FORMALIZED MATHEMATICS
Vol. 29, No. 4, Pages 229–240, 2021
DOI: 10.2478/forma-2021-0021

sciendo
https://sciendo.com/journal/forma

Quadratic Extensions

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Agnieszka Rowińska-Schwarzweller
Sopot, Poland

Summary. In this article we further develop field theory [6], [7], [12] in Mizar [1], [2], [3]: we deal with quadratic polynomials and quadratic extensions [5], [4]. First we introduce quadratic polynomials, their discriminants and prove the midnight formula. Then we show that - in case the discriminant of p being non square - adjoining a root of p's discriminant results in a splitting field of p. Finally we prove that these are the only field extensions of degree 2, e.g. that an extension E of F is quadratic if and only if there is a non square Element $a \in F$ such that E and $F(\sqrt{a})$ are isomorphic over F.

MSC: 12F05 68V20

Keywords: field extensions; quadratic polynomials; quadratic extensions

MML identifier: `FIELD_9`, version: `8.1.11 5.68.1412`

1. Preliminaries

Now we state the proposition:

(1) Let us consider natural numbers a, b. If $a \leqslant b$, then $a -' 1 \leqslant b -' 1$.

Let i be an integer. One can check that $i^{\mathbf{2}}$ is integer.

Let R be a ring, S be a ring extension of R, and a be an R-membered element of S. The functor ${}^{@}a$ yielding an element of R is defined by the term

(Def. 1) a.

One can verify that $-a$ is R-membered.

Let a, b be R-membered elements of S. One can verify that $a + b$ is R-membered and $a \cdot b$ is R-membered and 0_S is R-membered.

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

Let R be a non degenerated ring. One can check that 1_S is non zero and R-membered and there exists an element of S which is non zero and R-membered.

Let F be a field, E be an extension of F, and a be a non zero, F-membered element of E. Let us observe that a^{-1} is F-membered.

Let R be a ring and a, b, c be elements of R. One can check that $\langle a, b, c\rangle$ is (the carrier of R)-valued and there exists a field which is strict and has not characteristic 2.

Let R be a ring. One can check that $(0_R)^{\mathbf{2}}$ reduces to 0_R and $(1_R)^{\mathbf{2}}$ reduces to 1_R and $(-1_R)^{\mathbf{2}}$ reduces to 1_R.

Now we state the propositions:

(2) Let us consider a commutative ring R, and elements a, b of R. Then $(a \cdot b)^{\mathbf{2}} = a^{\mathbf{2}} \cdot b^{\mathbf{2}}$.

(3) Let us consider a field F, an element a of F, a non zero element b of F, and an integer i. Suppose $i \star a \neq 0_F$ and $i \star b \neq 0_F$. Then $(i \star a) \cdot (i \star b)^{-1} = a \cdot b^{-1}$.

(4) Let us consider a commutative ring R, an element a of R, and an integer i. Then $(i \star a)^{\mathbf{2}} = i^{\mathbf{2}} \star a^{\mathbf{2}}$.

Let us consider an integral domain R with non characteristic 2 and an element a of R. Now we state the propositions:

(5) $2 \star a = 0_R$ if and only if $a = 0_R$.

(6) $4 \star a = 0_R$ if and only if $a = 0_R$. The theorem is a consequence of (5).

(7) Let us consider a ring R, a ring extension S of R, an element a of R, and an element b of S. If $b = a$, then for every integer i, $i \star a = i \star b$.

PROOF: Define $\mathcal{P}[\text{integer}] \equiv$ for every integer k such that $k = \$_1$ holds $k \star a = k \star b$. For every integer u such that $\mathcal{P}[u]$ holds $\mathcal{P}[u-1]$ and $\mathcal{P}[u+1]$ by [11, (62), (64)], [8, (15)]. For every integer i, $\mathcal{P}[i]$. $\square$

(8) Let us consider an integral domain R, a domain ring extension S of R, an element a of R, and an element b of S. If $b^{\mathbf{2}} = a^{\mathbf{2}}$, then $b = a$ or $b = -a$.

