Variations on a theme of Glauberman

Tim Penttila [*] Alessandro Siciliano[†]

April 14, 2021

Abstract

A new and elementary proof of the Artin-Zorn theorem that finite alternative division rings are fields is given. The characterisation of finite fields of Glauberman and Heimbeck is also extended to a broader class of fields, the two subjects being connected via geometry.

1 Introduction

In 1905, Wedderburn [29] proved that *a finite (associative) division ring is a field* – a result now known as *Wedderburn's little theorem.* A recent proof was given by Bamberg and Penttila [2], which exploited the connection with geometry – that the theorem is equivalent to the statement that *a finite Desarguesian projective space is Pappian.* Artin proved a stronger theorem, first published by his student Zorn in 1931 [30] and now known as the *Artin-Zorn theorem*: *a finite alternative division ring is a field.* It, too, has an equivalent geometric counterpart, first stated by Levi in 1942 [19, Sixth lecture]: *a finite projective plane satisfying little Desargues' theorem is Pappian.* The connection between alternative division rings and projective planes satisfying the special case of Desargues' theorem known as little Desargues' theorem (where the point of perspective is incident with the line of perspective) first

[*] Tim Penttila: penttila86@msn.com
School of Mathematical Sciences, The University of Adelaide, Adelaide, South Australia, 5005 Australia

[†] Alessandro Siciliano: alessandro.siciliano@unibas.it
Dipartimento di Matematica, Informatica ed Economia, Università degli Studi della Basilicata, I-85100 Potenza, Italy

arose in work of Moufang [21] (but she credits Brauer for pointing this out to her: see [7, p.333]) and, as a consequence, projective planes satisfying little Desargues' theorem are now called *Moufang planes*.

On another topic, in his 1972 exploration of p-stability and the control of strong fusion in finite groups, Glauberman [12] had occasion to use the following characterisation of finite fields of odd order: *a subset S of invertible matrices over finite field of odd order containing the identity matrix forms, together with the zero matrix, a field under matrix addition and matrix multiplication if and only if S is closed under inversion and $S \cup \{0\}$ is closed under addition and scalar multiplication.* In 1984, Heimbeck [16] gave an elementary proof of Glauberman's characterisation and also extended it to fields of even order (while additionally dropping the condition about closure under scalar multiplication). Glauberman's original proof was not elementary, involving, for instance, results on Jordan algebras due to McCrimmon [20] and Albert [1]. Despite having used arguments from Section 11 of Bruck-Bose [4] in the earlier paper [11], Glauberman failed to notice that the conditions he used to characterise finite fields of odd order had arisen in that section in connection with Moufang planes.

This paper exploits the connection between three areas: group theory, projective geometry and the theory of alternative division rings, to give a new and elementary proof of the Artin-Zorn theorem that finite alternative division rings are fields (see Sections 3, 4). We note that the "standard" proof of Artin-Zorn is also elementary; see [24].

The corresponding result in projective geometry is that a finite Moufang plane satisfies Pappus theorem. In fact, while the inspiration is geometric, the proofs are written so as to require no geometry. This connection does not depend on finiteness, which allows the extension of the Glauberman-Heimbeck result in the case where the dimension of the set $S \cup \{0\}$ is maximal to a broader class of fields (see Section 5). In particular, by exploiting the Bruck-Kleinfeld-Skornyakov-San Soucie theorem that Moufang planes (finite or infinite) are coordinatised by fields or octonion algebras, the Glauberman-Heimbeck result can be extended to algebraically closed fields, to complete, discretely valued fields with finite residue class field, and to perfect fields with cohomological dimension at most two.

Special care must be taken with $8m$ by $8m$ matrices, as there is a connection with non-associative alternative division rings. All examples of sets of matrices of maximal dimension satisfying Glauberman's conditions over a general field that are not themselves associative division rings are also characterised (Theorem 5.7) by using the Bruck-Kleinfeld-Skornyakov classification of alternative division rings (Theorem 2.7).

The results contained in this paper are in a similar vein to the results by Bamberg and Penttila [2] and Penttila and Siciliano [22] (proving that a finite Bol field of even order is a nearfield without using the Feit-Thomson theorem that group of odd order are soluble), both also obtained using the underlying connections between the three areas.

2 Background on alternative division rings

A (not necessarily associative) **division ring** is a set A endowed with two operations, addition and multiplication that is an abelian group under addition, satisfies both distributive laws, has a multiplicative identity $1 \neq 0$ and such that, for all $a, b \in A$, with $a \neq 0$, the equation $ax = b$ has a unique solution $x \in A$ and the equation $xa = b$ has a unique solution $x \in A$. A (not necessarily associative) division ring has the **left inverse property** if whenever $x \in A$, $x \neq 0$, then $y = x^{-1}(xy)$, for all $y \in A$. An **alternative ring** is an abelian group A under addition, together with a product which satisfies both distributive laws, and such that $a(ab) = (aa)b$ and $(ba)a = b(aa)$, for all $a, b \in A$. (Note that multiplication need not be associative.)

