FORMALIZED MATHEMATICS
Volume 12, Number 1, 2004
University of Białystok

Witt's Proof of the Wedderburn Theorem[1]

Broderick Arneson
University of Alberta
Edmonton

Matthias Baaz
Technische Universität Wien

Piotr Rudnicki
University of Alberta
Edmonton

Summary. We present a formalization of Witt's proof of the Wedderburn theorem following Chapter 5 of *Proofs from THE BOOK* by Martin Aigner and Günter M. Ziegler, 2nd ed., Springer 1999.

MML Identifier: `WEDDWITT`.

The notation and terminology used in this paper have been introduced in the following articles: [23], [31], [20], [8], [12], [24], [3], [29], [14], [32], [6], [7], [4], [5], [27], [16], [9], [15], [2], [28], [18], [10], [26], [13], [1], [17], [25], [30], [33], [19], [22], [21], and [11].

1. Preliminaries

The following propositions are true:

(1) For every natural number a and for every real number q such that $1 < q$ and $q^a = 1$ holds $a = 0$.

(2) For all natural numbers a, k, r and for every real number x such that $1 < x$ and $0 < k$ holds $x^{a \cdot k + r} = x^a \cdot x^{a \cdot (k -' 1) + r}$.

(3) For all natural numbers q, a, b such that $0 < a$ and $1 < q$ and $q^a -' 1 \mid q^b -' 1$ holds $a \mid b$.

(4) For all natural numbers n, q such that $0 < q$ holds $\overline{\overline{q^n}} = q^n$.

[1]This work has been supported by NSERC Grant OGP9207.

ISSN 1426–2630

(5) Let f be a finite sequence of elements of $\mathbb{N}$ and i be a natural number. If for every natural number j such that $j \in \operatorname{dom} f$ holds $i \mid f_j$, then $i \mid \sum f$.

(6) Let X be a finite set, Y be a partition of X, and f be a finite sequence of elements of Y. Suppose f is one-to-one and $\operatorname{rng} f = Y$. Let c be a finite sequence of elements of $\mathbb{N}$. Suppose $\operatorname{len} c = \operatorname{len} f$ and for every natural number i such that $i \in \operatorname{dom} c$ holds $c(i) = \overline{\overline{f(i)}}$. Then $\operatorname{card} X = \sum c$.

2. Class Formula for Groups

Let us observe that there exists a group which is finite.

Let G be a finite group. Observe that $\mathrm{Z}(G)$ is finite.

Let G be a group and let a be an element of G. The functor $\mathrm{Centralizer}(a)$ yields a strict subgroup of G and is defined by:

(Def. 1) The carrier of $\mathrm{Centralizer}(a) = \{b; b$ ranges over elements of G: $a \cdot b = b \cdot a\}$.

Let G be a finite group and let a be an element of G. Observe that $\mathrm{Centralizer}(a)$ is finite.

Next we state two propositions:

(7) For every group G and for every element a of G and for every set x such that $x \in \mathrm{Centralizer}(a)$ holds $x \in G$.

(8) For every group G and for all elements a, x of G holds $a \cdot x = x \cdot a$ iff x is an element of $\mathrm{Centralizer}(a)$.

Let G be a group and let a be an element of G. One can verify that $a^{\bullet}$ is non empty.

Let G be a group and let a be an element of G. The functor a-con_map yields a function from the carrier of G into $a^{\bullet}$ and is defined by:

(Def. 2) For every element x of G holds $(a\text{-con\_map})(x) = a^x$.

One can prove the following propositions:

(9) For every finite group G and for every element a of G and for every element x of $a^{\bullet}$ holds $\operatorname{card}((a\text{-con\_map})^{-1}(\{x\})) = \operatorname{ord}(\mathrm{Centralizer}(a))$.

(10) Let G be a group, a be an element of G, and x, y be elements of $a^{\bullet}$. If $x \neq y$, then $(a\text{-con\_map})^{-1}(\{x\})$ misses $(a\text{-con\_map})^{-1}(\{y\})$.

(11) Let G be a group and a be an element of G. Then $\{(a\text{-con\_map})^{-1}(\{x\}) :$ x ranges over elements of $a^{\bullet}\}$ is a partition of the carrier of G.

(12) For every finite group G and for every element a of G holds $\overline{\overline{\{(a\text{-con\_map})^{-1}(\{x\}) : x \text{ ranges over elements of } a^{\bullet}\}}} = \operatorname{card} a^{\bullet}$.

(13) For every finite group G and for every element a of G holds $\operatorname{ord}(G) = \operatorname{card} a^{\bullet} \cdot \operatorname{ord}(\mathrm{Centralizer}(a))$.

