

# Vieta's Formula about the Sum of Roots of Polynomials

Artur Kornilowicz  
Institute of Informatics  
University of Białystok  
Poland

Karol Pałk  
Institute of Informatics  
University of Białystok  
Poland

**Summary.** In the article we formalized in the Mizar system [2] the Vieta formula about the sum of roots of a polynomial  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  defined over an algebraically closed field. The formula says that  $x_1 + x_2 + \dots + x_{n-1} + x_n = -\frac{a_{n-1}}{a_n}$ . In the article the sum is denoted by **SumRoots**.

MSC: 03B35

Keywords:

MML identifier: POLYVIE1, version: 8.1.06 5.43.1297

Let  $F$  be a finite sequence and  $f$  be a function from  $\text{dom } F$  into  $\text{dom } F$ . Observe that  $F \cdot f$  is finite sequence-like.

Now we state the propositions:

(1) Let us consider objects  $a, b$ . Suppose  $a \neq b$ . Then

(i)  $\text{CFS}(\{a, b\}) = \langle a, b \rangle$ , or

(ii)  $\text{CFS}(\{a, b\}) = \langle b, a \rangle$ .

(2) Let us consider a finite set  $X$ . Then  $\text{CFS}(X)$  is an enumeration of  $X$ .

Let  $A$  be a set and  $X$  be a finite subset of  $A$ . Observe that  $\text{CFS}(X)$  is  $A$ -valued.

Now we state the proposition:

(3) Let us consider a right zeroed, non empty additive loop structure  $L$ , and an element  $a$  of  $L$ . Then  $2 \cdot a = a + a$ .

Let  $L$  be an almost left invertible multiplicative loop with zero structure. Let us note that every element of  $L$  which is non zero is also left invertible.

Let  $L$  be an almost right invertible multiplicative loop with zero structure. Observe that every element of  $L$  which is non zero is also right invertible.

Let  $L$  be an almost left cancelable multiplicative loop with zero structure. Let us observe that every element of  $L$  which is non zero is also left mult-cancelable.

Let  $L$  be an almost right cancelable multiplicative loop with zero structure. One can verify that every element of  $L$  which is non zero is also right mult-cancelable.

Now we state the proposition:

- (4) Let us consider a right unital, associative, non trivial double loop structure  $L$ , and elements  $a, b$  of  $L$ . Suppose  $b$  is left invertible and right mult-cancelable and  $b \cdot \frac{1}{b} = \frac{1}{b} \cdot b$ . Then  $\frac{a \cdot b}{b} = a$ .

Let  $L$  be a non degenerated zero-one structure,  $z_0$  be an element of  $L$ , and  $z_1$  be a non zero element of  $L$ . Note that  $\langle z_0, z_1 \rangle$  is non-zero and  $\langle z_1, z_0 \rangle$  is non-zero.

Let us consider a non trivial zero structure  $L$  and a polynomial  $p$  over  $L$ . Now we state the propositions:

- (5) If  $\text{len } p = 1$ , then there exists a non zero element  $a$  of  $L$  such that  $p = \langle a \rangle$ .  
 (6) If  $\text{len } p = 2$ , then there exists an element  $a$  of  $L$  and there exists a non zero element  $b$  of  $L$  such that  $p = \langle a, b \rangle$ .  
 (7) If  $\text{len } p = 3$ , then there exist elements  $a, b$  of  $L$  and there exists a non zero element  $c$  of  $L$  such that  $p = \langle a, b, c \rangle$ .

Now we state the propositions:

- (8) Let us consider an add-associative, right zeroed, right complementable, associative, commutative, left distributive, well unital, almost left invertible, non empty double loop structure  $L$ , and elements  $a, b, x$  of  $L$ . If  $b \neq 0_L$ , then  $\text{eval}(\langle a, b \rangle, -\frac{a}{b}) = 0_L$ .  
 (9) Let us consider a field  $L$ , elements  $a, x$  of  $L$ , and a non zero element  $b$  of  $L$ . Then  $x$  is a root of  $\langle a, b \rangle$  if and only if  $x = -\frac{a}{b}$ . The theorem is a consequence of (4) and (8).