Let us consider a field F, an extension E of F, and an element a of E. Now we state the propositions:

(9) $\mathrm{FAdj}(F, \{a, -a\}) = \mathrm{FAdj}(F, \{a\})$.

(10) $\mathrm{FAdj}(F, \{a\}) = \mathrm{FAdj}(F, \{-a\})$. The theorem is a consequence of (9).

One can check that there exists a polynomial-disjoint field which is non algebraic closed.

Let F be a non algebraic closed field. One can verify that there exists an element of the carrier of $\mathrm{PolyRing}(F)$ which is irreducible and non linear.

Let F be a field. One can verify that every element of the carrier of $\mathrm{PolyRing}(F)$ which is irreducible and non linear and has also not roots and every element of the carrier of PolyRing(F) which is irreducible and has roots is also linear.

Let F be a polynomial-disjoint field and p be an irreducible element of the carrier of PolyRing(F). Note that KrRootP(p) is F-algebraic.

Let F be a non algebraic closed, polynomial-disjoint field and p be an irreducible, non linear element of the carrier of PolyRing(F). Let us note that KrRootP(p) is non zero and non F-membered.

2. More on Polynomials

Now we state the proposition:

(11) Let us consider a non degenerated ring R, a non zero polynomial p over R, and a polynomial q over R. Then $\deg(p * q) \leqslant \deg p + \deg q$.

Let L be a well unital, non degenerated double loop structure, k be a non zero element of $\mathbb{N}$, and a be an element of L. Let us note that rpoly(k, a) is monic.

Let R be a non degenerated ring, a be a non zero element of R, and b be an element of R. Let us note that $\langle b, a\rangle$ is linear and $\langle b, 1_R\rangle$ is monic and linear.

Now we state the propositions:

(12) Let us consider a ring R, and elements a, b, x of R. Then $x \cdot \langle b, a\rangle = \langle x \cdot b, x \cdot a\rangle$.

(13) Let us consider a ring R, and a polynomial p over R. Suppose $\deg p < 2$. Let us consider an element a of R. Then there exist elements y, z of R such that $p = \langle y, z\rangle$.

(14) Let us consider a commutative ring R, and a polynomial p over R. Suppose $\deg p < 2$. Let us consider an element a of R. Then there exist elements y, z of R such that $\mathrm{eval}(p, a) = y + a \cdot z$. The theorem is a consequence of (13).

(15) Let us consider a field F, an extension E of F, and a polynomial p over F. Suppose $\deg p < 2$. Let us consider an element a of E. Then there exist F-membered elements y, z of E such that $\mathrm{ExtEval}(p, a) = y + a \cdot z$. The theorem is a consequence of (13).

Let R be a ring and a be an element of R. The functors: X- a and X+ a yielding elements of the carrier of PolyRing(R) are defined by terms

(Def. 2) rpoly($1, a$),

(Def. 3) rpoly($1, -a$),

respectively. Let R be a non degenerated ring. Let us observe that X- a is linear and monic and X+ a is linear and monic.

3. Quadratic Polynomials

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

(Def. 4) $\deg p = 2$.

Let R be a non degenerated ring. Note that there exists a polynomial over R which is monic and quadratic and there exists an element of the carrier of PolyRing(R) which is monic and quadratic and every quadratic polynomial over R is non constant and every quadratic element of the carrier of PolyRing(R) is non constant.

Let L be a non empty zero structure and a, b, c be elements of L. The functor $\langle c, b, a\rangle$ yielding a sequence of L is defined by the term

(Def. 5) $((\mathbf{0}.L +\cdot (0, c)) +\cdot (1, b)) +\cdot (2, a)$.

Note that $\langle c, b, a\rangle$ is finite-Support.

Let us consider a non empty zero structure L and elements a, b, c of L. Now we state the propositions:

(16) (i) $\langle c, b, a\rangle(0) = c$, and

(ii) $\langle c, b, a\rangle(1) = b$, and

(iii) $\langle c, b, a\rangle(2) = a$, and

(iv) for every natural number n such that $n \geqslant 3$ holds $\langle c, b, a\rangle(n) = 0_L$.

(17) $\deg\langle c, b, a\rangle \leqslant 2$.

(18) $\deg\langle c, b, a\rangle = 2$ if and only if $a \neq 0_L$.

