ON WEDDERBURN'S THEOREM ABOUT FINITE DIVISION ALGEBRAS

MICHAEL ADAM AND BIRTE JULIA MUTSCHLER

Abstract. Wedderburn's first proof of his theorem on finite division algebras contains a gap. We analyse the gap, give a variant of Wedderburn's proof that goes completely without the gap-producing statement, and we show how to fill the gap in a way Wedderburn could probably have done it.

Contents

1. Introduction

In the famous paper "A theorem on finite algebras" [15] from the year 1905, Wedderburn[1] first stated his theorem that any finite division algebra is commutative and he gave three different proofs for it. In 1927, Emil Artin [1] remarked that Wedderburn's first proof is not valid. Artin did however not explicate what the gap or flaw is, not even whether it is a gap that can be closed or a serious error that vitiates the whole argument. Instead, he gave a new proof in the spirit of Wedderburn's original ideas. Karen H. Parshall, in her article [21] about the history of Wedderburn's finite division algebra theorem, also discussed the first proof. She explained that it is in fact a gap that can be filled today (but she did not say how) and judged that this would probably have been beyond Wedderburn's scope.

In this paper, we first describe and analyse the gap. Then we present a variant of Wedderburn's first proof which makes no use at all of the statement that produced the gap. We also demonstrate how to fill the gap in a manner that Wedderburn might have done had he been aware of it. Finally, we give a (hopefully rather complete) chronological list of proofs of Wedderburn's theorem in literature.

Acknowledgements. We would like to express our gratitude to Ina Kersten for her kind support and encouragement. We further thank Keith Dennis for pointing out Kasch's proof of Wedderburn's theorem to us.

Date: 23 April, 2003.

2000 *Mathematics Subject Classification.* 16K20, 12E20; 16K50.

Key words and phrases. finite dimensional division algebras, finite fields, Brauer groups.

[1] Why is he called "Joseph H. M. Wedderburn" nowadays while according to his papers, his name appears to have been "J. H. Maclagan-Wedderburn"?

2. The gap

We first describe the gap in Wedderburn's proof. This incorporates a good amount of interpretation, for what Wedderburn writes down in the decisive section is rather vague and misleading at first sight, which is probably due to the fact that the strict modern language and perception of algebra was just emerging at that time. We therefore go into this in rather detail in the beginning.

Wedderburn considers a finite division ring A. It is an algebra of finite dimension s over its center $\mathbb{F}_{p^m} = GF[p^m]$, where p is a prime number. He chooses a basis $x_1, \ldots, x_s$ of A over $\mathbb{F}_{p^m}$ and hence for each $x \in A$ a representation $x = \sum_{i=1}^{s} \xi_i x_i$ with coefficients $\xi_i \in \mathbb{F}_{p^m}$ (called the coördinates of x by Wedderburn). The questionable section in Wedderburn's article (pages 350 and 351 in [15]) starts as follows[2]:

> It follows from the theory of hypercomplex numbers, that there is an equation of lowest degree,
>
> $$f(x) \equiv x^r + a_1 x^{r-1} + a_2 x^{r-2} + \cdots + a_r = 0, \tag{2}$$
>
> with coefficients in $GF[p^m]$, which is satisfied identically by any given number x of the algebra, irrespective of any special relation between the coördinates of x, except the condition that they lie in $GF[p^m]$. Further, there is at least one element of the algebra which satisfies no similar equation of lower degree.

At first sight, Wedderburn really seems to consider the normed polynomial $f \in \mathbb{F}_{p^m}[X]$ of lowest degree which is satisfied by each element of the algebra[3] and then to claim that it is the minimal polynomial of some specific element x of the algebra. This is of course impossible since under these circumstances, f would be on the one hand irreducible, and would on the other hand contain a linear factor $(X - a)$ for each $a \in \mathbb{F}_{p^m}$. So in an attempt to rescue the statement one could consider the polynomial which is satisfied only by all $a \in A \setminus \mathbb{F}_{p^m}$. But this f cannot be the minimal polynomial of an element of the algebra either, which can be seen as follows[4]: For each root a, the polynomial f can be divided (from the right) by the linear polynomial $(X - a)$. In general, if an irreducible polynomial $f \in \mathbb{F}_{p^m}[X]$ is divisible in $A[X]$ from the right by two linear factors $(X - a)$ and $(X - b)$, then a and b are conjugate in A (cf. Artin [1]). Thus, because each element of $A \setminus \mathbb{F}_{p^m}$ is a root of f, it follows that $A \setminus \mathbb{F}_{p^m}$ would consist of one single conjugacy class. So we would obtain for any $a \in A \setminus \mathbb{F}_{p^m}$ with centralizer $Z(a)$

$$p^{ms} - p^m = |A \setminus \mathbb{F}_{p^m}| = |A^*|/|Z(a)^*| = (p^{ms} - 1)/(p^{mt} - 1)$$

where $[Z(a) : \mathbb{F}_{p^m}] = t$. In any case this would yield the contradiction that p divides one. But even if there was such an element with f as minimal polynomial, this polynomial f would not fulfill the requirements for the rest of the proof. See section 4.

