FORMALIZED MATHEMATICS
Vol. 30, No. 1, Pages 23–30, 2022
ISSN: 1426–2630, e-ISSN: 1898–9934
DOI: 10.2478/forma-2022-0003

sciendo.com/journal/forma

Splitting Fields for the Rational Polynomials X^2-2, X^2+X+1, X^3-1, and X^3-2

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Sara Burgoa
Weston, Florida
United States of America

Summary. In [11] the existence (and uniqueness) of splitting fields has been formalized. In this article we apply this result by providing splitting fields for the polynomials X^2-2, X^3-1, X^2+X+1 and X^3-2 over $\mathcal{Q}$ using the Mizar [2], [1] formalism. We also compute the degrees and bases for these splitting fields, which requires some additional registrations to adopt types properly.

The main result, however, is that the polynomial X^3-2 does not split over $\mathcal{Q}(\sqrt[3]{2})$. Because X^3-2 obviously has a root over $\mathcal{Q}(\sqrt[3]{2})$, this shows that the field extension $\mathcal{Q}(\sqrt[3]{2})$ is not normal over $\mathcal{Q}$ [3], [4], [5] and [7].

MSC: 12F05 68V20

Keywords: splitting fields; rational polynomials

MML identifier: FIELD_10, version: 8.1.12 5.71.1431

1. Preliminaries

Let L be a non empty double loop structure and a, b, c be elements of L. Note that the functor $\{a, b, c\}$ yields a subset of L. Let i be an integer. Let us observe that i^3 is integer.

Let i be an even integer. Let us observe that i^3 is even.

Let i be an odd integer. Let us observe that i^3 is odd.

Now we state the propositions:

(1) Let us consider complex numbers r, s. Then $(r \cdot s)^3 = r^3 \cdot s^3$.

(2) Let us consider a rational number r. Then $r^3 \geqslant 0$ if and only if $r \geqslant 0$.

(3) There exists no rational number r such that $r^3 = 2$. The theorem is a consequence of (2) and (1).

Note that $\mathrm{root}_3(2)$ is non rational. Now we state the proposition:

(4) Let us consider finite sets X_1, X_2. Suppose $X_1 \subseteq X_2$ and $\overline{\overline{X_1}} = \overline{\overline{X_2}}$. Then $X_1 = X_2$.

Let F be a field. Observe that there exists an element of the carrier of PolyRing(F) which is linear and there exists an element of the carrier of PolyRing (F) which is non linear and non constant.

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

(5) If $\deg(p) = 2$, then p is reducible iff p has roots.

(6) If $\deg(p) = 3$, then p is reducible iff p has roots.

2. More on Field Extensions

One can check that $\mathbb{C}_\mathrm{F}$ is $(\mathbb{F}_\mathbb{Q})$-extending and there exists an element of $\mathbb{R}_\mathrm{F}$ which is $(\mathbb{F}_\mathbb{Q})$-membered and there exists an element of $\mathbb{R}_\mathrm{F}$ which is non $(\mathbb{F}_\mathbb{Q})$-membered and there exists an element of $\mathbb{C}_\mathrm{F}$ which is $(\mathbb{R}_\mathrm{F})$-membered and there exists an element of $\mathbb{C}_\mathrm{F}$ which is non $(\mathbb{R}_\mathrm{F})$-membered and there exists an element of $\mathbb{C}_\mathrm{F}$ which is $(\mathbb{F}_\mathbb{Q})$-membered and there exists an element of $\mathbb{C}_\mathrm{F}$ which is non $(\mathbb{F}_\mathbb{Q})$-membered.

Now we state the propositions:

(7) Let us consider a field F, an extension E of F, an E-extending extension K of F, an element p of the carrier of PolyRing(F), and an element q of the carrier of PolyRing(E). If $p = q$, then $\mathrm{Roots}(K, p) = \mathrm{Roots}(K, q)$.