Let us consider a field  $L$ , an element  $a$  of  $L$ , and a non zero element  $b$  of  $L$ . Now we state the propositions:

- (10)  $\text{Roots}(\langle a, b \rangle) = \{-\frac{a}{b}\}$ . The theorem is a consequence of (9).  
 (11)  $\text{multiplicity}(\langle a, b \rangle, -\frac{a}{b}) = 1$ . The theorem is a consequence of (9).  
 (12)  $\text{BRoots}(\langle a, b \rangle) = (\{-\frac{a}{b}\}, 1)$ -bag. The theorem is a consequence of (10) and (11).

Now we state the propositions:

- (13) Let us consider a field  $L$ , elements  $a, c$  of  $L$ , and non zero elements  $b, d$  of  $L$ . Then  $\text{Roots}(\langle a, b \rangle * \langle c, d \rangle) = \{-\frac{a}{b}, -\frac{c}{d}\}$ . The theorem is a consequence of (10).

- (14) Let us consider a field  $L$ , elements  $a, x$  of  $L$ , and a non zero element  $b$  of  $L$ . If  $x \neq -\frac{a}{b}$ , then  $\text{multiplicity}(\langle a, b \rangle, x) = 0$ . The theorem is a consequence of (10).

Let us consider a field  $L$ , a non-zero polynomial  $p$  over  $L$ , an element  $a$  of  $L$ , and a non zero element  $b$  of  $L$ . Now we state the propositions:

- (15) Suppose  $-\frac{a}{b} \notin \text{Roots}(p)$ . Then  $\overline{\overline{\text{Roots}(\langle a, b \rangle * p)}} = 1 + \overline{\overline{\text{Roots}(p)}}$ . The theorem is a consequence of (10).
- (16) Suppose  $-\frac{a}{b} \notin \text{Roots}(p)$ . Then  $\text{CFS}(\text{Roots}(p)) \wedge \langle -\frac{a}{b} \rangle$  is an enumeration of  $\text{Roots}(\langle a, b \rangle * p)$ . The theorem is a consequence of (10).

Now we state the proposition:

- (17) Let us consider a field  $L$ , a non-zero polynomial  $p$  over  $L$ , an element  $a$  of  $L$ , a non zero element  $b$  of  $L$ , and an enumeration  $E$  of  $\text{Roots}(\langle a, b \rangle * p)$ . Suppose  $E = \text{CFS}(\text{Roots}(p)) \wedge \langle -\frac{a}{b} \rangle$ . Then
- (i)  $\text{len } E = 1 + \overline{\overline{\text{Roots}(p)}}$ , and
  - (ii)  $E(1 + \overline{\overline{\text{Roots}(p)}}) = -\frac{a}{b}$ , and
  - (iii) for every natural number  $n$  such that  $1 \leq n \leq \overline{\overline{\text{Roots}(p)}}$  holds  $E(n) = (\text{CFS}(\text{Roots}(p)))(n)$ .

Let  $L$  be a non empty double loop structure,  $B$  be a bag of the carrier of  $L$ , and  $E$  be a (the carrier of  $L$ )-valued finite sequence. The functor  $B(++)E$  yielding a finite sequence of elements of  $L$  is defined by

- (Def. 1)  $\text{len } it = \text{len } E$  and for every natural number  $n$  such that  $1 \leq n \leq \text{len } it$  holds  $it(n) = (B \cdot E)(n) \cdot E_n$ .

Now we state the propositions:

- (18) Let us consider an integral domain  $L$ , a non-zero polynomial  $p$  over  $L$ , a bag  $B$  of the carrier of  $L$ , and an enumeration  $E$  of  $\text{Roots}(p)$ . If  $\text{Roots}(p) = \emptyset$ , then  $B(++)E = \emptyset$ .
- (19) Let us consider a left zeroed, add-associative, non empty double loop structure  $L$ , bags  $B_1, B_2$  of the carrier of  $L$ , and a (the carrier of  $L$ )-valued finite sequence  $E$ . Then  $B_1 + B_2(++)E = (B_1(++)E) + (B_2(++)E)$ .
- (20) Let us consider a left zeroed, add-associative, non empty double loop structure  $L$ , a bag  $B$  of the carrier of  $L$ , and (the carrier of  $L$ )-valued finite sequences  $E, F$ . Then  $B(++)E \wedge F = (B(++)E) \wedge (B(++)F)$ .
- (21) Let us consider a left zeroed, add-associative, non empty double loop structure  $L$ , bags  $B_1, B_2$  of the carrier of  $L$ , and (the carrier of  $L$ )-valued finite sequences  $E, F$ . Then  $B_1 + B_2(++)E \wedge F = (B_1(++)E) \wedge (B_1(++)F) + (B_2(++)E) \wedge (B_2(++)F)$ . The theorem is a consequence of (19) and (20).