[2] Like Parshall, we have corrected a misprint in the quotation: The constant coefficient in equation (2) was called a_{r-1} instead of a_r.

[3] Note that such a polynomial exists if and only if the algebra is finite.

[4] A word of warning: One cannot simply divide f by each linear factor $(X - a)$, concluding that f would have degree at least $|A \setminus \mathbb{F}_{p^m}| = p^{ms} - p^m$, while a minimal polynomial of an element $a \in A$ can have degree at most $[A : \mathbb{F}_{p^m}] = s$. The reason is that evaluation of polynomials with non-commutative coefficients is not compatible with multiplication, and this leads to strange phenomena. Here is an example of a polynomial of degree 2 which has at least 6 different roots: Let $D = F \oplus Fu \oplus Fv \oplus Fw$ be the quaternion algebra over some field F, i.e. $u^2 = v^2 = w^2 = -1$ and $uv = w$. Then the polynomial $X^2 + 1$ has $\pm u$, $\pm v$ and $\pm w$ as roots.

This indicates that Wedderburn must have meant something else than he apparently wrote down. A first hint is given by the argument for the claim cited above:

> Indeed, (2) states that $x^{r-1}, x^{r-2}, \dots, x^0$ are linearely independent with respect to $GF[p^m]$, and the condition of independence can evidently be put in a form which states that certain determinants, whose elements are rational integral functions of the coördinates of x, do not all vanish identically. Hence there must be some set of values of the coördinates for which $x^{r-1}, x^{r-2}, \dots, x^0$ are independent and hence the particular x so obtained can satisfy no equation of lower degree than r. (2) is called the characteristic or identical equation, while the equation of lowest degree satisfied by a given x is called its reduced equation.

Furthermore, comparing with the section "The identical equation" of his article "On hypercomplex numbers" [16] from 1907, one sees[5] that Wedderburn must actually be talking about the *generic minimal polynomial* $M_{X,A} = M_X$ of A (using modern terminology): Let $X_1, \dots, X_s$ be algebraically independent over $\mathbb{F}_{p^m}$. The *generic element* of A is defined to be

$$X = \sum_{i=1}^{s} X_i \cdot x_i \ \in \ \mathbb{F}_{p^m}(X_1, \dots, X_s) \otimes_{\mathbb{F}_{p^m}} A.$$

Its minimal polynomial $M_{X,A}$ over the function field $\mathbb{F}_{p^m}(X_1, \dots, X_s)$ is called the generic minimal polynomial of A. We will see in section 4 that this polynomial does the job in the rest of the proof, which leaves no doubt as to which polynomial Wedderburn was talking about. The coefficients of the generic minimal polynomial are in fact polynomials in the X_i, and so we can evaluate the coefficients of $M_{X,A}$ at the coordinates ξ_i of an element $x = \sum_i \xi_i x_i$ of A, thus obtaining a polynomial $M_{x,A} \in \mathbb{F}_{p^m}[T]$, called *the generic minimal polynomial of A evaluated at x*. It has the property that $M_{x,A}(x) = 0$. In this terminology, Wedderburn's claim reads as follows:

2.1. **Claim.** *For a finite dimensional central division algebra A over $\mathbb{F}_{p^m}$, there exists an element $x \in A$ such that $M_{x,A}$ equals the minimal polynomial of x over $\mathbb{F}_{p^m}$.*

Wedderburn argues as follows: Write $X^j = \sum_i f_{ij}(X_1, \dots, X_s) x_i$ with $f_{ij} \in \mathbb{F}_{p^m}[X_1, \dots, X_s]$, and let $M_{X,A}$ be of degree r. Then from the $\mathbb{F}_{p^m}(X_1, \dots, X_s)$-linear independence of the powers $1, X, X^2, \dots, X^{r-1}$ it follows that some r-minor of the matrix $(f_{ij})_{ij}$ is a nonzero polynomial in $\mathbb{F}_{p^m}[X_1, \dots, X_s]$. Now Wedderburn concludes without further reasoning that there are elements in $\mathbb{F}_{p^m}$ for which this polynomial does not vanish.