(8) Let us consider a field F, an extension E of F, an F-extending extension K of E, an element a of E, and an element b of K. Suppose $b = a$. Then $\mathrm{RAdj}(F, \{a\}) = \mathrm{RAdj}(F, \{b\})$.

(9) Let us consider a field F, an extension E of F, an F-extending extension K of E, an F-algebraic element a of E, and an F-algebraic element b of K. Suppose $b = a$. Then $\mathrm{FAdj}(F, \{a\}) = \mathrm{FAdj}(F, \{b\})$.

(10) Let us consider a field F, an extension E of F, an E-extending extension K of F, an F-algebraic element a of E, and an F-algebraic element b of K. If $a = b$, then $\mathrm{MinPoly}(a, F) = \mathrm{MinPoly}(b, F)$.

(11) Let us consider a field F, an F-finite extension E of F, and an element a of E. Then $\deg(\mathrm{MinPoly}(a, F)) \mid \deg(E, F)$.

Let F be a field, E be an extension of F, and T_1, T_2 be subsets of E. One can check that $\mathrm{FAdj}(F, T_1 \cup T_2)$ is $(\mathrm{FAdj}(F, T_1))$-extending and $(\mathrm{FAdj}(F, T_2))$-extending.

Let a, b be elements of E. Observe that $\mathrm{FAdj}(F, \{a, b\})$ is $(\mathrm{FAdj}(F, \{a\}))$-extending and $(\mathrm{FAdj}(F, \{b\}))$-extending. Let a, b, c be elements of E. Let us observe that $\mathrm{FAdj}(F, \{a, b, c\})$ is $(\mathrm{FAdj}(F, \{a, b\}))$-extending, $(\mathrm{FAdj}(F, \{a, c\}))$-extending, and $(\mathrm{FAdj}(F, \{b, c\}))$-extending.

3. The Rational Polynomials $X^2 - 2$, $X^3 - 1$, $X^2 + X + 1$ and $X^3 - 2$

The functors: $\mathrm{X}^2{-}2$, $\mathrm{X}^3{-}1$, $\mathrm{X}^3{-}2$, and $\mathrm{X}^2 + \mathrm{X} + 1$ yielding elements of the carrier of $\mathrm{PolyRing}(\mathbb{F}_{\mathbb{Q}})$ are defined by terms

(Def. 1) $\langle -(1_{\mathbb{F}_{\mathbb{Q}}} + 1_{\mathbb{F}_{\mathbb{Q}}}), 0_{\mathbb{F}_{\mathbb{Q}}}, 1_{\mathbb{F}_{\mathbb{Q}}} \rangle$,

(Def. 2) $(\mathbf{0}.\mathbb{F}_{\mathbb{Q}} +\cdot (0, -1)) +\cdot (3, 1)$,

(Def. 3) $(\mathbf{0}.\mathbb{F}_{\mathbb{Q}} +\cdot (0, -2)) +\cdot (3, 1)$,

(Def. 4) $\langle 1_{\mathbb{F}_{\mathbb{Q}}}, 1_{\mathbb{F}_{\mathbb{Q}}}, 1_{\mathbb{F}_{\mathbb{Q}}} \rangle$,

respectively. The functors: $\sqrt{2}$ and $\sqrt[3]{2}$ yielding non zero elements of $\mathbb{R}_{\mathrm{F}}$ are defined by terms

(Def. 5) $\sqrt{2}$,

(Def. 6) $\mathrm{root}_3(2)$,

respectively. The functors: $\sqrt{2}$, $\sqrt[3]{2}$, and $\sqrt{-3}$ yielding non zero elements of $\mathbb{C}_{\mathrm{F}}$ are defined by terms

(Def. 7) $\sqrt{2}$,

(Def. 8) $\mathrm{root}_3(2)$,

(Def. 9) $(i) \cdot \sqrt{3}$,

respectively. The functor ζ yielding a non zero element of $\mathbb{C}_{\mathrm{F}}$ is defined by the term

(Def. 10) $\frac{-1+(i)\cdot\sqrt{3}}{2}$.