Let R be a non degenerated ring, a be a non zero element of R, and b, c be elements of R. One can check that $\langle c, b, a\rangle$ is quadratic and $\langle c, b, 1_R\rangle$ is quadratic and monic.

Let R be an integral domain and a, x be non zero elements of R. Observe that $x \cdot \langle c, b, a\rangle$ is quadratic.

Let us consider a ring R and elements a, b, c, x of R. Now we state the propositions:

(19) $x \cdot \langle c, b, a\rangle = \langle x \cdot c, x \cdot b, x \cdot a\rangle$.

(20) $\mathrm{eval}(\langle c, b, a\rangle, x) = c + b \cdot x + a \cdot x^{\mathbf{2}}$.

(21) Let us consider a non degenerated ring R, and a polynomial p over R. Then p is quadratic if and only if there exists a non zero element a of R and there exist elements b, c of R such that $p = \langle c, b, a\rangle$.

(22) Let us consider a non degenerated ring R, and a monic polynomial p over R. Then p is quadratic if and only if there exist elements b, c of R such that $p = \langle c, b, 1_R\rangle$. The theorem is a consequence of (21).

(23) Let us consider a non degenerated ring R, a ring extension S of R, elements a_1, b_1, c_1 of R, and elements a_2, b_2, c_2 of S. Suppose $a_1 = a_2$ and $b_1 = b_2$ and $c_1 = c_2$. Then $\langle c_2, b_2, a_2 \rangle = \langle c_1, b_1, a_1 \rangle$.

Let R be a non degenerated ring and p be a polynomial over R. We say that p is purely quadratic if and only if

(Def. 6) there exists a non zero element a of R and there exists an element c of R such that $p = \langle c, 0_R, a \rangle$.

Let a be a non zero element of R and c be an element of R. Let us note that $\langle c, 0_R, a \rangle$ is purely quadratic and there exists a polynomial over R which is monic and purely quadratic and every polynomial over R which is purely quadratic is also quadratic.

Let R be a ring and a be an element of R. The functors: $\mathrm{X}^2\text{-}\, a$ and $\mathrm{X}^2 + a$ yielding elements of the carrier of PolyRing(R) are defined by terms

(Def. 7) $\langle -a, 0_R, 1_R \rangle$,

(Def. 8) $\langle a, 0_R, 1_R \rangle$,

respectively. Let R be a non degenerated ring. One can check that every polynomial over R which is linear is also non quadratic and every polynomial over R which is quadratic is also non linear.

Let a be an element of R. One can verify that $\mathrm{X}^2\text{-}\, a$ is purely quadratic, monic, and non constant and $\mathrm{X}^2 + a$ is purely quadratic, monic, and non constant.

Now we state the propositions:

(24) Let us consider a field F, and elements b_1, c_1, b_2, c_2 of F. Then $\langle c_1, b_1 \rangle * \langle c_2, b_2 \rangle = \langle c_1 \cdot c_2, b_1 \cdot c_2 + b_2 \cdot c_1, b_1 \cdot b_2 \rangle$. The theorem is a consequence of (1).

(25) Let us consider a field F with non characteristic 2, a non zero element a of F, elements b, c of F, and an element w of F. Suppose $w^{\mathbf{2}} = b^{\mathbf{2}} - (4 \star a) \cdot c$. Then

(i) $\mathrm{eval}(\langle c, b, a \rangle, (-b + w) \cdot (2 \star a)^{-1}) = 0_F$, and

(ii) $\mathrm{eval}(\langle c, b, a \rangle, (-b - w) \cdot (2 \star a)^{-1}) = 0_F$.

The theorem is a consequence of (5), (2), (4), and (20).

(26) Let us consider a field F, a non zero element a of F, and elements b, c of F. Suppose $\mathrm{Roots}(\langle c, b, a \rangle) \neq \emptyset$. Then $b^{\mathbf{2}} - (4 \star a) \cdot c$ is a square. The theorem is a consequence of (20), (4), and (2).