Let G be a group. The functor conjugate_Classes(G) yielding a partition of the carrier of G is defined by:

(Def. 3) conjugate_Classes$(G) = \{S; S$ ranges over subsets of G: $\bigvee_{a\,:\,\text{element of } G} S = a^{\bullet}\}$.

The following two propositions are true:

(14) For every group G and for every set x holds $x \in$ conjugate_Classes(G) iff there exists an element a of G such that $a^{\bullet} = x$.

(15) Let G be a finite group and f be a finite sequence of elements of conjugate_Classes(G). Suppose f is one-to-one and $\operatorname{rng} f =$ conjugate_Classes(G). Let c be a finite sequence of elements of $\mathbb{N}$. Suppose $\operatorname{len} c = \operatorname{len} f$ and for every natural number i such that $i \in \operatorname{dom} c$ holds $c(i) = \overline{\overline{f(i)}}$. Then $\operatorname{ord}(G) = \sum c$.

3. Centers and Centralizers of Skew Fields

We now state the proposition

(16) Let F be a finite field, V be a vector space over F, and n, q be natural numbers. Suppose V is finite dimensional and $n = \dim(V)$ and $q = \overline{\overline{\text{the carrier of } F}}$. Then $\overline{\overline{\text{the carrier of } V}} = q^{n}$.

Let R be a skew field. The functor $\mathrm{Z}(R)$ yielding a strict field is defined by the conditions (Def. 4).

(Def. 4)(i) The carrier of $\mathrm{Z}(R) = \{x; x$ ranges over elements of R: $\bigwedge_{s\,:\,\text{element of } R} x \cdot s = s \cdot x\}$,

(ii) the addition of $\mathrm{Z}(R) =$ (the addition of R)$\restriction[\!:$ the carrier of $\mathrm{Z}(R)$, the carrier of $\mathrm{Z}(R)\,:\!]$,

(iii) the multiplication of $\mathrm{Z}(R) =$ (the multiplication of R)$\restriction[\!:$ the carrier of $\mathrm{Z}(R)$, the carrier of $\mathrm{Z}(R)\,:\!]$,

(iv) the zero of $\mathrm{Z}(R) =$ the zero of R, and

(v) the unity of $\mathrm{Z}(R) =$ the unity of R.

The following proposition is true

(17) For every skew field R holds the carrier of $\mathrm{Z}(R) \subseteq$ the carrier of R.

Let R be a finite skew field. Note that $\mathrm{Z}(R)$ is finite.

We now state several propositions:

(18) Let R be a skew field and y be an element of R. Then $y \in \mathrm{Z}(R)$ if and only if for every element s of R holds $y \cdot s = s \cdot y$.

(19) For every skew field R holds $0_R \in \mathrm{Z}(R)$.

(20) For every skew field R holds $\mathbf{1}_R \in \mathrm{Z}(R)$.

(21) For every finite skew field R holds $1 < \operatorname{card}$ (the carrier of $\mathrm{Z}(R)$).

(22) For every finite skew field R holds card (the carrier of $\mathrm{Z}(R)$) = card (the carrier of R) iff R is commutative.

(23) For every skew field R holds the carrier of $\mathrm{Z}(R)$ = (the carrier of $\mathrm{Z}(\mathrm{MultGroup}(R))) \cup \{0_R\}$.

Let R be a skew field and let s be an element of R. The functor centralizer(s) yields a strict skew field and is defined by the conditions (Def. 5).

(Def. 5)(i) The carrier of centralizer(s) = $\{x; x$ ranges over elements of R: $x \cdot s = s \cdot x\}$,

(ii) the addition of centralizer(s) = (the addition of R)$\restriction$[: the carrier of centralizer(s), the carrier of centralizer(s) :],

(iii) the multiplication of centralizer(s) = (the multiplication of R)$\restriction$[: the carrier of centralizer(s), the carrier of centralizer(s) :],

(iv) the zero of centralizer(s) = the zero of R, and

(v) the unity of centralizer(s) = the unity of R.

Next we state several propositions:

(24) For every skew field R and for every element s of R holds the carrier of centralizer(s) $\subseteq$ the carrier of R.

(25) For every skew field R and for all elements s, a of R holds $a \in$ the carrier of centralizer(s) iff $a \cdot s = s \cdot a$.

(26) For every skew field R and for every element s of R holds the carrier of $\mathrm{Z}(R) \subseteq$ the carrier of centralizer(s).

(27) Let R be a skew field and s, a, b be elements of R. Suppose $a \in$ the carrier of $\mathrm{Z}(R)$ and $b \in$ the carrier of centralizer(s). Then $a \cdot b \in$ the carrier of centralizer(s).