Observe that $\mathrm{X}^2{-}2$ is monic, purely quadratic, and irreducible and $\mathrm{X}^3{-}2$ is monic, non constant, and irreducible and $\mathrm{X}^3{-}1$ is monic, non constant, and reducible and $\mathrm{X}^2 + \mathrm{X} + 1$ is monic, quadratic, and irreducible and $\sqrt{2}$ is non $(\mathbb{F}_{\mathbb{Q}})$-membered and $(\mathbb{F}_{\mathbb{Q}})$-algebraic and $\sqrt{2}$ is non $(\mathbb{F}_{\mathbb{Q}})$-membered and $(\mathbb{F}_{\mathbb{Q}})$-algebraic and $\sqrt[3]{2}$ is non $(\mathbb{F}_{\mathbb{Q}})$-membered and $(\mathbb{F}_{\mathbb{Q}})$-algebraic and $\sqrt[3]{2}$ is non $(\mathbb{F}_{\mathbb{Q}})$-membered and $(\mathbb{F}_{\mathbb{Q}})$-algebraic and ζ is non $(\mathbb{R}_{\mathrm{F}})$-membered and $(\mathbb{F}_{\mathbb{Q}})$-algebraic.

$(\zeta)^{\mathbf{2}}$ is non $(\mathbb{R}_{\mathrm{F}})$-membered and $(\mathbb{F}_{\mathbb{Q}})$-algebraic and $\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}\})$ is $(\mathbb{F}_{\mathbb{Q}})$-finite and $\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}, \zeta\})$ is $(\mathbb{F}_{\mathbb{Q}})$-finite and $\mathbb{R}_{\mathrm{F}}$ is $(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{2}\}))$-extending and $\mathbb{R}_{\mathrm{F}}$ is $(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}\}))$-extending and $\mathbb{C}_{\mathrm{F}}$ is $(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{2}\}))$-extending and $\mathbb{C}_{\mathrm{F}}$ is $(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}\}))$-extending and $\mathbb{C}_{\mathrm{F}}$ is $(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}, \zeta\}))$-extending.

Now we state the propositions:

(12) $\zeta = -\frac{1}{2} + (i) \cdot \frac{\sqrt{3}}{2}$.

(13) $(\zeta)^{\mathbf{2}} = -\frac{1}{2} - \frac{(i)\cdot\sqrt{3}}{2}$.

(14) (i) $\zeta^2 \neq 1$, and

(ii) $\zeta^3 = 1$, and

(iii) $\zeta^2 = -\zeta - 1$.

(15) (i) ζ is a complex root of 3, 1, and

(ii) $(\zeta)^{\mathbf{2}}$ is a complex root of 3, 1.

(16) $\sqrt[3]{2}^3 = 2$.

(17) $\mathrm{X}^3{-}1 = (\mathrm{X}{-}\, 1_{\mathbb{F}_\mathbb{Q}}) \cdot (\mathrm{X}^2 + \mathrm{X} + 1)$.

(18) (i) $\deg(\mathrm{X}^2{-}2) = 2$, and

(ii) $\deg(\mathrm{X}^3{-}2) = 3$, and

(iii) $\deg(\mathrm{X}^3{-}1) = 3$, and

(iv) $\deg(\mathrm{X}^2 + \mathrm{X} + 1) = 2$.

Let us consider an element x of $\mathbb{F}_\mathbb{Q}$. Now we state the propositions:

(19) $\mathrm{eval}(\mathrm{X}^2{-}2, x) = x^2 - 2$.

(20) $\mathrm{eval}(\mathrm{X}^3{-}1, x) = x^3 - 1$.

(21) $\mathrm{eval}(\mathrm{X}^2 + \mathrm{X} + 1, x) = x^2 + x + 1$.

