Submitted exclusively to the London Mathematical Society
doi:10.1112/0000/000000

Completing Segre's proof of Wedderburn's little theorem

John Bamberg and Tim Penttila

Abstract

We use the Dandelin–Gallucci Theorem to give a proof of Wedderburn's little theorem that every finite division ring is commutative, and the proof is geometric in the sense that the non-geometric concepts employed are of an elementary nature. As a consequence, we obtain a geometric proof that a finite Desarguesian projective space is Pappian.

1. *Introduction*

J. H. Maclagan-Wedderburn (1905) [24] exploited the interplay between a finite division ring and its group of units to prove the following famous result:

Theorem 1.1 (Wedderburn's Little Theorem). *A finite division ring is commutative (and hence a field).*

Wedderburn gave three proofs, with only the first (and the most well-known proof) having a gap that was identified and resolved by his close colleague L. E. Dickson[†] [14] (see also [28]). The other two proofs rely on a number theoretic result[‡] that Wedderburn attributes to Birkhoff and Vandiver [6], but which was proved 18 years earlier by Bang [4] and is often attributed to Zsigmondy [35], who proved it six years after Bang. There have been further simplifications, generalisations, and novel approaches taken in reproving Wedderburn's Theorem and we refer to the preprint [1] for a brief synopsis of some of the known[§] proofs. To the authors' knowledge, with the possible exception of the proof of Tecklenburg [31], every known proof of Wedderburn's Theorem uses only techniques that could be typified as number theoretic or stemming from *abstract algebra*, and in particular, the theory of rings and groups. Our approach is to use *finite geometry*, preceded by elementary facts on division rings. In particular, our approach can be summarised in the following steps:

- We begin by proving that a finite division ring with all proper subrings commutative, has odd dimension over its centre (Theorem 4.2).
- We then show that such a finite division ring has a quadratic extension (Corollary 4.6).

2000 *Mathematics Subject Classification* Primary 12E15, Secondary 05B25.

[†]Amusingly, Dickson was attempting to find a counter-example to Wedderburn's result, and established that there was none. He published his proof in the same year as Wedderburn's work, with the following footnote:

> First proved by Wedderburn ... Following my simpler proof above, and using the same lemma, Wedderburn constructed two further simple proofs, *loc. cit.*

[‡]If q is a prime and n is an integer with $n > 1$, then apart from some exceptions, there exists a prime p dividing $q^n - 1$ but not dividing $q^m - 1$ for any $1 \leqslant m < n$. The exceptions are $(q, n) = (2, 6)$, and $n = 2$ with q a Mersenne prime.

[§]Their synopsis does not include the notable proofs of Henderson (1965) [16], Outcalt and Yaqub (1967) [26], McCrimmon (1969) [25], and Tecklenburg (1987) [31].

– If D' is the quadratic extension of a finite division ring D, then we obtain a spread of the projective space $\mathsf{PG}(3, D)$ by *division-ring reduction* of the projective line $\mathsf{PG}(1, D')$.
– We apply the Dandelin–Gallucci Theorem to a minimal counterexample to Wedderburn's theorem to show that D is a field.

Tecklenburg's proof that a finite Desarguesian plane is Pappian avoids the representation theorem for Desarguesian planes (that every Desarguesian plane can be coordinatised by a division ring). But it relies on Witt's proof [34] of Wedderburn's Theorem using cyclotomic polynomials. In his review of Tecklenburg's paper, Payne concludes with: "... the proof seems likely to discourage all but the most determined readers." In his posthumously published notes "Projektive Geometrie" [23], Lüneburg says of the theorem that every finite Desarguesian plane is Pappian:

> "Alle Beweise ..., die ich kenne, benutzen den Satz von Wedderburn, dass alle endlichen Körper kommutativ sind. Einen geometrischen Beweis zu finden, scheint also sehr schwierig zu sein. Den Beweis von Tecklenburg 1987 kann ich nicht als einen solchen werten, da er nur den einfachen wittschen Beweis des wedderburnschen Satzes in eine komplizierte geometrische Sprache übersetzt."

This is a fair assessment: the geometric notation of Tecklenburg's proof *is* complicated.

Beniamino Segre, in his *Lectures on Modern Geometry* [29], had also attempted to use projective geometry to prove Wedderburn's Theorem, without success [29, §196,204]. He provided several different approaches, all of which are as yet, incomplete. The centrepiece of our approach is to use the "Dandelin–Gallucci Theorem" [11, 15]; one of the most beautiful results on configurations in projective three-space.

THEOREM 1.2 (Dandelin–Gallucci Theorem). *Given three pairwise skew lines in a projective space of dimension three and another three pairwise skew transversal lines to these, the underlying division ring is a field if and only if every transversal to the first set of lines meets every transversal to the second set of lines.*

For a proof, see Baker [2, Chapter 1, pp. 47 – 49 and pp. 77 – 83], to whom the result is due, with origins in theorems for real projective 3-space in [10, 11, 12] and, independently, [15]. See also [5, Theorem 2.4.2]. We point out that Baker's treatment gives a direct synthetic connection to Pappus' theorem in the spirit of Dandelin's original work.