(27) Let us consider a field F with non characteristic 2, a non zero element a of F, elements b, c of F, and an element w of F. Suppose $w^{\mathbf{2}} = b^{\mathbf{2}} - (4 \star a) \cdot c$. Then $\mathrm{Roots}(\langle c, b, a \rangle) = \{(-b + w) \cdot (2 \star a)^{-1}, (-b - w) \cdot (2 \star a)^{-1}\}$. The theorem is a consequence of (5), (20), (4), (2), and (25).

(28) Let us consider a field F with non characteristic 2, a non zero element a of F, elements b, c of F, and an element w of F. Suppose $w^{\mathbf{2}} = b^{\mathbf{2}} - (4 \star a) \cdot c$. Let us consider elements r_1, r_2 of F. Suppose $r_1 = (-b + w) \cdot (2 \star a)^{-1}$ and $r_2 = (-b - w) \cdot (2 \star a)^{-1}$. Then $\langle c, b, a \rangle = a \cdot (\mathrm{X}\text{-}\, r_1 * \mathrm{X}\text{-}\, r_2)$.
PROOF: $\langle a \cdot r_1 \cdot r_2, a \cdot (-(r_1 + r_2)), a \cdot (1_F) \rangle = a \cdot (\mathrm{rpoly}(1, r_1) * \mathrm{rpoly}(1, r_2))$. $2 \star a \neq 0_F$ and $4 \star a \neq 0_F$ and $a \neq 0_F$. $a \cdot r_1 \cdot r_2 = c$ by [9, (5),(9)]. $a \cdot (-(r_1 + r_2)) = b$ by [10, (2)],(3). $\square$

Let R be a non degenerated ring and p be a quadratic polynomial over R. The functor Discriminant(p) yielding an element of R is defined by

(Def. 9) there exists a non zero element a of R and there exist elements b, c of R such that $p = \langle c, b, a \rangle$ and $it = b^{\mathbf{2}} - (4 \star a) \cdot c$.

We introduce the notation DC(p) as a synonym of Discriminant(p).

Let p be a monic, quadratic polynomial over R. Observe that the functor Discriminant(p) is defined by

(Def. 10) there exist elements b, c of R such that $p = \langle c, b, 1_R \rangle$ and $it = b^{\mathbf{2}} - 4 \star c$.

Let p be a monic, purely quadratic polynomial over R. One can check that the functor Discriminant(p) is defined by

(Def. 11) there exists an element c of R such that $p = \langle c, 0_R, 1_R \rangle$ and $it = -4 \star c$.

Let us consider a field F with non characteristic 2 and a quadratic polynomial p over F. Now we state the propositions:

(29) Roots$(p) \neq \emptyset$ if and only if DC(p) is a square. The theorem is a consequence of (21), (25), and (26).

(30) $\overline{\overline{\mathrm{Roots}(p)}} = 1$ if and only if DC$(p) = 0_F$. The theorem is a consequence of (21), (27), (5), and (29).

(31) $\overline{\overline{\mathrm{Roots}(p)}} = 2$ if and only if DC(p) is non zero and a square. The theorem is a consequence of (21), (5), (29), and (27).

(32) Let us consider a field F with non characteristic 2, and a quadratic element p of the carrier of PolyRing(F). Then p is reducible if and only if DC(p) is a square. The theorem is a consequence of (21), (28), and (19).

(33) Let us consider a field F with non characteristic 2, and an element a of F. Then $\mathrm{X}^2\text{-}\, a$ is reducible if and only if a is a square. The theorem is a consequence of (5), (6), and (32).

4. Quadratic Polynomials over $\mathbb{Z}/2$

Now we state the propositions:

(34) The carrier of $\mathbb{Z}/2 = \{0_{\mathbb{Z}/2}, 1_{\mathbb{Z}/2}\}$.

(35) $-1_{\mathbb{Z}/2} = 1_{\mathbb{Z}/2}$.

One can verify that $\mathbb{Z}/2$ is polynomial-disjoint and every element of $\mathbb{Z}/2$ is a square and every non zero polynomial over $\mathbb{Z}/2$ is monic and every non zero element of the carrier of PolyRing($\mathbb{Z}/2$) is monic.