(22) $\mathrm{eval}(\mathrm{X}^3{-}2, x) = x^3 - 2$.

(23) Let us consider an element r of $\mathbb{R}_\mathrm{F}$. Then $\mathrm{ExtEval}(\mathrm{X}^2{-}2, r) = r^2 - 2$.

Let us consider an element z of $\mathbb{C}_\mathrm{F}$. Now we state the propositions:

(24) $\mathrm{ExtEval}(\mathrm{X}^3{-}1, z) = z^3 - 1$.

(25) $\mathrm{ExtEval}(\mathrm{X}^2 + \mathrm{X} + 1, z) = z^2 + z + 1$.

(26) $\mathrm{ExtEval}(\mathrm{X}^3{-}2, z) = z^3 - 2$.

(27) Let us consider an element z of the carrier of $\mathbb{C}_\mathrm{F}$.
Then $\mathrm{ExtEval}(\mathrm{X}^3{-}1, z) = 0_{\mathbb{C}_\mathrm{F}}$ if and only if z is a complex root of 3, 1.

(28) $\mathrm{Discriminant}(\mathrm{X}^2 + \mathrm{X} + 1) = -3$.

(29) $\mathrm{FAdj}(\mathbb{F}_\mathbb{Q}, \{\zeta\}) = \mathrm{FAdj}(\mathbb{F}_\mathbb{Q}, \{\sqrt{-3}\})$.
PROOF: $\{\zeta\}$ is a subset of $\mathrm{FAdj}(\mathbb{F}_\mathbb{Q}, \{\sqrt{-3}\})$ by [10, (35)], [9, (12)], [6, (2)]. $\{\sqrt{-3}\}$ is a subset of $\mathrm{FAdj}(\mathbb{F}_\mathbb{Q}, \{\zeta\})$. □

4. A Splitting Field of $X^2 - 2$

Now we state the propositions:

(30) $\mathrm{MinPoly}(\sqrt{2}, \mathbb{F}_{\mathbb{Q}}) = \mathrm{X}^2{-}2$.

(31) $\deg(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{2}\}), \mathbb{F}_{\mathbb{Q}}) = 2$.

(32) $\{1, \sqrt{2}\}$ is a basis of $\mathrm{VecSp}(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{2}\}), \mathbb{F}_{\mathbb{Q}})$. The theorem is a consequence of (30).

(33) $\mathrm{Roots}(\mathrm{X}^2{-}2) = \emptyset$.

(34) $\mathrm{X}^2{-}2$ does not split in $\mathbb{F}_{\mathbb{Q}}$.

(35) $\mathrm{Roots}(\mathbb{R}_{\mathrm{F}}, \mathrm{X}^2{-}2) = \{\sqrt{2}, -\sqrt{2}\}$.

Proof: $\overline{\overline{\mathrm{Roots}(\mathbb{R}_{\mathrm{F}}, \mathrm{X}^2{-}2)}} = 2$ by [12, (22)], [13, (13)]. □

(36) $\mathrm{X}^2{-}2 = (\mathrm{X}{-}\sqrt{2}) \cdot (\mathrm{X}{+}\sqrt{2})$.

(37) $\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{2}\})$ is a splitting field of $\mathrm{X}^2{-}2$.

Proof: Set $F = \mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{2}\})$. $\mathrm{X}^2{-}2 = 1_{\mathbb{R}_{\mathrm{F}}} \cdot (\mathrm{rpoly}(1, \sqrt{2}) * \mathrm{rpoly}(1, -\sqrt{2}))$. $\{\sqrt{2}, -\sqrt{2}\} \subseteq$ the carrier of F. $\mathrm{X}^2{-}2$ splits in F. □

(38) $\sqrt[3]{2}$ is not an element of $\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{2}\})$. The theorem is a consequence of (10), (30), and (11).