2. *Background on division rings*

A division ring could be informally described as something that is like a field, but with the multiplication operation not necessarily being commutative. More precisely, it is a unital ring (with $1 \neq 0$) in which every nonzero element has a multiplicative inverse. In the literature, division rings are sometimes called *skew-fields*. Fields are division rings, but the ring of quaternions is an example of a division ring that is not a field. A left-module M over a division ring D is a left-vector space, and as long as we are careful with the order in which we apply our operations, we retain many of the results of linear algebra over fields. For example, the row-rank and column-rank of a matrix are equal (and so we can *define* the rank of a matrix) and every two bases of a finitely generated left-vector space V have the same size (and so we can *define* the left-dimension of V). We must be careful: there do exist abelian groups V equipped with division rings D whose left-dimension is not equal to their right-dimension (see [20, p. 158]).

All vector spaces in our paper will be left-vector spaces, that is, scalar multiplication is applied to the left of (row) vectors. We also still have the nice property that left-degrees are multiplicative. If we have a tower of division rings, $D \leqslant D' \leqslant D''$, with each extension finite,

then $|D'' : D|_L = |D'' : D'|_L \cdot |D' : D|_L$, where $|E : F|_L$ is the dimension of E as a left vector space over F. The centre $\mathsf{Z}(D)$ of a division ring D is a field and hence we obtain a canonical vector space of D over its centre. For example, the quaternions form a 4-dimensional vector space over its centre, and its centre is isomorphic to the real numbers. We refer the reader to Jacobson's book [20], Chapter VII, for more on the theory of division rings, but we will conclude with more technical facts that will become useful in Section 4.

If a is a nonzero element of a division ring D, then the *centraliser* $C_D(a)$ of a in D is the set of elements $d \in D$ that commute with a (i.e., $ad = da$). It is not difficult to see that $C_D(a)$ forms a subring of D, and contains the centre $\mathsf{Z}(D)$ and the element a. In §64 of [29], the following is proved:

LEMMA 2.1. *Let D be a division ring. If $f(x) \in D[x]$ is a polynomial with coefficients in $\mathsf{Z}(D)$ and irreducible over $\mathsf{Z}(D)$, then any two zeros of $f(x)$ (in D) are conjugate in D.*

That is, if $c, c' \in D$ have the same minimal polynomial over $\mathsf{Z}(D)$, then there exists $d \in D^*$ such that $dcd^{-1} = c'$.

3. *Background on projective geometry*

A *projective space* is a point-line incidence structure that is a linear space such that, given a pair of intersecting lines, every pair of lines meeting both of them, not at their point of intersection, intersect and every point lies on at least three lines and every line lies on at least three points. A *subspace* is a set of points such that, if two points of the set are collinear, then every point of the line joining them is in the set. The incidence structure of one-dimensional subspaces and two-dimensional subspaces of a left vector space V of dimension at least three over a division ring D is a projective space $\mathbb{P}V$. The subspaces of $\mathbb{P}V$ are in one-to-one correspondence with the subspaces of V. The *projective dimension* of a projective space is one less than the maximum length of a chain of subspaces if this is finite; when this is the case, the projective space is *finite-dimensional*. Indeed, $\mathbb{P}V$ is finite-dimensional if and only if V is finite-dimensional, in which case $\dim(V) = \dim(\mathbb{P}V) + 1$. In the particular case that we know the dimension $n + 1$ of V and its defining division ring D, we will often use the notation $\mathsf{PG}(n, D)$ for $\mathbb{P}V$. Each subspace of a projective space properly containing a line, when endowed with the lines it contains, is itself a projective space. The *dimension* of a subspace is -1 if the subspace is empty, 0 if the subspace is a point, 1 if the subspace is a line, and the dimension of this projective space otherwise. We call subspaces of dimension 2 *planes* and subspaces of dimension one less than that of a finite-dimensional space *hyperplanes*.

The next theorem dates from 1648, when it was first published by Abraham Bosse [7] and attributed to Girard Desargues.

THEOREM 3.1 (Desargues' theorem for projective spaces [13, pp. 206–212]). *In a projective space of dimension at least three, given triangles a, b, c and a', b', c' in perspective from a point o, the lines ab and $a'b'$ meet in a point p, the lines ac and $a'c'$ meet in a point q, the line bc and $b'c'$ meet in a point r, and p, q and r are collinear.*

Projective spaces satisfying the conclusion of Desargues' theorem are called *Desarguesian*.

COROLLARY 3.2. *In a projective space of dimension at least three, every plane is Desarguesian.*

There exist non-Desarguesian projective planes, so the condition on the dimension is necessary. The first finite non-Desarguesian projective planes were constructed in 1907 by Veblen and Wedderburn [33].