(22) Let us consider a field  $L$ , a non-zero polynomial  $p$  over  $L$ , an element  $a$  of  $L$ , a non zero element  $b$  of  $L$ , an enumeration  $E$  of  $\text{Roots}(\langle a, b \rangle * p)$ , and a permutation  $P$  of  $\text{dom } E$ . Then  $(\text{BRoots}(\langle a, b \rangle * p)(++)E) \cdot P = \text{BRoots}(\langle a, b \rangle * p)(++)E \cdot P$ .

PROOF: Set  $q = \langle a, b \rangle$ . Set  $B = \text{BRoots}(q * p)$ . Reconsider  $P_1 = P$  as a permutation of  $\text{dom}(B(++)E)$ .  $(B(++)E) \cdot P_1 = B(++)E \cdot P$  by [12, (27)], [11, (29), (25)], [4, (13)].  $\square$

Let us consider a field  $L$ , a non-zero polynomial  $p$  over  $L$ , an element  $a$  of  $L$ , a non zero element  $b$  of  $L$ , and an enumeration  $E$  of  $\text{Roots}(\langle a, b \rangle * p)$ . Now we state the propositions:

(23) Suppose  $-\frac{a}{b} \notin \text{Roots}(p)$ . Then suppose  $E = \text{CFS}(\text{Roots}(p)) \wedge \langle -\frac{a}{b} \rangle$ . Then  $(\text{CFS}(\text{Roots}(\langle a, b \rangle * p)))^{-1} \cdot E$  is a permutation of  $\text{dom } E$ . The theorem is a consequence of (15) and (10).

(24) Suppose  $-\frac{a}{b} \notin \text{Roots}(p)$ . Then suppose  $E = \text{CFS}(\text{Roots}(p)) \wedge \langle -\frac{a}{b} \rangle$ . Then  $\sum(\text{BRoots}(\langle a, b \rangle * p)(++)E) = \sum(\text{BRoots}(\langle a, b \rangle * p)(++) \text{CFS}(\text{Roots}(\langle a, b \rangle * p)))$ .

PROOF: Set  $q = \langle a, b \rangle$ . Set  $B = \text{BRoots}(q * p)$ . Set  $D = \text{CFS}(\text{Roots}(q * p))$ . Reconsider  $P = D^{-1} \cdot E$  as a permutation of  $\text{dom } E$ .  $E \cdot E^{-1} \cdot D = D$  by [4, (37)], [12, (27)], [4, (35), (12)].  $(B(++)E) \cdot P^{-1} = B(++)E \cdot P^{-1}$ .  $\square$

(25)  $\sum(\text{BRoots}(\langle a, b \rangle)(++)E) = -\frac{a}{b}$ . The theorem is a consequence of (10), (11), and (14).

Let  $L$  be an integral domain and  $p$  be a non-zero polynomial over  $L$ . The functor  $\text{SumRoots}(p)$  yielding an element of  $L$  is defined by the term

(Def. 2)  $\sum(\text{BRoots}(p)(++) \text{CFS}(\text{Roots}(p)))$ .

Now we state the propositions:

(26) Let us consider an integral domain  $L$ , and a non-zero polynomial  $p$  over  $L$ . If  $\text{Roots}(p) = \emptyset$ , then  $\text{SumRoots}(p) = 0_L$ . The theorem is a consequence of (2) and (18).

(27) Let us consider a field  $L$ , an element  $a$  of  $L$ , and a non zero element  $b$  of  $L$ . Then  $\text{SumRoots}(\langle a, b \rangle) = -\frac{a}{b}$ . The theorem is a consequence of (10), (2), and (11).

(28) Let us consider a field  $L$ , a non-zero polynomial  $p$  over  $L$ , an element  $a$  of  $L$ , and a non zero element  $b$  of  $L$ . Then  $\text{SumRoots}(\langle a, b \rangle * p) = -\frac{a}{b} + \text{SumRoots}(p)$ . The theorem is a consequence of (16), (17), (24), (2), (10), (11), (25), and (19).

(29) Let us consider a field  $L$ , elements  $a, c$  of  $L$ , and non zero elements  $b, d$  of  $L$ . Then  $\text{SumRoots}(\langle a, b \rangle * \langle c, d \rangle) = -\frac{a}{b} + -\frac{c}{d}$ . The theorem is a consequence of (27) and (28).