The functors: X^2, X^2+1, $\mathrm{X}^2+\mathrm{X}$, and $\mathrm{X}^2+\mathrm{X}+1$ yielding quadratic elements of the carrier of PolyRing($\mathbb{Z}/2$) are defined by terms

(Def. 12) $\langle 0_{\mathbb{Z}/2}, 0_{\mathbb{Z}/2}, 1_{\mathbb{Z}/2}\rangle$,

(Def. 13) $\langle 1_{\mathbb{Z}/2}, 0_{\mathbb{Z}/2}, 1_{\mathbb{Z}/2}\rangle$,

(Def. 14) $\langle 0_{\mathbb{Z}/2}, 1_{\mathbb{Z}/2}, 1_{\mathbb{Z}/2}\rangle$,

(Def. 15) $\langle 1_{\mathbb{Z}/2}, 1_{\mathbb{Z}/2}, 1_{\mathbb{Z}/2}\rangle$,

respectively. The functors: X- and X-1 yielding linear elements of the carrier of PolyRing($\mathbb{Z}/2$) are defined by terms

(Def. 16) $\langle 0_{\mathbb{Z}/2}, 1_{\mathbb{Z}/2}\rangle$,

(Def. 17) $\langle 1_{\mathbb{Z}/2}, 1_{\mathbb{Z}/2}\rangle$,

respectively. Now we state the propositions:

(36) the set of all p where p is a quadratic polynomial over $\mathbb{Z}/2 = \{\mathrm{X}^2, \mathrm{X}^2+1, \mathrm{X}^2+\mathrm{X}, \mathrm{X}^2+\mathrm{X}+1\}$. The theorem is a consequence of (22) and (34).

(37) $\overline{\overline{\text{the set of all } p \text{ where } p \text{ is a quadratic polynomial over } \mathbb{Z}/2}} = 4$. The theorem is a consequence of (36).

(38) Let us consider a quadratic polynomial p over $\mathbb{Z}/2$. Then DC(p) is a square.

(39) (i) $\mathrm{X}^2 = \text{X-} * \text{X-}$, and

(ii) $\mathrm{Roots}(\mathrm{X}^2) = \{0_{\mathbb{Z}/2}\}$.

(40) (i) $\mathrm{X}^2+1 = \text{X-1} * \text{X-1}$, and

(ii) $\mathrm{Roots}(\mathrm{X}^2+1) = \{1_{\mathbb{Z}/2}\}$.

The theorem is a consequence of (35).

(41) (i) $\mathrm{X}^2+\mathrm{X} = \text{X-} * \text{X-1}$, and

(ii) $\mathrm{Roots}(\mathrm{X}^2+\mathrm{X}) = \{0_{\mathbb{Z}/2}, 1_{\mathbb{Z}/2}\}$.

The theorem is a consequence of (35).

(42) $\mathrm{Roots}(\mathrm{X}^2+\mathrm{X}+1) = \emptyset$. The theorem is a consequence of (34) and (20).

Let us note that X^2 is reducible and X^2+1 is reducible and $\mathrm{X}^2+\mathrm{X}$ is reducible and $\mathrm{X}^2+\mathrm{X}+1$ is irreducible. Now we state the propositions:

(43) $\mathbb{Z}/2$ is a splitting field of X^2.

(44) $\mathbb{Z}/2$ is a splitting field of $X^2 + 1$.

(45) $\mathbb{Z}/2$ is a splitting field of $X^2 + X$.

The functor α yielding an element of embField(canHomP($X^2 + X + 1$)) is defined by the term

(Def. 18) KrRootP($X^2 + X + 1$).

The functor $\alpha - 1$ yielding an element of embField(canHomP($X^2 + X + 1$)) is defined by the term

(Def. 19) $\alpha - 1_{\mathrm{embField(canHomP}(X^2+X+1))}$.

Let us observe that α is non zero and ($\mathbb{Z}/2$)-algebraic.

Now we state the propositions:

(46) (i) $-\alpha = \alpha$, and

(ii) $(\alpha)^{-1} = \alpha - 1$, and

(iii) $(\alpha)^{-1} \neq \alpha$.

(47) $X^2 + X + 1 = X\text{-}\,\alpha * X\text{-}(\alpha)^{-1} = X\text{-}\,\alpha * X\text{-}\,\alpha - 1$.