THEOREM 3.3 (Desargues' theorem for projective planes, c.f., [19, Satz 32 and 33]). *In $\mathbb{P}V$, for V a vector space over a division ring, given triangles a, b, c and a', b', c' in perspective from a point o, the lines ab and $a'b'$ meet in a point p, the lines ac and $a'c'$ meet in a point q, the lines bc and $b'c'$ meet in a point r, and p, q and r are collinear.*

THEOREM 3.4 (Converse to Desargues' theorem [19, §24–29 and Satz 35]). *If a projective space $\mathcal{S}$ of dimension at least two is Desarguesian, then $\mathcal{S}$ is isomorphic to $\mathbb{P}V$, for some vector space V over some division ring D.*

Hilbert only worked with ordered division rings. The first proofs without the assumption of order were those of Vahlen [32, Satz 137, p. 128] and Hessenberg [18].

The next theorem dates from around 340 AD, when it was proved in a different context by Pappus of Alexandria.

THEOREM 3.5 (Pappus [27, 19]). *In $\mathbb{P}V$, for V a vector space over a field F, with $\dim(\mathbb{P}V) \geqslant 2$, let l, l' be lines of $\mathbb{P}V$ meeting in the point o, let distinct points x, y, z be on l, and distinct points x', y', z' be on l', such that none of them are equal to o. Let $u = xy' \cap x'y$, $v = zx' \cap z'x$, and $w = yz' \cap y'z$. Then u, v and w are collinear.*

Projective spaces satisfying the conclusion of Pappus' theorem are called *Pappian*.

THEOREM 3.6 (Hessenberg [17]). *A Pappian projective space is Desarguesian.*

Hessenberg's proof has a flaw, as did most later proofs. See [30] for a wonderful critical treatment of all prior proofs. Cronheim's 1953 proof [9] is considered definitive.

THEOREM 3.7 (Converse to Pappus' theorem [19]). *If a projective space $\mathcal{S}$ of dimension at least two is Pappian, then $\mathcal{S}$ is isomorphic to $\mathbb{P}V$, for some vector space V over some field F.*

In [19], Hilbert needed to assume that the space was Desarguesian, as his work preceded that of Hessenberg, and he also only worked with ordered fields. The first proofs without the assumption of order were those of Vahlen [32] and Hessenberg [18], both in 1905.

Combining the above results, we obtain the following three fundamental theorems:

THEOREM 3.8 (Representation theorem for Desarguesian projective planes). *A projective plane is Desarguesian if and only if it is isomorphic to $\mathbb{P}V$ where V is a three-dimensional vector space over a division ring.*

THEOREM 3.9. *A projective space of dimension at least three is isomorphic to $\mathbb{P}V$ where V is a vector space over a division ring.*

THEOREM 3.10 (Representation theorem for Pappian projective spaces). *A projective space of dimension at least two is Pappian if and only if it is isomorphic to $\mathbb{P}V$ where V is a vector space over a field, and V has dimension at least three.*

Given three skew lines l_1, l_2, l_3 of $\mathsf{PG}(3, D)$, we define the *regulus* $\mathcal{R}(l_1, l_2, l_3)$ to be the set of transversals to these three lines. A *spread* of $\mathsf{PG}(3, D)$ is a set of lines $\mathcal{S}$ that forms a partition of the set of points of $\mathsf{PG}(3, D)$; every point is incident with precisely one element of $\mathcal{S}$. Given a quadratic extension D' of D, we can construct a spread by *division-ring reduction* as follows. Consider the points on the projective line $\mathsf{PG}(1, D')$; they are 1-dimensional subspaces of the two-dimensional (left) vector space $(D')^2$ over D'. Since D is a subring of D' we can consider a different vector space on the same ground set by only taking scalar multiplication in D. This then creates on $(D')^2$ a four-dimensional (left) vector space V over D. Each of the 1-dimensional subspaces $\langle v \rangle_{D'}$ gives rise to a 2-dimensional subspace $\langle v \rangle_D$ of V. Hence, each point of $\mathsf{PG}(1, D')$ maps to a line of $\mathsf{PG}(3, D)$ under this correspondence. Two distinct points of $\mathsf{PG}(1, D')$ have no nontrivial vectors in their intersection and so are mapped to disjoint lines of $\mathsf{PG}(3, D)$. As every nonzero vector of $(D')^2$ lies in a unique one-dimensional D'-subspace, it follows that every nonzero vector is contained in a unique two-dimensional D-subspace. Therefore, we obtain a spread $\mathcal{S}$ of $\mathsf{PG}(3, D)$.

The endomorphisms K of V that map each element of the spread $\mathcal{S}$ into itself form a ring (under component-wise addition and function composition) called the *kernel* of $\mathcal{S}$ (see [22, p. 3]). Given three lines l_1, l_2, l_3 lying in $\mathcal{S}$, it is well-known (see [22, Chapter 1, Section 1, especially p. 6]) that the multiplicative group of K acts transitively on the elements of $\mathcal{R}(l_1, l_2, l_3)$. The last geometric property of $\mathsf{PG}(3, D)$ that we will use in our proof is that this geometry has a high degree of symmetry. The projective general linear group $\mathsf{PGL}(4, D)$ provides a large group of collineations (incidence preserving permutations) of $\mathsf{PG}(3, D)$, and it is well-known[†] that $\mathsf{PGL}(4, D)$ acts transitively on triples of skew lines of $\mathsf{PG}(3, D)$.

We refer the reader to Segre's book [29], Chapter 18, for more on the theory of projective spaces over division rings (*corpora* in Segre's words).