The **centre** of a (not necessarily associative) ring A is the set $Z(A)$ of all elements a of A such that $(ab)c = a(bc), (ba)c = b(ac), b(ca) = (bc)a$, and $ab = ba$, for all $b, c \in A$. Note that the centre of an alternative division ring is a field. The **characteristic** of an alternative division ring is the characteristic of its centre.

An **involution** in a ring A is an anti-automorphism (so that it preserves addition and reverses multiplication) with square the identity. An involution $a \mapsto \overline{a}$ of a ring A is **central** if both $a\overline{a}$ and $a + \overline{a}$ lie in the centre of A, for all $a \in A$.

Non-associative alternative rings date back to the construction of the octonions, which Graves, in a letter of 26 December, 1843 to Hamilton, described in response to Hamilton's construction of the quaternions on 16 October, 1843, which Hamilton in turn had described in a letter to Graves the day after Hamilton had constructed them. This led to the coining of the term *associative*, either by Graves or by Hamilton in 1843 or 1844. Graves did not publish the result until 1845, by which time it had been independently discovered by Cayley [6]. In 1914, Dickson [9, p.15] recontextualised the octonions by constructing them as pairs of quaternions, much as Hamilton had recontextualised the complex numbers as pairs of real numbers in 1835 [15]. This method is now referred to as the *Cayley-Dickson process.*

Given a ring A with identity and with a central involution $a \mapsto \overline{a}$, fix an element ζ of the centre of A such that $\overline{\zeta} = \zeta$. Define A' to have underlying set $A \times A$ with addition

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$$

and multiplication

$$(a_1, a_2)(b_1, b_2) = (a_1 b_1 + \zeta b_2 \overline{a_2}, \overline{a_1} b_2 + b_1 a_2).$$

We say that A' is obtained from A by **the Cayley-Dickson process**.

Lemma 2.1 ([10, Lemma 4.8])**.** *Suppose that A' is obtained from A by the Cayley-Dickson process via the central involution $a \mapsto \overline{a}$. Then*
(i) A' is an alternative ring if and only if A is associative.
(ii) A' is an associative ring if and only if A is associative and commutative.
(iii) A' is a commutative ring if and only if the involution of A used was the identity.
Moreover, $(a_1, a_2) \mapsto (\overline{a_1}, -a_2)$ is a central involution of A'.

So Hamilton's [15] construction of the complex numbers can be described as applying the Cayley-Dickson process to the real numbers with the identity involution and $\zeta = -1$. If the Cayley-Dickson process is applied to the complex numbers with complex conjugation as the involution and $\zeta = -1$, the result is Hamilton's quaternions. If the Cayley-Dickson process is applied to the quaternions with conjugation of quaternions as the involution and $\zeta = -1$, the result is Graves' (and Cayley's) octonions. Moreover, the octonions are a non-associative alternative division ring.

An **octonion algebra** over a field F is the result of applying the Cayley-Dickson process twice to a separable quadratic extension of F (with the intermediate result being a **quaternion algebra** over F). We take the quadratic extension, rather then applying the Cayley-Dickson process three times to F, in order to include characteristic 2.

Artin conjectured that octonion algebras are alternative rings, and this was proved by his student Zorn in 1931 [30].

Theorem 2.2. *An octonion algebra is an alternative ring.*

The octonion algebra constructed from a quaternion algebra by the Cayley-Dickson process with $\zeta = 1$ is not a division ring. Octonion algebras of this form are called **split**.

Theorem 2.3 ([10, Theorems 4.9, 4.10])**.** *An octonion algebra is either split or an alternative division ring.*

We will also need the following lemma. Indeed, it is vital to our approach.

Lemma 2.4 ([10, Lemma 4.6])**.** *In an alternative ring A with identity the following are equivalent:*

(a) left multiplication by a is invertible with inverse left multiplication by b;

(b) right multiplication by a is invertible with inverse right multiplication by b;

(c) $ab = ba = 1$ and $(ab)c = a(bc)$, for all $c \in A$.

When any of the conditions of Lemma 2.4 hold, we say that a is **invertible** with **inverse** $a^{-1} = b$.

Corollary 2.5. *In an alternative division ring, all non-zero elements are invertible.*

We note that a unit in a ring is not necessarily invertible, unless the ring is alternative.