Wedderburn really does not seem to have had any further argument for this step in mind because two years later, he made the same statement as claim 2.1 for an arbitrary finite dimensional (associative) algebra instead of a division algebra, saying it was obvious. While for a division algebra this can be proven, as shown in section 5 below, it is false for an arbitrary algebra. The following counterexample is tributetd to K. McCrimmon by Parshall ([21], p. 285): Let $A = \mathbb{F}_{p^m} e_1 \oplus \cdots \oplus \mathbb{F}_{p^m} e_n$ with orthogonal idempotents e_i. Then the generic minimal polynomial of X has degree n while each element of the algebra satisfies the equation $x^{p^m} - x = 0$. So one just has to choose n large enough to obtain an algebra for which the generic

[5] Parshall [21, p. 285] also made this—to our judgement non-obvious—interpretation but gave no hint as to how she arrived at this viewpoint.

minimal polynomial has degree strictly larger than any of the minimal polynomials of elements of A.

2.2. **Conclusion.** *We consider the gap in Wedderburn's first proof to be the insufficient proof for statement* 2.1. ◇

3. The generic minimal polynomial

In this section, we present some lemmas around the generic minimal polynomial of a finite dimensional algebra, specifically a division algebra. Note that even if the proofs are given in a modern language, they use only methods that were available to Wedderburn.

Let us fix some notations. We consider finite dimensional algebras A over some field F. These are always meant to be associative and to have a unit. Then for an element $a \in A$ we denote the minmal polynomial of a over F by m_a or $m_{a/F}$ if the reference to the ground field has to be made clear. Similarly, the characteristic polynomial of a in A is denoted by $p_a = p_{a,A/F}$. If A is a division algebra, we have $p_{a,A/F} = m_{a/F}^\alpha$ for some integer α.

Let $x_1, \ldots, x_s$ be a F-basis of A, and let $X = \sum X_i \cdot x_i \in F(X_1, \ldots, X_s) \otimes_F A$ be the *generic element* of A. We have already defined the generic minimal polynomial of A as the minimal polynomial $M_{X,A} := m_{X/F(X_1,\ldots,X_s)}$ of X. Now we define the *generic characteristic polynomial* of A as the characteristic polynomial $P_{X,A} := p_{X,F(X_1,\ldots,X_s)\otimes A}$ of X. As with the generic minimal polynomial, the coefficients of $P_{X,A}$ are polynomials in the X_i and hence for any $a = \sum a_i x_i \in A$, we can *evaluate* (the coefficients of) $P_{X,A}$ at a to obtain $P_{a,A} \in F[T]$. We always have $P_{a,A} = p_{a,A/F}$. In particular, $\deg P_{X,A} = [A : F]$.

3.1. **Lemma.** *Let F be any field, and let A be a finite dimensional non-commutative algebra over F with $F \subset C(A)$, the center of A. Then* $\deg M_{X,A} < [A : F]$.

Proof. Let $x_1, \ldots, x_s$ be an F-basis for A, and let $L = F(X_1, \ldots, X_s)$. The L-subalgebra $L[X]$ of $L \otimes_F A$ generated by the generic element $X = \sum_i X_i \cdot x_i$ is of dimension $\deg M_{X,A}$. Now $L \subset C(L \otimes_F A) = L \otimes_F C(A)$ since $F \subset C(A)$, and so $L[X]$ is commutative. Hence $L[X] \subsetneq L \otimes_F A$, because $L \otimes_F A$ is non-commutative. □

3.2. **Lemma.** *Let A be a finite dimensional division algebra over some field F. Let $T_1, \ldots, T_n$ be indeterminates over F. Then $F(T_1, \ldots, T_n) \otimes_F A$ is a division algebra.*

This lemma is well known. We we reproduce the following proof from Jacobson [11, p. 33] in order to show that the result was within Wedderburn's reach.

