JOURNAL OF FORMALIZED MATHEMATICS
Volume 15, Released 2003, Published 2003
Inst. of Computer Science, Univ. of Białystok

# Witt's Proof of the Wedderburn Theorem[1]

Broderic Arneson
University of Alberta, Edmonton, Canada

Matthias Baaz
Technische Universität Wien, Vienna, Austria

Piotr Rudnicki
University of Alberta, Edmonton, Canada

**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.

WWW: http://mizar.org/JFM/Vol15/weddwitt.html

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

## 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 $\overline{\overline{q^n}} = q^n$.

(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 $\operatorname{card} X = \sum c$.

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

## 2. Class Formula for Groups

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

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

Let $G$ be a group and let $a$ be an element of $G$. The functor Centralizer$(a)$ yields a strict subgroup of $G$ and is defined as follows:

(Def. 1) The carrier of 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 $G$. Note that Centralizer$(a)$ is finite.

We now state two propositions:

(7) For every group $G$ and for every element $a$ of $G$ and for every set $x$ such that $x \in$ 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 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 $(a - \mathrm{con\_map})(x) = a^x$.

We now state several propositions:

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

(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 $(a - \mathrm{con\_map})^{-1}(\{x\})$ misses $(a - \mathrm{con\_map})^{-1}(\{y\})$.

(11) Let $G$ be a group and $a$ be an element of $G$. Then $\{(a - \mathrm{con\_map})^{-1}(\{x\}) : x$ 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 $\overline{\overline{\{(a - \mathrm{con\_map})^{-1}(\{x\}) : x \text{ ranges over elements of } a^\bullet\}}} = \mathrm{card}\, a^\bullet$.

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

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 $G$: $\bigvee_{a\,:\,\text{element of } G} S = a^\bullet\}$.

One can prove the following propositions:

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

## 3. Centers and Centralizers of Skew Fields

One can prove the following 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 $\mathrm{Z}(R)$ yields a strict field and 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 $\mathrm{Z}(R) = (\text{the addition of } R) \restriction [\!:\text{the carrier of } \mathrm{Z}(R),\ \text{the carrier of } \mathrm{Z}(R):\!]$,

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

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

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

We now state the proposition

(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.
One can prove the following 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 $1 < \mathrm{card}(\text{the carrier of } \mathrm{Z}(R))$.

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

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

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$(s) = (\text{the addition of } R) \restriction [\!:\text{the carrier of centralizer}(s),\ \text{the carrier of centralizer}(s):\!]$,

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

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

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

The following propositions are true:

(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 $R$. Note that centralizer$(s)$ is finite.
The following propositions are true:

(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_center$(R)$ yielding a strict vector space over $\mathrm{Z}(R)$ is defined by the conditions (Def. 6).

(Def. 6)(i) The loop structure of VectSp_over_center$(R) =$ the loop structure of $R$, and

(ii) the left multiplication of VectSp_over_center$(R) =$ (the multiplication of $R) \restriction [:$the carrier of $\mathrm{Z}(R)$, the carrier of $R:]$.

The following two propositions are true:

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

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

Let $R$ be a skew field and let $s$ be an element of $R$. The functor VectSp_over_center$(s)$ yielding a strict vector space over $\mathrm{Z}(R)$ is defined by the conditions (Def. 7).

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

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

One can prove the following propositions:

(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 $\mathrm{Z}(R)))^{\dim(\text{VectSp\_over\_center}(s))}$.

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

(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 $\mathrm{Z}(R)))^{\dim(\text{VectSp\_over\_center}(r))} - 1 \mid$ (card(the carrier of $\mathrm{Z}(R)))^{\dim(\text{VectSp\_over\_center}(R))} - 1$.

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

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

## 5. WITT'S PROOF OF WEDDERBURN'S THEOREM

The following proposition is true

(39) Every finite skew field is commutative.

## REFERENCES


[1] Broderic Arneson and Piotr Rudnicki. Primitive roots of unity and cyclotomic polynomials. *Journal of Formalized Mathematics*, 15, 2003. `http://mizar.org/JFM/Vol15/uniroots.html`.

[2] Grzegorz Bancerek. Cardinal numbers. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/card_1.html`.

[3] Grzegorz Bancerek. The fundamental properties of natural numbers. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/nat_1.html`.

[4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/finseq_1.html`.

[5] Czesław Byliński. Functions and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/funct_1.html`.

[6] Czesław Byliński. Functions from a set to a set. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/funct_2.html`.

[7] Czesław Byliński. Some basic properties of sets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/zfmisc_1.html`.

[8] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/finseq_2.html`.

[9] Czesław Byliński. The sum and product of finite sequences of real numbers. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/rvsum_1.html`.

[10] Agata Darmochwał. Finite sets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/finset_1.html`.

[11] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Euler's Theorem and small Fermat's Theorem. *Journal of Formalized Mathematics*, 10, 1998. `http://mizar.org/JFM/Vol10/euler_2.html`.

[12] Krzysztof Hryniewiecki. Basic properties of real numbers. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/real_1.html`.

[13] Andrzej Kondracki. The Chinese Remainder Theorem. *Journal of Formalized Mathematics*, 9, 1997. `http://mizar.org/JFM/Vol9/wsierp_1.html`.

[14] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/vectsp_1.html`.

[15] Anna Justyna Milewska. The field of complex numbers. *Journal of Formalized Mathematics*, 12, 2000. `http://mizar.org/JFM/Vol12/complfld.html`.

[16] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Journal of Formalized Mathematics*, 5, 1993. `http://mizar.org/JFM/Vol5/binarith.html`.

[17] Beata Padlewska. Families of sets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/setfam_1.html`.

[18] Konrad Raczkowski. Integer and rational exponents. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/prepower.html`.

[19] Konrad Raczkowski and Paweł Sadowski. Equivalence relations and classes of abstraction. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/eqrel_1.html`.

[20] Andrzej Trybulec. Binary operations applied to functions. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/funcop_1.html`.

[21] Andrzej Trybulec. Tarski Grothendieck set theory. *Journal of Formalized Mathematics*, Axiomatics, 1989. `http://mizar.org/JFM/Axiomatics/tarski.html`.

[22] Andrzej Trybulec. Function domains and Frænkel operator. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/fraenkel.html`.

[23] Andrzej Trybulec. Subsets of real numbers. *Journal of Formalized Mathematics*, Addenda, 2003. `http://mizar.org/JFM/Addenda/numbers.html`.

[24] Michał J. Trybulec. Integers. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/int_1.html`.

[25] Wojciech A. Trybulec. Vectors in real linear space. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/rlvect_1.html`.

[26] Wojciech A. Trybulec. Classes of conjugation. Normal subgroups. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/group_3.html`.

[27] Wojciech A. Trybulec. Groups. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/group_1.html.

[28] Wojciech A. Trybulec. Pigeon hole principle. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/finseq_4.html.

[29] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/group_2.html.

[30] Wojciech A. Trybulec. Commutator and center of a group. *Journal of Formalized Mathematics*, 3, 1991. http://mizar.org/JFM/Vol3/group_5.html.

[31] Zinaida Trybulec. Properties of subsets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/subset_1.html.

[32] Edmund Woronowicz. Relations and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/relat_1.html.

[33] Mariusz Żynel. The Steinitz theorem and the dimension of a vector space. *Journal of Formalized Mathematics*, 7, 1995. http://mizar.org/JFM/Vol7/vectsp_9.html.

*Received December 30, 2003*

*Published January 6, 2004*