Theorem 2.6 ([8, 3.1.22],[14, p.81], [17, Theorem 6.17])**.** *In an alternative division ring A, if $x \in A, x \neq 0$, then $y = x^{-1}(xy)$, for all $y \in A$.*

The following theorem was proved for characteristic not equal to two or three by Skornyakov [26], for characteristic not equal to two by Bruck-Kleinfeld [5] and for characteristic two by Kleinfeld [18].

Theorem 2.7 (Bruck-Kleinfeld-Skornyakov Theorem, [10, Theorem 4.13])**.** *An alternative division ring is either associative or an octonion algebra over its centre.*

The following theorem was proved by Skornyakov [27] for characteristic not two and San Soucie [23] for characteristic two. For this theorem, we're going to need to extend the concept of a division ring to non-associative rings. Theorem 2.6 shows that an alternative division ring has the left inverse property. The converse also holds:

Theorem 2.8 (Skornyakov-San Soucie Theorem, [17, Theorem 6.16])**.** *A (not necessarily associative) division ring that has the left inverse property is alternative.*

3 Glauberman's characterisation of finite fields of odd order and its extension by Heimbeck

Theorem 3.1 ([12, Lemma 4.3])**.** *A subset S of the n by n invertible matrices over a finite field of odd order containing the identity matrix forms, together with the zero matrix, a field under matrix addition and matrix multiplication if and only if S is closed under inversion and $S \cup \{0\}$ is closed under addition and scalar multiplication.*

Theorem 3.2 (Glauberman-Heimbeck Theorem, [16])**.** *Let $V \neq \{0\}$ be a finite vector space and M be a subset of* $\mathrm{GL}(V)$ *which is closed under inverses, has $M \cup \{0\}$ closed under addition and contains the identity. Then $M \cup \{0\}$ is a field.*

Proof. We give the proof of Heimbeck [16] to keep the paper self-contained.

Since V is finite, the underlying associative division ring K of V is finite of characteristic $p > 0$. Let $L = M \cup \{0\}$. Then L is an abelian group under addition of exponent equal to p, a prime number. We denote the subgroup of $\mathrm{GL}(V)$ generated by a subset X by $\langle X \rangle$. We proceed by a sequence of observations.

a) $\alpha, \beta \in M$ implies $\alpha\beta\alpha \in M$.

We may assume that $\alpha \neq \beta^{-1}$. Then $\alpha - \beta^{-1} \in M$ and also $-\alpha^{-1} + (\alpha - \beta^{-1})^{-1} =$

$$(-\alpha^{-1}(\alpha - \beta^{-1}) + 1)(\alpha - \beta^{-1})^{-1} = \alpha^{-1}\beta^{-1}(\alpha - \beta^{-1})^{-1} = ((\alpha - \beta^{-1})\beta\alpha)^{-1} =$$

$(\alpha\beta\alpha - \alpha)^{-1}$ is an element of M. Thus $\alpha\beta\alpha - \alpha \in M$, so $\alpha\beta\alpha \in M$.

b) $\alpha \in M$ implies $\langle \alpha \rangle \in M$.

Put $\beta = 1 \in M$ in a). Then $\alpha^2 \in M$. It now follows from a) that $\alpha^n \in M$, for all natural numbers n. Since $\langle \alpha \rangle$ is finite, this completes the proof of b).

c) $\alpha, \beta, \gamma \in M$ implies $\alpha\beta + \beta\alpha \in L$ and $\alpha\beta\gamma + \gamma\beta\alpha \in L$.

Since L is a group under addition, it follows from a) that $\alpha\beta\gamma + \gamma\beta\alpha = (\alpha + \gamma)\beta(\alpha + \gamma) - \alpha\beta\alpha - \gamma\beta\gamma \in L$. Setting $\gamma = 1$ gives $\alpha\beta + \beta\alpha \in L$.

d) For $\alpha, \beta \in M$ and integers $\epsilon_0, \dots, \epsilon_r, \eta_0, \dots, \eta_r$, we have

$$\prod_{i=0}^{r}(\alpha^{\epsilon_i}\beta^{\eta_i}) + \prod_{i=0}^{r}(\beta^{\eta_{r-i}}\alpha^{\epsilon_{r-i}}) \in L.$$

We prove this by induction on r. The case $r = 0$ follows from b) and c). Using the fact that L is a group under addition, c) and the following calculation completes the proof of d).