Proof. The polynomial ring $A[T_1] = F[T_1] \otimes_F A$ is a domain. Hence by induction, $F[T_1, \ldots, T_n] \otimes_F A = A[T_1, \ldots, T_n]$ is a domain. Since every element of $F(T_1, \ldots, T_n) \otimes_F A$ can be written in the form $f \cdot g^{-1}$ with $f \in A[T_1, \ldots, T_n]$ and $g \in F[T_1, \ldots, T_n] \setminus \{0\}$, it follows that $F(T_1, \ldots, T_n) \otimes_F A$ is a domain, too. As a finite dimensional algebra over the field $F(T_1, \ldots, T_n)$ it is thus a division algebra. □

3.3. **Corollary.** *For a finite dimensional division algebra A over a field F, we have $P_{X,A} = M_{X,A}^\alpha$ for a suitable integer α.*

Proof. $P_{X,A}$ and $M_{X,A}$ are, respectively, the characteristic and minimal polynomial of the same element X of the division algebra $F(X_1 \ldots, X_s) \otimes_F A$. □

3.4. **Lemma.** *Let F be any field, and let A be a finite dimensional division algebra over F. Let $a \in A$. Then $M_{a,A}$ is a power of the minimal polynomial $m_{a/F}$ of a over F. In particular, the degree of m_a divides the degree of the generic minimal polynomial.*

Proof. By the above corollary, $P_{X,A} = M_{X,A}^{\alpha}$ for some integer α. Hence also for any $a \in A$, we have $P_{a,A} = M_{a,A}^{\alpha}$. Now $P_{a,A} = p_{a,A/F} = m_{a/F}^{\beta}$ for some integer β. From the irreducibility of m_a, we conclude that β is divisible by α and that $M_{a,A} = m_a^{\gamma}$ for $\gamma = \beta/\alpha$. □

4. A variant of Wedderburn's first proof

In this section, we present a variant of Wedderburn's first proof in a slightly modernised language, which does not use the gap-producing claim 2.1 at all.

Variant of Wedderburn's proof. Let A be a finite division ring. It is of some dimension s over its center $C(A) \cong \mathbb{F}_{p^m} = \mathbb{F}_q$, where p is a prime number. We divide the proof into two steps:

(1) We choose representatives $a_1, \dots, a_t$ for the conjugacy classes of elements of $A \setminus \mathbb{F}_{p^m}$. Denoting $s_i := [C(a_i) : \mathbb{F}_q]$, we then have by the class equation

$$q^s - 1 = |A^*| = |\mathbb{F}_q^*| + \sum_{i=1}^{t} \frac{|A^*|}{|C(a_i)|} = q - 1 + \sum \frac{q^s - 1}{q^{s_i} - 1}$$

It follows, that $q - 1$ is divisible by

$$\begin{aligned} \gcd\left(\frac{q^s-1}{q^{s_i}-1} : i = 1, \dots t\right) &= \frac{q^s - 1}{\operatorname{lcm}(q^{s_i} - 1 : i = 1, \dots, t)} \\ &= \frac{q^s - 1}{q^{\operatorname{lcm}(s_1, \dots, s_t)} - 1} \end{aligned}$$

Hence, denoting $s' = \operatorname{lcm}(s_1, \dots, s_t)$, we have

$$(q-1) \cdot (q^{s'} - 1) = l \cdot (q^s - 1)$$

for some integer l. It follows that $l \equiv -1 \pmod{q}$, hence $l = k \cdot q - 1$ for some postive k. Using $s' \leq s$, we see that $k = 1$ and $s' = s$.

(2) Now we suppose by induction that all division rings of order strictly less than $|A|$ are commutative. Then in particular, the centralizers $C(a)$ of elements $a \in A \setminus \mathbb{F}_q$ are commutative, so these are precisely the maximal subfields of A. Since $\mathbb{F}_q$ is perfect, each centralizer C is, as a finite field extension of $\mathbb{F}_q$, generated by one element a, hence $[C : \mathbb{F}_q]$ equals the degree of the minimal polynomial of a. But by lemma 3.4, the degree of the minimal polynomial always divides the degree r of the generic minimal polynomial. So we have

$$s = \operatorname{lcm}\big([C(a) : \mathbb{F}_q] \ : \ a \in A \setminus \mathbb{F}_q\big) \ | \ r \ \leq \ s \tag{4.1}$$

which implies $[A : F] = s = r = \deg M_{X,A}$. But by lemma 3.1, this yields $A = F$. □

4.2. **Remark.** Step one above is taken more or less directly from Wedderburn's proof. In the second step, Wedderburn argues that in addition by claim 2.1, there is one $b \in A \setminus \mathbb{F}_q$, for which $m_{b/\mathbb{F}_q} = M_{b,A}$, whence equation (4.1) simplifies to

$$s = \operatorname{lcm}\big([C(a) : \mathbb{F}_q] \ : \ a \in A \setminus \mathbb{F}_q\big) = [C(b) : \mathbb{F}_q] = r.$$

Then he concludes that $C(b) = A$, contradicting $b \in A \setminus C(A)$. ◇

5. Filling the gap

In this section we demonstrate how to fill the gap in Wedderburn's proof. We do not rescue his insufficient argument but instead give a new proof of claim 2.1. The proof is based upon the following three statements:

5.1. **Lemma.** *Let F be any field, and let A be finite dimensional central division algebra over F.*

(1) *The dimension of A over F is a square.*
(2) *Each maximal subfield L of A has degree $[L : F] = \sqrt{[A : F]}$.*
(3) *The degree of the generic minimal polynomial of A is $\sqrt{[A : F]}$.*

We first show how to prove claim 2.1 using these statements.