4. *A little theory of finite division rings*

Since our strategy to prove Wedderburn's Theorem will be to take a minimal counterexample, we explore the consequences of the hypothesis that every proper subring is a field for a finite division ring. The first key observation is that for a finite division ring, every subring other than $\{0\}$ is a division ring.

LEMMA 4.1. *Suppose D is a finite non-commutative division ring such that every proper subring of D is a field. Then all maximal subfields F of D have prime degree over $\mathsf{Z}(D)$.*

Proof. Let F be a maximal subfield of D. Let a be an element of F, not in $\mathsf{Z}(D)$. Now $C_D(a)$ is a subring of D containing $\mathsf{Z}(D)$ and a, and since $a \notin \mathsf{Z}(D)$, we know that $C_D(a)$ is properly contained in D and is hence a field. Since F centralises any element of itself, it is contained in $C_D(a)$, and therefore equal to $C_D(a)$. Then $C_{D^*}(a) = F^*$ and hence the orbit $\mathcal{O}$ of a under $\mathrm{Inn}(D)$ has length $|D^* : F^*|$ (by the Orbit-Stabiliser Theorem). On the other hand, if we take the orbit of F under $\mathrm{Inn}(D)$ (in the action on subsets), we obtain an orbit of length $|D^* : N_{D^*}(F^*)|$. Since every element b of D not in $\mathsf{Z}(D)$ lies in a unique maximal

[†]It is implicit in [29, §190], but is also a straight-forward exercise for the reader.

subfield (namely $C_D(b)$), it follows that $|\mathcal{O} \cap F| = |N_{D^*}(F^*) : F^*|$, and so the value $|\mathcal{O} \cap F|$ is independent of a. Now $N_{D^*}(F^*)$ induces an automorphism group A of F fixing all elements of $\mathsf{Z}(D)$. So the size of any A-orbit on $F \setminus \mathsf{Z}(D)$ is $|\mathcal{O} \cap F|$, which is equal to the size of A. Since all orbits of A have the same length, there are no nontrivial proper subgroups of A. Therefore, $|A|$ is prime and equal to the degree of F over $\mathsf{Z}(D)$, or $|A| = 1$. We will show that the latter does not occur. Let $q_0 := |\mathsf{Z}(D)|$. By Lemma 2.1, there exists $d \in D^*$ such that $dad^{-1} = a^{q_0}$ and hence $dF^*d^{-1} = F^*$. So the inner automorphism τ given by d normalises F^*, but does not centralise F^*. That is, τ is a nontrivial element of A, and therefore, the degree of F over $\mathsf{Z}(D)$ is prime. □

THEOREM 4.2. *Suppose D is a finite division ring such that every proper subring of D is a field. Then D has odd dimension over its centre.*

Proof. Suppose, by way of contradiction, that $n = \dim_{\mathsf{Z}(D)}(D)$ is even. Let $q_0 := |\mathsf{Z}(D)|$. Consider the set $D \setminus \mathsf{Z}(D)$, of size $q_0^n - q_0$, and observe that this value is congruent[†] to 2 modulo $q_0 + 1$. If an element a in $D \setminus \mathsf{Z}(D)$ has $|C_D(a)| = q_0^m$ with m odd (dividing n), then its orbit under $\mathrm{Inn}(D)$ has length $\frac{q_0^n - 1}{q_0^m - 1}$ which is divisible[‡] by $q_0 + 1$. Thus, there exists an element a in $D \setminus \mathsf{Z}(D)$ with $|C_D(a)| = q_0^m$, m even, and hence by Lemma 4.1, $m = 2$. By Lemma 2.1, there is an element b of D with $a^{q_0} = bab^{-1}$. So

$$a = (a^{q_0})^{q_0} = (bab^{-1})^{q_0} = ba^{q_0}b^{-1} = b^2ab^{-2}.$$

Consider the set X of all (left) linear combinations of $1, a, b, ab$ over $\mathsf{Z}(D)$. We claim that X is a division ring. Now a is quadratic over $\mathsf{Z}(D)$, so there exist z_1, z_2 in $\mathsf{Z}(D)$ with $a^2 = z_1a + z_2$ and the zeros of $x^2 + z_1x + z_2$ in $C_D(a)$ are a and a^{q_0}, so $a^{q_0} = -z_1 - a$. So a^2, a^2b are in X and $ba = a^{q_0}b = (-z_1 - a)b \in X$. Now the smallest division ring containing $\mathsf{Z}(D)$, a, and b is D. We know that b^2 commutes with a and with b, so b^2 lies in $\mathsf{Z}(D)$. Thus $b^2 \in X$. Finally, $bab = (-z_1 - a)b^2 \in X$, and hence $aba = -z_1a - z_1ab - z_2b$ and $abab = -z_1ab - (b^2)a^2$. So X is a division ring, and therefore, $X = D$. Now n is even, larger than 2, and at most 4. So $n = 4$. Now all elements a of $D \setminus \mathsf{Z}(D)$ have $|C_D(a)| = q_0^2$, so have orbits of length $q_0^2 + 1$; thus no union of them can have size $q_0^4 - q_0$, a contradiction. □