(39) $\mathbb{R}_{\mathrm{F}}$ is not a splitting field of $\mathrm{X}^2{-}2$. The theorem is a consequence of (37) and (38).

(40) $\mathbb{C}_{\mathrm{F}}$ is not a splitting field of $\mathrm{X}^2{-}2$. The theorem is a consequence of (37) and (38).

5. A Splitting Field of $X^3 - 1$ and $X^2 + X + 1$

Now we state the propositions:

(41) $\mathrm{Roots}(\mathrm{X}^3{-}1) = \{1\}$.

(42) $\mathrm{Roots}(\mathrm{X}^2 + \mathrm{X} + 1) = \emptyset$.

(43) $\mathrm{MinPoly}(\zeta, \mathbb{F}_{\mathbb{Q}}) = \mathrm{X}^2 + \mathrm{X} + 1$.

(44) $\mathrm{Roots}(\mathbb{C}_{\mathrm{F}}, \mathrm{X}^3{-}1) = \{1, \zeta, (\zeta)^{\mathbf{2}}\}$.

(45) $\mathrm{Roots}(\mathbb{C}_{\mathrm{F}}, \mathrm{X}^2 + \mathrm{X} + 1) = \{\zeta, (\zeta)^{\mathbf{2}}\}$.

(46) $\mathrm{X}^3{-}1$ does not split in $\mathbb{F}_{\mathbb{Q}}$.

(47) $\mathrm{X}^3{-}1$ does not split in $\mathbb{R}_{\mathrm{F}}$.

(48) $\mathrm{X}^2 + \mathrm{X} + 1$ does not split in $\mathbb{F}_{\mathbb{Q}}$.

(49) $\mathrm{X}^2 + \mathrm{X} + 1$ does not split in $\mathbb{R}_{\mathrm{F}}$.

(50) $\mathrm{X}^2 + \mathrm{X} + 1 = (\mathrm{X}{-}\zeta) \cdot (\mathrm{X}{-}(\zeta)^{\mathbf{2}})$.

(51) $\mathrm{X}^3-1 = (\mathrm{X}- 1_{\mathbb{C}_\mathrm{F}}) \cdot (\mathrm{X}- \zeta) \cdot (\mathrm{X}-(\zeta)^{\mathbf{2}})$. The theorem is a consequence of (50).

(52) $\mathrm{FAdj}(\mathbb{F}_\mathbb{Q}, \{\zeta\})$ is a splitting field of $\mathrm{X}^2 + \mathrm{X} + 1$.
PROOF: Set $F = \mathrm{FAdj}(\mathbb{F}_\mathbb{Q}, \{\zeta\})$. $\mathrm{Roots}(\mathbb{C}_\mathrm{F}, \mathrm{X}^2 + \mathrm{X} + 1) \subseteq$ the carrier of F. □

(53) $\mathrm{FAdj}(\mathbb{F}_\mathbb{Q}, \{\zeta\})$ is a splitting field of X^3-1.
PROOF: Set $F = \mathrm{FAdj}(\mathbb{F}_\mathbb{Q}, \{\zeta\})$. $\mathrm{Roots}(\mathbb{C}_\mathrm{F}, \mathrm{X}^3-1) \subseteq$ the carrier of F. □

(54) $\deg(\mathrm{FAdj}(\mathbb{F}_\mathbb{Q}, \{\zeta\}), \mathbb{F}_\mathbb{Q}) = 2$.

(55) $\{1, \zeta\}$ is a basis of $\mathrm{VecSp}(\mathrm{FAdj}(\mathbb{F}_\mathbb{Q}, \{\zeta\}), \mathbb{F}_\mathbb{Q})$. The theorem is a consequence of (43).

(56) $\sqrt{2}$ is not an element of $\mathrm{FAdj}(\mathbb{F}_\mathbb{Q}, \{\zeta\})$. The theorem is a consequence of (55).