Proof of claim 2.1. For a finite ground field $F = \mathbb{F}_{p^m}$ and a central division algebra A of dimension $s = r^2$ over F, take a maximal subfield L and choose a generator a (note that $\mathbb{F}_{p^m}$ is perfect and hence L is separable over $\mathbb{F}_{p^m}$). Then the minimal polynomial m_a of a has degree r. The degree of the generic minimal polynomial also equals r and, since $M_a(a) = 0$, we conclude $m_a = M_a$. □

We now investigate to what extent Wedderburn knew or could have proven the above statements.

Statement (1)*:* The first statement has surely been within Wedderburn's reach. He could have argued as follows using his famous structure theorem [16] on simple algebras: Central simple algebras stays simple under extension of the base field. So in particular for any algebraically closed field extension F' of F, the F'-algebra $F' \otimes_F A$ is isomorphic to a matrix algebra over a finite dimensional division algebra over F' by the structure theorem. But over an algebraically closed field, there is no finite dimensional division algebra except for F' itself since any bigger algebra would contain a proper finite commutative field extension of F' which is impossible. So as a matrix algebra, $F' \otimes_F A$ has square dimension over F', and this dimension equals the dimension of A over F.

Statement (2)*:* Statement (2) (and therefore also (1)) can be proven completely elementary for a finite base field, cf. e.g. Artin [1] or Schue [23]. Artin's proof uses polynomials with coefficients in a skew field, conjugation of subfields, some linear algebra and counting arguments. Schue's proof employs normalizers, some Galois theory and a lot of linear algebra. All of these means have been available to Wedderburn.

5.2. **Remark.** Although Wedderburn could have proven statement (2), he was surely not aware of this fact. If he had been, he would also have noticed that this immediately yields another, much shorter proof of his theorem, since it stongly simplifies the class equation also employed in Wedderburn's proof:

Let A be a central division algebra of dimension $s = r^2$ over $F = \mathbb{F}_q$. Assume by induction, that all division algebras of lower dimension are commutative. In particular all centralizers $C_1, \dots, C_t$ of elements of $A \setminus F$ are maximal subfields, hence $[C_i : F] = r$. Then the class equation for conjugacy classes of A^* reads

$$q^{r^2} - 1 = |A^*| = |F^*| + \sum_{i=1}^{t} \frac{q^{r^2} - 1}{q^r - 1},$$

which implies that $\frac{q^{r^2}-1}{q^r-1}$ divides $q - 1$ and hence that $r = 1$. (This is also how Schue completes his proof of Wedderburn's theorem.)

Furthermore, statement (2) also abbreviates step (2) of Wedderburn's original proof, if one wants to use the class equation in his way:

> As before, we have by induction that the centralizers are exactly the maximal subfields. Combined with the statement that the maximal subfields all have degree r with $r^2 = s$, this yields $r^2 = s = \operatorname{lcm}\big([C(a) : \mathbb{F}_q] \ : \ a \in A \setminus \mathbb{F}_q\big) = r$, and thus $r = 1$. $\diamond$

Statement (3)*:* So we are left with the task of proving the third statement, using only means available to Wedderburn.

Proof of (3). Let A be a central division algebra of dimension $s = r^2$ over a field F. We first prove that the degree of the generic minimal polynomial is at least r. Choose an algebraically extension field F' of F. Then $F' \otimes_F A = A_{F'} \cong \mathrm{M}_r(F')$, the F'-algebra of $r \times r$ matrices with entries in F', as shown in the argument for statement (1). We choose an F-basis $e_{i,j}$ $(i, j = 1, \dots r)$ of A such that the $1 \otimes e_{i,j}$ correspond to the standard basis of $\mathrm{M}_r(F')$. Since $M_{X,A_{F'}}$ divides $M_{X,A}$, it suffices to show that $\deg M_{X,A_{F'}} \geq r$. Over F', the generic element $X = \sum X_{ij} e_{ij}$ is thus the "generic matrix" (X_{ij}). If we specialise (X_{ij}) to a diagonal matrix in $A_{F'} \cong \mathrm{M}_r(F')$ with pairwise distinct non-vanishing diagonal entries, the minimal polynomial of this matrix equals its characteristic polynomial and hence has degree r. (Note that for such a matrix to exist, F' must contain at least $r + 1$ distinct elements; since we choose F' to be algebraically closed, we are on the safe side.) We conclude $\deg M_{X,A_{F'}} \geq r$, as required[6].