PROPOSITION 4.3. *Let D be a finite division ring and let x be an element of D not in $\mathsf{Z}(D)$. Then:*

(i) *The subring $\mathsf{Z}(D)[x]$ generated by x (over $\mathsf{Z}(D)$) is a subfield of D.*
(ii) *If $x^2 + x \in \mathsf{Z}(D)$, then $\mathsf{Z}(D)[x]$ is a quadratic extension of $\mathsf{Z}(D)$.*

Proof. Let $C := \mathsf{Z}(D)[x]$. For the proof of (i), notice that the elements of the form x^i commute with other elements of the form x^j, and so clearly C is commutative. Now suppose $x^2 + x \in \mathsf{Z}(D)$. If $x \notin \mathsf{Z}(D)$ and $x^2 + x = z_0 \in \mathsf{Z}(D)$ then the minimal polynomial of x over $\mathsf{Z}(D)$ is $X^2 + X - z_0$, so $|\mathsf{Z}(D)[x] : \mathsf{Z}(D)| = 2$. □

COROLLARY 4.4. *Suppose D is a finite division ring such that every proper subring of D is a field. Then there is an element β of $\mathsf{Z}(D)$ not in $\{x^2 + x : x \in D\}$.*

[†]Note that $q_0 \equiv -1 \pmod{q_0 + 1}$ and so $q_0^n \equiv (-1)^n \equiv 1 \pmod{q_0 + 1}$ since n is even.

[‡]We have $2m \mid n$ and hence $q_0^n - 1$ is divisible by $(q_0^m - 1)(q_0^m + 1)$. Now m is odd, so $q_0 + 1$ divides $q_0^m + 1$ and hence $(q_0^m - 1)(q_0 + 1)$ divides $q^n - 1$.

Proof. By Theorem 4.2, the left degree $|D : \mathsf{Z}(D)|_L$ is odd. Suppose x is an element of D, not in the centre $\mathsf{Z}(D)$, such that $x^2 + x \in \mathsf{Z}(D)$. By Proposition 4.3, $\mathsf{Z}(D)[x]$ is a quadratic extension of $\mathsf{Z}(D)$. Now left degree of division ring extensions is multiplicative, and hence

$$|D : \mathsf{Z}(D)|_L = |D : \mathsf{Z}(D)[x]|_L \cdot |\mathsf{Z}(D)[x] : \mathsf{Z}(D)|_L = 2|D : \mathsf{Z}(D)[x]|_L$$

which is a contradiction as $|D : \mathsf{Z}(D)|_L$ is odd. Therefore, there does not exist $x \in D \setminus \mathsf{Z}(D)$ with $x^2 + x \in \mathsf{Z}(D)$. We now look to $\mathsf{Z}(D)$. The map $f : x \mapsto x^2 + x$ on $\mathsf{Z}(D)$ is not one-to-one as $f(0) = f(-1) = 0$. Since $\mathsf{Z}(D)$ is finite, f is not onto, and so it follows that there is an element β of $\mathsf{Z}(D)$ not of the form $x^2 + x$ (for any $x \in D$). □

Although the following result can be ascertained from a result in Cohn's book [8, Theorem 3.6.1 (ii) (with $\alpha = 1$, $\delta = 0$ and $\mu = -\beta$)], for reasons of self-containment, we include a fully worked and explicit proof that a finite division ring such that every proper subring of D is a field has a quadratic extension. This demonstrates the elementary nature of the facts about division rings that we use in our proof of Wedderburn's theorem.

THEOREM 4.5. *Let $(D; +, \cdot, 0, 1)$ be a finite division ring, and let $\beta \in \mathsf{Z}(D)$. Define a new algebraic structure D_β^2 on the Cartesian product D^2 equipped with the following binary operations $\oplus$ and $\circ$ on D^2:*

$$(d_1, d_2) \oplus (d_1', d_2') := (d_1 + d_1', d_2 + d_2')$$
$$(d_1, d_2) \circ (d_1', d_2') := (d_1 d_1' + d_2 d_2' \beta, d_2 d_2' + d_2 d_1' + d_1 d_2')$$

If β is not in $\{x^2 + x \colon x \in D\}$, then D_β^2 is a division ring.

Proof. Throughout, we will be using the fact that a one-sided inverse, identity, and associativity imply that a set equipped with a binary operation is a group. First we see that $(0, 0)$ is an additive identity and $(1, 0)$ is a multiplicative identity for D_β^2. At this stage, we do not know if they are unique. Clearly, $\oplus$ is commutative and associative, and if $(d_1, d_2) \in D^2$, then $(-d_1, -d_2)$ is an additive inverse of (d_1, d_2), and is in fact unique (since we know now that we have an Abelian group). The element $(1, 0)$ is a multiplicative identity, and we verify now that $\circ$ is associative. Let $(x_1, x_2), (y_1, y_2), (z_1, z_2) \in D^2$. Since β is central, we have:

$$\begin{aligned}
&(x_1, x_2) \circ ((y_1, y_2) \circ (z_1, z_2)) \\
=&(x_1, x_2) \circ (y_1 z_1 + y_2 z_2 \beta, y_2 z_2 + y_2 z_1 + y_1 z_2) \\
=&(x_1(y_1 z_1 + y_2 z_2 \beta) + x_2(y_2 z_2 + y_2 z_1 + y_1 z_2)\beta, \\
&\ x_2(y_2 z_2 + y_2 z_1 + y_1 z_2) + x_2(y_1 z_1 + y_2 z_2 \beta) + x_1(y_2 z_2 + y_2 z_1 + y_1 z_2)) \\
=&(x_1 y_1 z_1 + x_1 y_2 z_2 \beta + x_2 y_2 z_2 \beta + x_2 y_2 z_1 \beta + x_2 y_1 z_2 \beta, \\
&\ x_2 y_2 z_2 + x_2 y_2 z_1 + x_2 y_1 z_2 + x_2 y_1 z_1 + x_2 y_2 z_2 \beta + x_1 y_2 z_2 + x_1 y_2 z_1 + x_1 y_1 z_2) \\
=&((x_1 y_1 + x_2 y_2 \beta) z_1 + (x_2 y_2 + x_2 y_1 + x_1 y_2) z_2 \beta, \\
&\ (x_2 y_2 + x_2 y_1 + x_1 y_2) z_2 + (x_2 y_2 + x_2 y_1 + x_1 y_2) z_1 + (x_1 y_1 + x_2 y_2 \beta) z_2) \\
=&(x_1 y_1 + x_2 y_2 \beta, x_2 y_2 + x_2 y_1 + x_1 y_2) \circ (z_1, z_2) \\
=&((x_1, x_2) \circ (y_1, y_2)) \circ (z_1, z_2).
\end{aligned}$$

Therefore, $\circ$ is associative. We leave left-distributivity and right-distributivity to the reader, but we will finish by showing that every nonzero element has a multiplicative inverse. Let $(d_1, d_2) \in D^2$ such that $(d_1, d_2) \neq (0, 0)$. We have two cases: $d_1 = 0$ and $d_1 \neq 0$. In the first case, when $d_1 = 0$, we note that $(0, d_2)$ has inverse $(d_2^{-1}\beta^{-1}, -d_2^{-1}\beta^{-1})$. Now suppose $d_1 \neq 0$.

Let

$$(e_1, e_2) := \left(d_1^{-1} + d_1^{-1}C^{-1}\beta, -d_2^{-1}C^{-1}\right).$$

where $C = (d_1 d_2^{-1})^2 + (d_1 d_2^{-1}) - \beta$. By assumption, $C \neq 0$ since $\beta \neq x^2 + x$ for all $x \in D$, and $x = d_1 d_2^{-1}$ is such an instance. Then

$$\begin{aligned}(d_1, d_2) \circ (e_1, e_2) =& (d_1 e_1 + d_2 e_2 \beta, d_2 e_2 + d_2 e_1 + d_1 e_2)\\ =& (d_1(d_1^{-1} + d_1^{-1}C^{-1}\beta) - d_2 d_2^{-1} C^{-1}\beta,\\ & - d_2 d_2^{-1} C^{-1} + d_2(d_1^{-1} + d_1^{-1}C^{-1}\beta) - d_1 d_2^{-1} C^{-1})\\ =& (1, (-1 + d_2 d_1^{-1}\beta - d_1 d_2^{-1})C^{-1} + d_2 d_1^{-1})\\ =& (1, -d_2 d_1^{-1} C C^{-1} + d_2 d_1^{-1})\\ =& (1, 0).\end{aligned}$$

Therefore, (d_1, d_2) has a multiplicative inverse. So we have shown that D_β^2 is a division ring. □

COROLLARY 4.6. *Every finite division ring D such that every proper subring of D is a field has a quadratic extension.*

Proof. The result follows from Theorem 4.5, Proposition 4.3, and Corollary 4.4, again using the fact that the left degree of division ring extensions is multiplicative (and hence D contains no quadratic extension of $\mathsf{Z}(D)$). □

5. *Applying the Dandelin–Gallucci Theorem*

THEOREM 5.1. *Let D be a finite division ring such that every proper subring of D is a field. Take any three lines l, m, n in $\mathsf{PG}(3, D)$ that are pairwise skew. Let $\mathcal{R}$ be the set of transversals to l, m, and n. Then any point P of a line of $\mathcal{R}$ lies on a transversal to $\mathcal{R}$.*

Proof. Let P be a point lying on a line of $\mathcal{R}$. By Corollary 4.6, there exists a quadratic extension D' of D. Hence, we obtain a spread $\mathcal{S}$ of $\mathsf{PG}(3, D)$, by *division-ring reduction* to the points of $\mathsf{PG}(1, D')$. Since $\mathsf{PGL}(4, D)$ is transitive on triples of skew lines, we may assume that l, m, n lie in $\mathcal{S}$. But now the multiplicative group G of the kernel of the spread acts transitively on the points on each element of $\mathcal{S}$ [**22**, Chapter 1, Section 1, especially the paragraph between Theorem 1.2 and Theorem 1.3], and hence on $\mathcal{R}$. The orbit of P under G is a line s of $\mathcal{S}$. Since G fixes l, m, and n, we have that $\mathcal{R}$ is G-invariant, and therefore, every point of s is on a line of $\mathcal{R}$. Finiteness (of D) now ensures that s is a transversal to $\mathcal{R}$ through P. Hence any point P on a line of $\mathcal{R}$ lies on a transversal to $\mathcal{R}$. □