(48) Roots(FAdj($\mathbb{Z}/2, \{\alpha\}$), $X^2 + X + 1$) $= \{\alpha, \alpha - 1\}$. The theorem is a consequence of (46).

(49) $\overline{\overline{\mathrm{Roots}(\mathrm{FAdj}(\mathbb{Z}/2, \{\alpha\}), X^2 + X + 1)}} = 2$.

(50) MinPoly($\alpha, \mathbb{Z}/2$) $= X^2 + X + 1$.

(51) deg(FAdj($\mathbb{Z}/2, \{\alpha\}$), $\mathbb{Z}/2$) $= 2$. The theorem is a consequence of (50) and (18).

(52) FAdj($\mathbb{Z}/2, \{\alpha\}$) is a splitting field of $X^2 + X + 1$. The theorem is a consequence of (48).

5. Fields with Non Squares

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

(Def. 20) the carrier of $R \subseteq \mathrm{SQ}(R)$.

Let us observe that $-1_{\mathbb{R}_F}$ is non square and $-1_{\mathbb{F}_\mathbb{Q}}$ is non square and every non degenerated ring which is algebraic closed is also quadratic complete and every non degenerated ring which is preordered is also non quadratic complete and $\mathbb{F}_\mathbb{Q}$ is non quadratic complete and $\mathbb{R}_F$ is non quadratic complete and $\mathbb{C}_F$ is quadratic complete and there exists a field which is non quadratic complete, polynomial-disjoint, and strict and there exists a field which is quadratic complete and strict and every ring which is non quadratic complete is also non degenerated.

Let R be a non quadratic complete ring. One can check that there exists an element of R which is non square and there exists a field which is strict, polynomial-disjoint, and non quadratic complete and has not characteristic 2.

Let F be a non quadratic complete field without characteristic 2. Let us note that there exists an element of the carrier of PolyRing(F) which is monic, quadratic, and irreducible.

Let F be a field with non characteristic 2 and a be square element of F. One can verify that $\mathrm{X}^2\text{-}\,a$ is reducible.

Let F be a non quadratic complete field without characteristic 2 and a be a non square element of F. Note that $\mathrm{X}^2\text{-}\,a$ is irreducible.

Let F be a non quadratic complete, polynomial-disjoint field without characteristic 2. The functor $\sqrt{a}$ yielding an element of embField(canHomP($\mathrm{X}^2\text{-}\,a$)) is defined by the term

(Def. 21) KrRootP($\mathrm{X}^2\text{-}\,a$).

One can verify that $\sqrt{a}$ is non zero and F-algebraic and embField(canHomP ($\mathrm{X}^2\text{-}\,a$)) is (FAdj($F, \{\sqrt{a}\}$))-extending and $\sqrt{a}$ is (FAdj($F, \{\sqrt{a}\}$))-membered and non F-membered.

From now on F denotes a non quadratic complete, polynomial-disjoint field without characteristic 2.

Let us consider a non square element a of F. Now we state the propositions:

(53) $\sqrt{a} \cdot \sqrt{a} = a$. The theorem is a consequence of (20).

(54) $\mathrm{MinPoly}(\sqrt{a}, F) = \mathrm{X}^2\text{-}\,a$.

(55) $\deg(\mathrm{FAdj}(F, \{\sqrt{a}\}), F) = 2$.

(56) $\mathrm{X}\text{-}\,\sqrt{a} * \mathrm{X}\text{+}\,\sqrt{a} = \mathrm{X}^2\text{-}\,a$. The theorem is a consequence of (53).

(57) $\mathrm{Roots}(\mathrm{FAdj}(F, \{\sqrt{a}\}), \mathrm{X}^2\text{-}\,a) = \{\sqrt{a}, -\sqrt{a}\}$. The theorem is a consequence of (56).

(58) FAdj($F, \{\sqrt{a}\}$) is a splitting field of $\mathrm{X}^2\text{-}\,a$. The theorem is a consequence of (56) and (57).

(59) $\{1_F, \sqrt{a}\}$ is a basis of VecSp(FAdj($F, \{\sqrt{a}\}$), F).