(57) $\mathbb{C}_\mathrm{F}$ is not a splitting field of $\mathrm{X}^2 + \mathrm{X} + 1$. The theorem is a consequence of (52) and (56).

(58) $\mathbb{C}_\mathrm{F}$ is not a splitting field of X^3-1. The theorem is a consequence of (53) and (56).

6. A Splitting Field of $X^3 - 2$

Now we state the propositions:

(59) $\mathrm{MinPoly}(\sqrt[3]{2}, \mathbb{F}_\mathbb{Q}) = \mathrm{X}^3-2$.

(60) $\deg(\mathrm{FAdj}(\mathbb{F}_\mathbb{Q}, \{\sqrt[3]{2}\}), \mathbb{F}_\mathbb{Q}) = 3$.

(61) $\{1, \sqrt[3]{2}, \sqrt[3]{2}^{\mathbf{2}}\}$ is a basis of $\mathrm{VecSp}(\mathrm{FAdj}(\mathbb{F}_\mathbb{Q}, \{\sqrt[3]{2}\}), \mathbb{F}_\mathbb{Q})$. The theorem is a consequence of (59).

(62) $\mathrm{Roots}(\mathrm{X}^3-2) = \emptyset$. The theorem is a consequence of (6).

(63) X^3-2 does not split in $\mathbb{F}_\mathbb{Q}$. The theorem is a consequence of (6).

(64) $\mathrm{Roots}(\mathrm{FAdj}(\mathbb{F}_\mathbb{Q}, \{\sqrt[3]{2}\}), \mathrm{X}^3-2) = \{\sqrt[3]{2}\}$.

(65) X^3-2 does not split in $\mathrm{FAdj}(\mathbb{F}_\mathbb{Q}, \{\sqrt[3]{2}\})$.

(66) $\mathrm{Roots}(\mathbb{R}_\mathrm{F}, \mathrm{X}^3-2) = \{\sqrt[3]{2}\}$.

(67) X^3-2 does not split in $\mathbb{R}_\mathrm{F}$.

(68) $\mathrm{Roots}(\mathbb{C}_\mathrm{F}, \mathrm{X}^3-2) = \{\sqrt[3]{2}, \sqrt[3]{2} \cdot \zeta, \sqrt[3]{2} \cdot (\zeta)^{\mathbf{2}}\}$.

(69) $\mathrm{X}^3-2 = (\mathrm{X}- \sqrt[3]{2}) \cdot (\mathrm{X}- \sqrt[3]{2} \cdot \zeta) \cdot (\mathrm{X}- \sqrt[3]{2} \cdot (\zeta)^{\mathbf{2}})$.
PROOF: Set $F = \mathbb{C}_\mathrm{F}$. Set $a = \sqrt[3]{2} \cdot \zeta$. Set $b = \sqrt[3]{2} \cdot (\zeta)^{\mathbf{2}}$. Set $c = \sqrt[3]{2}$. Reconsider $p_1 = \mathrm{X}- c$ as a polynomial over F. $p_1 * \langle a \cdot b, -b + -a, 1_F\rangle = \mathrm{X}^3-2$ by [8, (10)]. □

(70) $\mathrm{FAdj}(\mathbb{F}_\mathbb{Q}, \{\sqrt[3]{2}, \zeta\})$ is a splitting field of X^3-2.

Proof: Set $F = \mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}, \zeta\})$. $\mathrm{Roots}(\mathbb{C}_{\mathrm{F}}, \mathrm{X}^3{-}2) \subseteq$ the carrier of F. $\square$

Let us observe that $\mathbb{C}_{\mathrm{F}}$ is $(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}\}))$-extending and $\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}, \zeta\})$ is $(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}\}))$-extending and ζ is $(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}\}))$-algebraic.

Now we state the propositions:

(71) $\mathrm{MinPoly}(\zeta, \mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}\})) = \mathrm{X}^2 + \mathrm{X} + 1$. The theorem is a consequence of (9), (5), and (7).