Proof of Wedderburn's Theorem. Take a minimal counterexample D to Wedderburn's Theorem. Then every proper subring of D is a field. Applying the Dandelin–Gallucci Theorem 1.2 to the conclusion of Theorem 5.1, we see that D is a field, in contradiction to our hypothesis that D was a minimal counterexample. □

Recall, from Section 3, Hessenberg's Theorem 3.6 that a Pappian projective space is Desarguesian. The first person to give a geometric proof of the following theorem, which is the converse of Hessenberg's theorem under the hypothesis of finiteness, was Tecklenburg in 1987 [**31**]. The usual proof is to apply the 1905 algebraic result of Wedderburn [**24**]; we instead deduce it as a corollary of Theorem 5.1.

THEOREM 5.2. *A finite Desarguesian projective space is Pappian.*

Proof. Since a Desarguesian projective plane can be embedded in a 3-dimensional projective space, it is sufficient to prove this in the 3-dimensional case. Let π be a plane, A, B, C be collinear points of π on a line l, A', B', C' be distinct points of π on another line l', with A, B, C, A', B', C' distinct from $l \cap l'$. Choose skew lines a and b with $a \cap \pi = A$ and $b \cap \pi = B$. Let a' be the transversal to a and b on A', b' be the transversal to a and b on B', c' be the transversal to a and b on C'. Let c be the transversal to a' and b' on C. Then, by Theorem 5.1, c and c' meet. Now consider the skew hexagon with sides $ab'ca'bc'$. Intersecting pairs of planes that correspond to opposite vertices in this skew hexagon give the three lines that can be obtained by joining the three points $a' \cap c$, $b' \cap a$, $c' \cap b$, and so these lines lie in the plane π' spanned by these three points. (To see this, consider the planes $\langle a, a' \rangle$ and $\langle b', c \rangle$: their intersection contains $a' \cap c$ and $a \cap c'$; consider the planes $\langle a', b \rangle$ and $\langle c, c' \rangle$: their intersection contains $a' \cap c$ and $b \cap c'$; consider the planes $\langle b, b' \rangle$ and $\langle c', a \rangle$: their intersection contains $b \cap c'$ and $a \cap b'$.)

Each side of the hexagon $AB'CA'BC'$ lies in a plane corresponding to a vertex of the skew hexagon, so the intersections of the opposite sides lie in π'. Hence the intersections of opposite sides of $AB'CA'BC'$ lie in the line $\pi \cap \pi'$; that is, they are collinear. □

A purely geometric proof by Baldwin and Howard of the embedding of a Desarguesian projective plane in 3-space is given in [**3**, Appendix]. This proof does not rely upon the representation theorem of Desarguesian planes by division rings. It builds on the earlier proof by Levi (1939) [**21**]. Levi's proof is also purely geometric. Hilbert (1899) [**19**] proved this under the assumption that the plane was ordered; the first proof without assuming order is due to Vahlen (1905) [**32**, Satz 137, p. 128].

We note that the proof above can be adapted to prove Pascal's theorem, by choosing π to meet the lines of a regulus in a conic, which is an idea which goes back to Dandelin.

Note that Theorem 5.2 also gives a proof of Wedderburn's theorem without citing the Dandelin–Gallucci theorem, since a projective plane is Pappian if and only if it is coordinatised by a field, by Theorem 3.10.

Acknowledgements

The authors are indebted to the referee for their close reading of the paper. The first author acknowledges the support of the Australian Research Council Future Fellowship FT120100036.

References

1. M. Adam and B. J. Mutschler. On Wedderburn's theorem about finite division algebras. http://www.math.uni-bielefeld.de/LAG/man/, 2003.
2. H. F. Baker. *Principles of geometry. Volume 1. Foundations.* Cambridge Library Collection. Cambridge University Press, Cambridge, 2010. Reprint of the 1922 original.
3. J. T. Baldwin. Formalization, primitive concepts, and purity. *Rev. Symb. Log.*, 6(1):87–128, 2013.
4. A. S. Bang. Taltheoretiske undersølgelser. *Tidskrift f. Math*, 5:70–80 and 130–137, 1886.
5. A. Beutelspacher and U. Rosenbaum. *Projective geometry: from foundations to applications.* Cambridge University Press, Cambridge, 1998.
6. G. D. Birkhoff and H. S. Vandiver. On the integral divisors of $a^n - b^n$. *Ann. of Math. (2)*, 5(4):173–180, 1904.