(60) The carrier of FAdj($F, \{\sqrt{a}\}$) = the set of all $y + ({}^{@}\sqrt{a}) \cdot z$ where y, z are F-membered elements of FAdj($F, \{\sqrt{a}\}$).

(61) Let us consider a non square element a of F, and F-membered elements a_1, a_2, b_1, b_2 of FAdj($F, \{\sqrt{a}\}$). Suppose $a_1 + ({}^{@}\sqrt{a}) \cdot b_1 = a_2 + ({}^{@}\sqrt{a}) \cdot b_2$. Then

(i) $a_1 = a_2$, and

(ii) $b_1 = b_2$.

6. Splittingfields for Quadratic Polynomials

Let F be a field with non characteristic 2 and p be a quadratic element of the carrier of PolyRing(F). We say that p is DC-square if and only if

(Def. 22) DC(p) is a square.

Note that there exists a quadratic element of the carrier of PolyRing(F) which is monic and DC-square.

Let F be a non quadratic complete field without characteristic 2. One can check that there exists a quadratic element of the carrier of PolyRing(F) which is monic and non DC-square.

Let p be a non DC-square, quadratic element of the carrier of PolyRing(F). One can verify that DC(p) is non square and X^2- DC(p) is irreducible.

Let F be a field with non characteristic 2 and p be a DC-square, quadratic element of the carrier of PolyRing(F). One can verify that X^2- DC(p) is reducible.

Now we state the proposition:

(62) Let us consider a field F with non characteristic 2, and a quadratic element p of the carrier of PolyRing(F). Then F is a splitting field of p if and only if DC(p) is a square. The theorem is a consequence of (21), (28), and (26).

Let F be a non quadratic complete, polynomial-disjoint field without characteristic 2 and p be a non DC-square, quadratic element of the carrier of PolyRing(F). Observe that $\sqrt{\mathrm{DC}(p)}$ is non zero and F-algebraic.

The functor RootDC(p) yielding an element of $\mathrm{FAdj}(F, \{\sqrt{\mathrm{DC}(p)}\})$ is defined by the term

(Def. 23) $\sqrt{\mathrm{DC}(p)}$.

The functors: Root1(p) and Root2(p) yielding elements of $\mathrm{FAdj}(F, \{\sqrt{\mathrm{DC}(p)}\})$ are defined by terms

(Def. 24) $(-({}^{@}(p(1), \mathrm{FAdj}(F, \{\sqrt{\mathrm{DC}(p)}\}))) +$
$\mathrm{RootDC}(p)) \cdot (2 \star ({}^{@}(p(2), \mathrm{FAdj}(F, \{\sqrt{\mathrm{DC}(p)}\}))))^{-1}$,

(Def. 25) $(-({}^{@}(p(1), \mathrm{FAdj}(F, \{\sqrt{\mathrm{DC}(p)}\}))) -$
$\mathrm{RootDC}(p)) \cdot (2 \star ({}^{@}(p(2), \mathrm{FAdj}(F, \{\sqrt{\mathrm{DC}(p)}\}))))^{-1}$,

respectively. In the sequel p denotes a non DC-square, quadratic element of the carrier of PolyRing(F).

Now we state the propositions:

(63) $\mathrm{RootDC}(p) \cdot \mathrm{RootDC}(p) = \mathrm{DC}(p)$. The theorem is a consequence of (53).

(64) Let us consider a non zero element a of $\mathrm{FAdj}(F, \{\sqrt{\mathrm{DC}(p)}\})$, and elements b, c of $\mathrm{FAdj}(F, \{\sqrt{\mathrm{DC}(p)}\})$. Suppose $p = \langle c, b, a \rangle$. Then

(i) $\mathrm{Root1}(p) = (-b + \mathrm{RootDC}(p)) \cdot (2 \star a)^{-1}$, and

(ii) $\mathrm{Root2}(p) = (-b - \mathrm{RootDC}(p)) \cdot (2 \star a)^{-1}$.