(28) For every skew field R and for every element s of R holds 0_R is an element of centralizer(s) and $\mathbf{1}_R$ is an element of centralizer(s).

Let R be a finite skew field and let s be an element of R. Observe that centralizer(s) is finite.

Next we state three propositions:

(29) For every finite skew field R and for every element s of R holds $1 <$ card (the carrier of centralizer(s)).

(30) Let R be a skew field, s be an element of R, and t be an element of MultGroup(R). If $t = s$, then the carrier of centralizer(s) = (the carrier of Centralizer(t)) $\cup \{0_R\}$.

(31) Let R be a finite skew field, s be an element of R, and t be an element of MultGroup(R). If $t = s$, then ord(Centralizer(t)) = card (the carrier of centralizer(s)) $- 1$.

4. Vector Spaces over Centers of Skew Fields

Let R be a skew field. The functor VectSp_over Z(R) yielding a strict vector space over Z(R) is defined by the conditions (Def. 6).

(Def. 6)(i) The loop structure of VectSp_over Z(R) = the loop structure of R, and

(ii) the left multiplication of VectSp_over Z(R) = (the multiplication of R)$\restriction$[: the carrier of Z(R), the carrier of R :].

We now state two propositions:

(32) For every finite skew field R holds card (the carrier of R) = (card (the carrier of Z(R)))$^{\dim(\text{VectSp\_over Z}(R))}$.

(33) For every finite skew field R holds $0 < \dim(\text{VectSp\_over Z}(R))$.

Let R be a skew field and let s be an element of R. The functor VectSp_over Z(s) yields a strict vector space over Z(R) and is defined by the conditions (Def. 7).

(Def. 7)(i) The loop structure of VectSp_over Z(s) = the loop structure of centralizer(s), and

(ii) the left multiplication of VectSp_over Z(s) = (the multiplication of R)$\restriction$[: the carrier of Z(R), the carrier of centralizer(s) :].

The following propositions are true:

(34) For every finite skew field R and for every element s of R holds card (the carrier of centralizer(s)) = (card (the carrier of Z(R)))$^{\dim(\text{VectSp\_over Z}(s))}$.

(35) For every finite skew field R and for every element s of R holds $0 < \dim(\text{VectSp\_over Z}(s))$.

(36) Let R be a finite skew field and r be an element of R. Suppose r is an element of MultGroup(R).
Then (card (the carrier of Z(R)))$^{\dim(\text{VectSp\_over Z}(r))} - 1 \mid$ (card (the carrier of Z(R)))$^{\dim(\text{VectSp\_over Z}(R))} - 1$.

(37) For every finite skew field R and for every element s of R such that s is an element of MultGroup(R) holds $\dim(\text{VectSp\_over Z}(s)) \mid \dim(\text{VectSp\_over Z}(R))$.

(38) For every finite skew field R holds
card (the carrier of Z(MultGroup(R))) = card (the carrier of Z(R)) $-$ 1.

5. Witt's Proof of Wedderburn's Theorem

One can prove the following proposition

(39) Every finite skew field is commutative.

References

[1] Broderick Arneson and Piotr Rudnicki. Primitive roots of unity and cyclotomic polynomials. *Formalized Mathematics*,12(**1**):59–67,2004.

[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[3] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[5] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[6] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[7] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[8] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[9] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

[10] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[11] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Euler's Theorem and small Fermat's Theorem. *Formalized Mathematics*, 7(**1**):123–126, 1998.

[12] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

[13] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**):573–577, 1997.

[14] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

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

[16] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.

[17] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.

[18] Konrad Raczkowski. Integer and rational exponents. *Formalized Mathematics*, 2(**1**):125–130, 1991.

[19] Konrad Raczkowski and Paweł Sadowski. Equivalence relations and classes of abstraction. *Formalized Mathematics*, 1(**3**):441–444, 1990.

[20] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics.*

[21] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.

[22] Andrzej Trybulec. Function domains and Frænkel operator. *Formalized Mathematics*, 1(**3**):495–500, 1990.

[23] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[24] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[25] Wojciech A. Trybulec. Classes of conjugation. Normal subgroups. *Formalized Mathematics*, 1(**5**):955–962, 1990.

[26] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

[27] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.

[28] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(**5**):855–864, 1990.

[29] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

[30] Wojciech A. Trybulec. Commutator and center of a group. *Formalized Mathematics*, 2(**4**):461–466, 1991.

[31] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[32] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

[33] Mariusz Żynel. The Steinitz theorem and the dimension of a vector space. *Formalized Mathematics*, 5(**3**):423–428, 1996.

Received December 30, 2003