To show that the degree of the generic minimal polynomial is at most r, we note that by lemma 3.2 above, $F(X_{11}, \dots, X_{rr}) \otimes_F A$ is again a central division algebra of dimension r^2, and thus the subfield generated by X is of degree at most r over $F(X_{11}, \dots, X_{rr})$ by statement (2) of lemma 5.1; but the degree of this subfield is just the degree of the generic minimal polynomial, hence we are done. □

5.3. **Remark.** The statement of (3) is true more generally for any finite dimensional central simple algebra. One can also prove the more precise statement that the generic minimal polynomial equals the generic reduced characteristic polynomial. The proof is very similar to the proof given above, but one of course has to systematically introduce the reduced characteristic polynomial of a central simple algebra—which was implicitly used above in case of a matrix algebra—and show that it is well defined using the theorem of Skolem-Noether. As we need the statement only in the simpler form of (3), we skip this proof. $\diamond$

5.4. **Conclusion.** *Our final conclusion is that Wedderburn's proof did in fact contain a gap he was not aware of, but that he could well have provided the necessary arguments to fill it with.* $\diamond$

Appendix. Chronological list of proofs

All over the past century, new proofs of Wedderburn's theorem on finite division algebras have been given by numerous mathematicians. The proofs vary enormously with respect to length and depth of the means employed. In her graduation paper [18], the second author has searched through the literature for proofs and gave a detailed exposition of each proof found in a thematically ordered compilation as well as a comparison of the different proofs. As a result of this effort, we present here a chronologically ordered and hopefully rather complete list of (original) proofs of Wedderburn's theorem present in literature with short comments on each proof.

[6] By the theorem of Cayley-Hamilton, the $r \times r$-matrix (X_{ij}) satisfies its characteristic polynomial, which is of degree r. Thus, we do in fact have $\deg M_{X,A_{F'}} = r$.

1905, Wedderburn: There are three different proofs in "A theorem on finite algebras" [15]. The first proof was discussed in the preceding sections, the two others are more group theoretic, using Zsigmondy's theorem and the automorphism group of the algebra.

1905, Dickson: Dickson published a proof in the same year [5]. This proof is very similar to Wedderburn's second and third proof. Dickson remarked that Wedderburn found these proofs only after having seen Dickson's proof.

1927, Artin: In [1], after remarking that Wedderburn's first proof from [15] was not valid, Artin gave a new proof close to Wedderburn's main ideas, using some group theory, divisibility properties of polynomials, proving that all maximal subfields of the algebra are conjugate.

1928, Noether: This proof from lectures by E. Noether, written down in 1931 by van der Waerden [27], is very similar to that of Artin, using maximal subfields and group theoretic conjugacy arguments.

1929, Brauer: In the article [2] concerned with the study of algebras via group theoretic means using factor systems (certain Galois cocycles), Brauer derives Wedderburn's theorem from the more general theorem that the Schur index of a finite simple algebra equals one.

1931, Witt: In this one-page paper [28], Witt uses only cyclotomic polynomials and elementary group theory to prove Wedderburn's theorem.

1932, Hasse-Noether: Noether [20] and Hasse [9] remark that the relative Brauer group $\mathrm{Br}(L/K)$ is isomorphic to $K^*/N_{L/K}(L)$ for a finite cyclic extension L/K. Combined with the fact that the norm is surjective for finite extensions of finite fields, this yields Wedderburn's theorem.[7]

1935, Chevalley: Inspired by Tsens work [26] about function fields of transcendence degree one over an algebraically closed field, and a remark of Artin, Chevalley proved in [4] that finite fields are C_1 and that over a C_1-field, there are no finite dimensional central division algebras except for the field itself, obtaining Wedderburn's theorem as a corollary.

1951, Serre: In his report [25] on Galois cohomology and the theory of simple algebras, Serre proves Wedderburn's theorem using (and proving) the facts[8] that the relative Brauer group $\mathrm{Br}(L/K) \cong H^2\big(\mathrm{Gal}(L/K), L^*\big)$ for a finite Galois extension L/K, that $H^2\big(\mathrm{Gal}(L/K), L^*\big) \cong K^*/N_{L/K}(L^*)$ for a cyclic extension L/K, and the classical fact that the norm is onto for finite fields.