(72) $\deg(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}, \zeta\}), \mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}\})) = 2$. The theorem is a consequence of (71).

(73) $\{1, \zeta\}$ is a basis of $\mathrm{VecSp}(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}, \zeta\}), \mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}\}))$. The theorem is a consequence of (71).

(74) $\deg(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}, \zeta\}), \mathbb{F}_{\mathbb{Q}}) = 6$. The theorem is a consequence of (59), (9), and (72).

(75) $\{1, \sqrt[3]{2}, \sqrt[3]{2}^{\mathbf{2}}, \zeta, \sqrt[3]{2}\cdot\zeta, \sqrt[3]{2}^{\mathbf{2}}\cdot\zeta\}$ is a basis of $\mathrm{VecSp}(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}, \zeta\}), \mathbb{F}_{\mathbb{Q}})$.
Proof: Set $F = \mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}, \zeta\})$. Set $K = \mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}\})$. $K = \mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}\})$. Set $M = \{1, \sqrt[3]{2}, \sqrt[3]{2}^{\mathbf{2}}, \zeta, \sqrt[3]{2}\cdot\zeta, \sqrt[3]{2}^{\mathbf{2}}\cdot\zeta\}$. Reconsider $B_1 = \{1, \sqrt[3]{2}, \sqrt[3]{2}^{\mathbf{2}}\}$ as a basis of $\mathrm{VecSp}(K, \mathbb{F}_{\mathbb{Q}})$. Reconsider $B_2 = \{1, \zeta\}$ as a basis of $\mathrm{VecSp}(F, K)$. $\mathrm{Base}(B_1, B_2) = M$. $\square$

One can verify that $\mathbb{C}_{\mathrm{F}}$ is $(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{2}\}))$-extending and $\mathbb{C}_{\mathrm{F}}$ is $(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{2}, \zeta\}))$-extending and $\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{2}, \zeta\})$ is $(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{2}\}))$-extending and $\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}, \zeta, \sqrt{2}\})$ is $(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{2}, \zeta\}))$-extending and ζ is $(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{2}\}))$-algebraic and $\sqrt[3]{2}$ is $(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{2}, \zeta\}))$-algebraic and $\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}, \zeta, \sqrt{2}\})$ is $(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{2}, \zeta\}))$-finite.

Now we state the propositions:

(76) $\mathrm{MinPoly}(\zeta, \mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{2}\})) = \mathrm{X}^2 + \mathrm{X} + 1$. The theorem is a consequence of (9), (5), and (7).

(77) $\deg(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{2}, \zeta\}), \mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{2}\})) = 2$. The theorem is a consequence of (76).

(78) $\deg(\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{2}, \zeta\}), \mathbb{F}_{\mathbb{Q}}) = 4$. The theorem is a consequence of (30), (10), and (77).

(79) $\sqrt{2}$ is not an element of $\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}, \zeta\})$. The theorem is a consequence of (78) and (74).

(80) $\mathbb{C}_{\mathrm{F}}$ is not a splitting field of $\mathrm{X}^3{-}2$. The theorem is a consequence of (70) and (79).

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

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

[6] Anna Justyna Milewska. The field of complex numbers. *Formalized Mathematics*, 9(**2**): 265–269, 2001.

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

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

[9] Christoph Schwarzweller. Renamings and a condition-free formalization of Kronecker's construction. *Formalized Mathematics*, 28(**2**):129–135, 2020. doi:10.2478/forma-2020-0012.

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

[11] Christoph Schwarzweller. Splitting fields. *Formalized Mathematics*, 29(**3**):129–139, 2021. doi:10.2478/forma-2021-0013.

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

[13] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzweller. Algebraic extensions. *Formalized Mathematics*, 29(**1**):39–48, 2021. doi:10.2478/forma-2021-0004.

Accepted April 30, 2022