infor-*

mation 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] Artur Korniłowicz and Christoph Schwarzweller. The first isomorphism theorem and other properties of rings. *Formalized Mathematics*, 22(**4**):291–301, 2014. doi:10.2478/forma-2014-0029.

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

[7] Robert Milewski. The evaluation of polynomials. *Formalized Mathematics*, 9(**2**):391–395, 2001.

[8] Robert Milewski. Fundamental theorem of algebra. *Formalized Mathematics*, 9(**3**):461–470, 2001.

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

[10] Christoph Schwarzweller. The binomial theorem for algebraic structures. *Formalized Mathematics*, 9(**3**):559–564, 2001.

Accepted March 28, 2019