1952, Zassenhaus: In his rather long group theoretic proof [29], Zassenhaus derives Wedderburn's theorem from the theorem (proved in the same paper) that a finite group is abelian if for each abelian subgroup, the normalizer conincides with the centralizer.

1961, Herstein: Herstein [10] gives a completely elementary proof by longish calculations, using only some theory of finite fields and group theory.

1964, Kaczynski: Using deep results from the theory of finite groups, Kaczynski [12] shows that the group of units of a finite division algebra is simple and solvable, which is only possible for an abelian group.

1964, Scott: In this group theoretical proof [24, p. 427], Scott shows that all q-Sylow subgroups of the group of units of the division algebra are cyclic

[7] Although the authors do not mention this consequence explicitly, there is no doubt that they were aware of it. Furthermore, since the two articles given above do neither contain a proof of the result nor a reference, it is not clear to us to whom the proof should be tributed, and so we have cited both.

[8] Each of these statements was known before, cf. e.g. Eilenberg [7], but we have not found them put together like this to give a proof of Wedderburn's theorem, any earlier.

for $q \neq 2$ and cyclic or generalised quaternion groups for $q = 2$, and derives a contradiction studying the order of suitable elements and subgroups.

1969, Ebey and Sitaram: The authors [6] use projective geometries to describe the group of units as the Frobenius complement of a Frobenius group and then employ deep results from the theory of finite groups to prove Wedderburn's theorem.

1970, Burn and Maduram: Burn and Maduram [3] give a variant of [6], avoiding the use of geometry.

1971, Rogers: Rogers' proof [22] strongly resembles Herstein's proof [10] from 1961. Being hardly less elementary, the calculations are more structured and make use of conjugates of subfields.

1974, Nagahara and Tominaga: Proving a theorem of Jacobson in [19], the authors give two proofs of Wedderburn's theorem, applying elementary ring and group theory and several dimension arguments.

1988, Schue: Schue [23] calculates the dimension of centralizers as the square root of the dimension of the algebra by means of linear algebra and Galois theory, and then applies the class equation.

1989, Meixner: For a finite division algebra, Meixner [17] considers a Sylow subgroup for the maximal prime divisor of the order of the group of units. Using elementary group theory, he concludes that the corresponding cyclotomic number must be a power of 2, deriving a contradiction.

1990, Lorenz: Lorenz' textbook [14] on algebra contains a proof of Wedderburn's theorem on page 269, that we did not find earlier in literature. It uses an explicit formula for the behaviour of the presentation of central division algebras as crossed products under cyclic extensions.

1994, Kasch: In his booklet [13], Kasch gives a simple proof of the main theorem of Galois theory for skew fields. As an application, this theorem is used in a proof of Wedderburn's theorem (pages 22–23, loc. cit.) to calculate the degree of a maximal subfield of a finite central division algebra and to obtain an upper bound for the number of maximal subfields.

1998, Grundhöfer: Grundhöfer's proof [8] resembles Witt's proof in that he uses cyclotomic polynomials, group theory and elementary number theory, but the main argument is transferred to obtain a purely group theoretical result at first.

Remark. We have not taken into account any of the huge number of generalizations of Wedderburn's theorem but only listed publications which contain a "direct" proof that does not merely obtain the theorem as a special case of a more general result.

References

1. Emil Artin, *Über einen Satz von Herrn J. H. Maclagan Wedderburn*, Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität **5** (1927), 245–250.
2. Richard Brauer, *Über Systeme hyperkomplexer Zahlen*, Mathematische Zeitschrift **30** (1929), 79–107.
3. R. P. Burn and D. M. Maduram, *Frobenius groups and Wedderburn's theorem*, American Mathematical Monthly **77** (1970), no. 9, 984–984.
4. C. Chevalley, *Démonstration d'une hypothèse de M. Artin*, Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität **11** (1935), 73–75.
5. Leonard Eugene Dickson, *On finite algebras*, Nachrichten der Gesellschaft der Wissenschaften zu Göttingen (1905), 358–393.
6. S. Ebey and K. Sitaram, *Frobenius groups and Wedderburn's theorem*, American Mathematical Monthly **76** (1969), no. 5, 526–528.
7. Samuel Eilenberg, *Topological methods in abstract algebra. Cohomology theory of groups*, Bulletin of the American Mathematical Society **55** (1949), 3–37.