- (30) Let us consider an algebraic closed field  $L$ , and non-zero polynomials  $p, q$  over  $L$ . Suppose  $\text{len } p \geq 2$ . Then  $\text{SumRoots}(p * q) = \text{SumRoots}(p) + \text{SumRoots}(q)$ .

PROOF: Define  $\mathcal{P}[\text{natural number}] \equiv$  for every non-zero polynomial  $f$  over  $L$  such that  $\$1 = \text{len } f$  holds  $\text{SumRoots}(f * q) = \text{SumRoots}(f) + \text{SumRoots}(q)$ .  $\mathcal{P}[2]$ . For every non trivial natural number  $k$  such that  $\mathcal{P}[k]$  holds  $\mathcal{P}[k + 1]$  by [6, (29)], [1, (11)], [8, (17), (50)]. For every non trivial natural number  $k$ ,  $\mathcal{P}[k]$  from [6, Sch. 2].  $\square$

- (31) Let us consider an algebraic closed integral domain  $L$ , a non-zero polynomial  $p$  over  $L$ , and a finite sequence  $r$  of elements of  $L$ . Suppose  $r$  is one-to-one and  $\text{len } r = \text{len } p - 1$  and  $\text{Roots}(p) = \text{rng } r$ . Then  $\sum r = \text{SumRoots}(p)$ .

PROOF: Set  $B = \text{BRoots}(p)$ . Set  $s = \text{support } B$ . Set  $L_1 = \text{len } r \mapsto 1$ . Consider  $f$  being a finite sequence of elements of  $\mathbb{N}$  such that  $\text{degree}(B) = \sum f$  and  $f = B \cdot \text{CFS}(s)$ . Reconsider  $E = \text{CFS}(s)$  as a finite sequence of elements of  $L$ . For every natural number  $j$  such that  $j \in \text{Seg len } r$  holds  $f(j) \geq L_1(j)$  by [8, (52)], [4, (12)], [3, (57)]. For every natural number  $j$  such that  $1 \leq j \leq \text{len } E$  holds  $(B(++)E)(j) = E(j)$  by [5, (83)], [3, (57)], [9, (13)].  $\square$

Now we state the proposition:

- (32) VIETA'S FORMULA ABOUT THE SUM OF ROOTS:

Let us consider an algebraic closed field  $L$ , and a non-zero polynomial  $p$  over  $L$ . Suppose  $\text{len } p \geq 2$ . Then  $\text{SumRoots}(p) = -\frac{p(\text{len } p - 2)}{p(\text{len } p - 1)}$ .

PROOF: Define  $\mathcal{P}[\text{natural number}] \equiv$  for every non-zero polynomial  $p$  over  $L$  such that  $\$1 = \text{len } p$  holds  $\text{SumRoots}(p) = -\frac{p(\$1 - 2)}{p(\$1 - 1)}$ .  $\mathcal{P}[2]$  by (6), [7, (38)], (27). For every non trivial natural number  $k$  such that  $\mathcal{P}[k]$  holds  $\mathcal{P}[k + 1]$  by [6, (29)], [1, (11)], [8, (17)], [10, (5)]. For every non trivial natural number  $k$ ,  $\mathcal{P}[k]$  from [6, Sch. 2].  $\square$

## REFERENCES

- [1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(1):41–46, 1990.
- [2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Kornilowicz, 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.
- [3] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(3):529–536, 1990.
- [4] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(1):55–65, 1990.
- [5] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(4):661–668, 1990.

- [6] Robert Milewski. Natural numbers. *Formalized Mathematics*, 7(1):19–22, 1998.
- [7] Robert Milewski. Fundamental theorem of algebra. *Formalized Mathematics*, 9(3):461–470, 2001.
- [8] Piotr Rudnicki. Little Bezout theorem (factor theorem). *Formalized Mathematics*, 12(1):49–58, 2004.
- [9] Christoph Schwarzweller. The binomial theorem for algebraic structures. *Formalized Mathematics*, 9(3):559–564, 2001.
- [10] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(3):501–505, 1990.
- [11] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(3):569–573, 1990.
- [12] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(1):73–83, 1990.

*Received May 25, 2017*

---



The English version of this volume of Formalized Mathematics financed under agreement 548/P-DUN/2016 from the funds of the Polish Minister of Science and Higher Education for the dissemination of science.