7. A. Bosse. *Manière universelle de Mr Desargues pour pratiquer la perspective par petit-pied comme la géometral. Ensembles les places et proportions les fortes et foibles touches, teintes et couleurs.* Pierre Des-Hayes, Paris, 1648.
8. P. M. Cohn. *Skew fields*, volume 57 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1995. Theory of general division rings.
9. A. Cronheim. A proof of Hessenberg's theorem. *Proc. Amer. Math. Soc.*, 4:219–221, 1953.
10. G. Dandelin. *Mémoire sur quelques propriétés remarquables de la focale parabolique.* Nouveaux mémoires de l'Académie Royale des Sciences et Belles-Lettres de Bruxelles, 1822.
11. G. Dandelin. Géométrie pure. Recherches nouvelles sur les sections du cône et sur les hexagones inscrits et circonscrits à ces sections. *Ann. Math. Pures Appl.*, 15:387–396, 1824/25.
12. G. Dandelin. *Mémoire sur l'hyperboloïde de révolution, et sur les hexagones de Pascal et de M. Brianchon.* Nouveaux mémoires de l'Académie Royale des Sciences et Belles-Lettres de Bruxelles, 1826.
13. G. Desargues. *L'oeuvre mathématique de Desargues (ed. by René Taton)*. Presses Universitaires de France, Paris, 1951.
14. L. E. Dickson. On the Cyclotomic Function. *Amer. Math. Monthly*, 12(4):86–89, 1905.
15. G. Gallucci. Studio della figura delle otto rette e sue applicazioni alla geometria del tetraedro ed alla teoria delle configurazioni. *Rendiconto dell'Accademia delle scienze fisiche e matematiche (Sezione della Societá reale di Napoli)*, 12:49–79, 1906.
16. D. W. Henderson. A short proof of Wedderburn's theorem. *The American Mathematical Monthly*, 72(4):385–386, 1965.
17. G. Hessenberg. Beweis des Desarguesschen Satzes aus dem Pascalschen. *Math. Ann.*, 61(2):161–172, 1905.
18. G. Hessenberg. Über einen geometrischen Calcül (Verknüpfungs-Calcül). *Acta Math*, 29:1–23, 1905.
19. D. Hilbert. *Grundlagen der Geometrie.* Teubner, Leipzig, 1899.
20. N. Jacobson. *Structure of rings.* American Mathematical Society Colloquium Publications, Vol. 37. Revised edition. American Mathematical Society, Providence, R.I., 1964.
21. F. W. Levi. On a fundamental theorem of geometry. *J. Indian Math. Soc.*, 3:182–192, 1939.
22. H. Lüneburg. *Translation planes.* Springer-Verlag, Berlin-New York, 1980.
23. H. Lüneburg. Projektive Geometrie. http://arxiv.org/abs/1106.5691, 2011. edited by Theo Grundhoefer and Karl Strambach.
24. J. H. Maclagan-Wedderburn. A theorem on finite algebras. *Trans. Amer. Math. Soc.*, 6(3):349–352, 1905.
25. K. McCrimmon. A note on finite division rings. *Proc. Amer. Math. Soc.*, 23:598–600, 1969.
26. D. L. Outcalt and A. Yaqub. A generalization of Wedderburn's theorem. *Proc. Amer. Math. Soc.*, 18:175–177, 1967.
27. Pappus. *Book 7 of the Collection*, volume 8 of *Sources in the History of Mathematics and Physical Sciences*. Springer-Verlag, New York, 1986. Part 1. Introduction, text, and translation, Part 2. Commentary, index, and figures, Edited and with translation and commentary by Alexander Jones.
28. K. H. Parshall. In pursuit of the finite division algebra theorem and beyond: Joseph H. M. Wedderburn, Leonard E. Dickson, and Oswald Veblen. *Arch. Internat. Hist. Sci.*, 33(111):274–299 (1984), 1983.
29. B. Segre. *Lectures on modern geometry*, volume 7 of *Consiglio Nazionale delle Rierche Monografie Matematiche*. Edizioni Cremonese, Rome, 1961.
30. A. Seidenberg. Pappus implies Desargues. *Amer. Math. Monthly*, 83(3):190–192, 1976.
31. H. Tecklenburg. A proof of the theorem of Pappus in finite Desarguesian affine planes. *J. Geom.*, 30(2):172–181, 1987.
32. T. Vahlen. *Abstrakte Geometrie. Untersuchungen über die Grundlagen der Euklidischen und nicht-Euklidischen Geometrie.* S. Hirzel, Leipzig, 1940. Zweite, neubearbeitete Auflage. Zweites Beiheft zu Deutsche Mathematik.
33. O. Veblen and J. H. Maclagan-Wedderburn. Non-Desarguesian and non-Pascalian geometries. *Trans. Amer. Math. Soc.*, 8(3):379–388, 1907.
34. E. Witt. Über die Kommutativität endlicher Schiefkörper. *Abh. Math. Sem. Univ. Hamburg*, 8(1):413, 1931.
35. K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math. Phys.*, 3(1):265–284, 1892.

John Bamberg,
Centre for the Mathematics
of Symmetry and Computation,
School of Mathematics and Statistics,
The University of Western Australia
35 Stirling Highway, Crawley, W.A. 6009,
Australia.
john.bamberg@uwa.edu.au

Tim Penttila,
Department of Mathematics
Colorado State University
Fort Collins, CO 80523-1874,
USA.
penttila@math.colostate.edu