(65) $p = ({}^{@}(\mathrm{LC}\,p, \mathrm{FAdj}(F, \{\sqrt{\mathrm{DC}(p)}\}))) \cdot (\mathrm{X}\text{-}\,\mathrm{Root1}(p) * \mathrm{X}\text{-}\,\mathrm{Root2}(p))$. The theorem is a consequence of (28), (21), (23), (64), (63), and (7).

(66) $\mathrm{Roots}(\mathrm{FAdj}(F, \{\sqrt{\mathrm{DC}(p)}\}), p) = \{\mathrm{Root1}(p), \mathrm{Root2}(p)\}$. The theorem is a consequence of (65).

(67) $\mathrm{Root1}(p) \neq \mathrm{Root2}(p)$. The theorem is a consequence of (21), (23), (5), and (64).

(68) $\deg(\mathrm{FAdj}(F, \{\sqrt{\mathrm{DC}(p)}\}), F) = 2$.

(69) $\mathrm{FAdj}(F, \{\sqrt{\mathrm{DC}(p)}\})$ is a splitting field of p. The theorem is a consequence of (65), (66), (21), (5), (23), (64), and (7).

7. Quadratic Extensions

Let F be a field and E be an extension of F. We say that E is F-quadratic if and only if

(Def. 26) $\deg(E, F) = 2$.

Let F be a non quadratic complete, polynomial-disjoint field without characteristic 2. Let us observe that there exists an extension of F which is F-quadratic.

Let F be a field. One can check that every extension of F which is F-quadratic is also F-finite.

Let F be a non quadratic complete, polynomial-disjoint field without characteristic 2 and a be a non square element of F. Let us observe that $\mathrm{FAdj}(F, \{\sqrt{a}\})$ is F-quadratic.

Now we state the propositions:

(70) Let us consider a field F, and elements a, b of F. If $b^{\mathbf{2}} = a$, then $\mathrm{eval}(\mathrm{X}^2\text{-}\,a, b) = 0_F$.

(71) Let us consider a field F with non characteristic 2, an extension E of F, and an element a of F. Suppose there exists no element b of F such that $a = b^{\mathbf{2}}$. Let us consider an element b of E. Suppose $b^{\mathbf{2}} = a$. Then

(i) $\mathrm{FAdj}(F, \{b\})$ is a splitting field of $\mathrm{X}^2\text{-}\,a$, and

(ii) $\deg(\mathrm{FAdj}(F, \{b\}), F) = 2$.

The theorem is a consequence of (9), (70), and (33).

(72) Let us consider a field F with non characteristic 2, and an extension E of F. Then $\deg(E, F) = 2$ if and only if there exists an element a of F such that there exists no element b of F such that $a = b^{\mathbf{2}}$ and there exists an element b of E such that $a = b^{\mathbf{2}}$ and $E \approx \mathrm{FAdj}(F, \{b\})$. The theorem is a consequence of (22), (23), (7), (26), (27), (5), (8), and (71).

(73) Let us consider an extension E of F. Then E is F-quadratic if and only if there exists a non square element a of F such that E and $\mathrm{FAdj}(F, \{\sqrt{a}\})$ are isomorphic over F. The theorem is a consequence of (22), (23), (7), (26), (27), (5), (8), (58), and (71).

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 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] Serge Lang. *Algebra.* Springer Verlag, 2002 (Revised Third Edition).

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

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

[8] Christoph Schwarzweller. Ring and field adjunctions, algebraic elements and minimal polynomials. *Formalized Mathematics*, 28(**3**):251–261, 2020. doi:10.2478/forma-2020-0022.

[9] Christoph Schwarzweller. Formally real fields. *Formalized Mathematics*, 25(**4**):249–259, 2017. doi:10.1515/forma-2017-0024.

[10] Christoph Schwarzweller. On roots of polynomials and algebraically closed fields. *Formalized Mathematics*, 25(**3**):185–195, 2017. doi:10.1515/forma-2017-0018.

[11] Christoph Schwarzweller and Artur Korniłowicz. Characteristic of rings. Prime fields. *Formalized Mathematics*, 23(**4**):333–349, 2015. doi:10.1515/forma-2015-0027.

[12] Steven H. Weintraub. *Galois Theory.* Springer-Verlag, 2 edition, 2009.

Accepted November 30, 2021