8. Theo Grundhöfer, *Commutativity of finite groups according to Wedderburn and Witt*, Archiv der Mathematik **70** (1998), 425–426.
9. Helmut Hasse, *Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper*, Mathematische Annalen **107** (1933), 731–760.
10. I. N. Herstein, *Wedderburns theorem and a theorem of Jacobson*, American Mathematical Monthly **68** (1961), 249–251.
11. Nathan Jacobson, *Finite-dimensional division algebras over fields*, Springer-Verlag, Berlin, 1996.
12. Theodore Kaczynski, *Another proof of Wedderburn's theorem*, American Mathematical Monthly **71** (1964), 652–653.
13. Friedrich Kasch, *Die Galoissche Theorie für Schiefkörper*, Algebra Berichte, vol. 72, Verlag Reinhard Fischer, München, 1994.
14. Falko Lorenz, *Einführung in die Algebra Teil II*, B.I.-Wissenschaftsverlag, Mannheim, Wien, Zürich, 1990.
15. J. H. Maclagan-Wedderburn, *A theorem on finite algebras*, Transactions of the American Mathematical Society **6** (1905), 349–352.
16. J. H. P Maclagan-Wedderburn, *On hypercomplex numbers*, Proceedings of the London Mathematical Society **6** (1908), 77–118.
17. Thomas Meixner, *Eine Bemerkung zu den Kreisteilungsolynomen*, Mathematische Semesterberichte **36** (1989), 125–138.
18. Birte Julia Mutschler, *Ältere und neuere Beweise des Satzes von Wedderburn, dass die Brauergruppe eines endlichen Körpers trivial ist*, Staatsexamensarbeit, Universität Göttingen, November 2002, 89 pages.
19. Takasi Nagahara and Hisao Tominaga, *Elementary proofs of a theorem of Wedderburn and a theorem of Jacobson*, Abhandlungen mathematisches Seminar der Universitt Hamburg **41** (1974), 72–74.
20. Emmy Noether, *Hyperkomplexe Systeme in ihren Beziehungen zur kommutativen Algebra und Zahlentheorie*, Verhandlungen des internationalen Mathematiker-Kongresses Zürich, erster Band, Bericht und allgemeine Vorträge (Zürich, Leipzig), Orell Füssli Verlag, 1932, pp. 189–194.
21. Karen Hunger Parshall, *In pursuit of the finite division algebra theorem and beyond: Joseph H. M. Wedderburn, Leonard E. Dickson and Oswald Veblen*, Archives Internationales d'Histoire des Sciences **33** (1983), no. 111, 274–299.
22. Kenneth Rogers, *An elementary proof of a theorem of Jacobson*, Abhandlungen des Mathematischen Seminars der Hamburgischen Universität **35** (1971), 223–229.
23. John Schue, *The Wedderburn theorem of finite division rings*, American Mathematical Monthly **95** (1988), no. 5, 436–437.
24. W. R. Scott, *Group Theory*, Prentice Hall, New Jersey, 1964.
25. Jean-Pierre Serre, *Applications algébriques de la cohomologie des groupes. II : Théorie des algèbres simples*, Séminaire Henri Cartan de l'Ecole Normale Supérieure, 1950/1951. Cohomologie des groupes, suite spectrale, faisceaux, Secrétariat mathématique, 11 rue Pierre Curie, Paris, 1955, 2e éd.
26. Chiungtze C. Tsen, *Divisionsalgebren über Funktionenkörpern*, Nachrichten der Gesellschaft der Wissenschaften zu Göttingen (1933), 333–339.
27. B. L. van der Waerden, *Moderne Algebra. Zweiter Teil. Unter Benutzung von Vorlesungen von E. Artin und E. Noether*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen mit besonderer Berücksichtigung der Anwendungsgebiete, vol. 34, Verlag von Julius Springer, 1931.
28. Ernst Witt, *Über die Kommutativität endlicher Schiefkörper*, Abhandlungen aus dem Maithematischen Seminar der Hamburgischen Universität **8** (1931), 413, see also *Collected Papers–Gesammelte Abhandlungen*, ed. by Ina Kersten, Springer 1998.
29. Hans J. Zassenhaus, *A group-theoretic proof of a theorem of Maclagan-Wedderburn*, Proceedings of the Glasgow Mathematical Association **1** (1952), 53–63.

Michael Adam, Mathematisches Institut, Universität Göttingen, Bunsenstrasse 3–5, D-37073 Göttingen, Germany

E-mail address: `mad@uni-math.gwdg.de`

Birte Julia Mutschler, Mathematisches Institut, Universität Göttingen, Bunsenstrasse 3–5, D-37073 Göttingen, Germany

E-mail address: `Birte.Julia@web.de`