$$\alpha^{\epsilon_0}(\alpha^{\epsilon_{r+1}}\beta^{\eta_r}\alpha^{\epsilon_r}\beta^{\eta_{r-1}}\dots\alpha^{\epsilon_1}\beta^{\eta_0} + \beta^{\eta_0}\alpha^{\epsilon_1}\dots\beta^{\eta_{r-1}}\alpha^{\epsilon_r}\beta^{\eta_r}\alpha^{\epsilon_{r+1}})\beta^{\eta_{r+1}}$$

$$+\beta^{\eta_{r+1}}(\alpha^{\epsilon_{r+1}}\beta^{\eta_r}\alpha^{\epsilon_r}\beta^{\eta_{r-1}}\dots\alpha^{\epsilon_1}\beta^{\eta_0} + \beta^{\eta_0}\alpha^{\epsilon_1}\dots\beta^{\eta_{r-1}}\alpha^{\epsilon_r}\beta^{\eta_r}\alpha^{\epsilon_{r+1}})\alpha^{\epsilon_0}$$

$$= (\alpha^{\epsilon_0+\epsilon_{r+1}}\beta^{\eta_r}\alpha^{\epsilon_r}\beta^{\eta_{r-1}}\dots\alpha^{\epsilon_1}\beta^{\eta_0+\eta_{r+1}} + \beta^{\eta_0+\eta_{r+1}}\alpha^{\epsilon_1}\dots\beta^{\eta_{r-1}}\alpha^{\epsilon_r}\beta^{\eta_r}\alpha^{\epsilon_0+\epsilon_{r+1}})$$

$$+(\alpha^{\epsilon_0}\beta^{\eta_0}\alpha^{\epsilon_1}\beta^{\eta_1}\dots\alpha^{\epsilon_{r+1}}\beta^{\eta_{r+1}} + \beta^{\eta_{r+1}}\alpha^{\epsilon_{r+1}}\dots\beta^{\eta_1}\alpha^{\epsilon_1}\beta^{\eta_0}\alpha^{\epsilon_0}).$$

e) If the elements of M pairwise commute under multiplication, then L is a field.
We have only to show that M is closed under multiplication. Let $\alpha, \beta \in M$.
Case 1. $p \neq 2$. From c), $2\alpha\beta = \alpha\beta + \beta\alpha \in L$ giving $\alpha\beta \in L$. Since $\alpha, \beta \in M$, they are invertible, so $\alpha\beta \neq 0$, giving $\alpha\beta \in M$.
Case 2. $p = 2$. By b) and the fact that L is a group under addition, the subring of the endomorphism ring of V generated by α is a field, necessarily of even order. Hence α has odd multiplicative order, and so, there exists $\gamma \in L$ with $\gamma^2 = \alpha$. Now $\alpha\beta = \gamma^2\beta = \gamma\beta\gamma \in M$, by a).

We now complete the proof of the theorem by induction on the dimension n of V. If $n = 1$, then $\mathrm{GL}(V)$ is isomorphic to the multiplicative group of K, and K is a field, by Wedderburn's little theorem, so the elements of M pairwise commute under multiplication. Thus, by e), L is a field. Now suppose $n > 1$ and that the theorem holds for finite vector spaces of dimension less then n over their underlying associative division ring. By e), it is enough to show that any pair α, β of elements of M commute under multiplication.

Case 1. $\langle \alpha, \beta \rangle$ leaves a non-trivial, proper subspace U of V invariant. Let $M_U = \{\gamma \in M \colon U^\gamma = U\}$. For $\gamma \in M_U$ the restriction $\overline{\gamma}$ to U of γ is in $GL(U)$. The system $\overline{M} = \{\overline{\gamma} \colon \gamma \in M_U\}$ therefore satisfies the hypotheses of the theorem, and so, by our inductive hypothesis forms a field. Since the multiplicative group of a finite field is cyclic, there exists $\gamma \in M_U$ with

$\overline{M} = \langle \overline{\gamma} \rangle$. For every $\delta \in M_U$, there is an integer k with $\overline{\delta} = \overline{\gamma}^k$. From b) and the fact that L is a group under addition, it follows that $\delta - \gamma^k \in L$ and then since $\delta - \gamma^k$ has kernel containing U, it is not invertible, so $\delta - \gamma^k = 0$. Thus $\delta = \gamma^k \in \langle \gamma \rangle$. Hence $\alpha, \beta \in M_U \subseteq \langle \gamma \rangle$, and therefore, $\alpha\beta = \beta\alpha$.

Case 2. $\langle \alpha, \beta \rangle$ acts irreducibly on V. Since a finite integral domain is a division ring, which by Wedderburn's little theorem is a field, it is sufficient to show that the subring R of the endomorphism ring of V generated by $\langle \alpha, \beta \rangle$ has no zero divisors. So suppose u is a zero divisor of R. As $u \in \langle \alpha, \beta \rangle$, it can be written as a sum of elements u_i of $\langle \alpha, \beta \rangle$: $u = \sum_{i=1}^{s} u_i$. Each summand u_i has a representation of the form

$$u_i = \prod_{j=0}^{r_i} (\alpha^{\epsilon_{ij}} \beta^{\eta_{ij}}),$$

for some positive integer r_i and some integers ϵ_{ij}, η_{ij}. We set

$$u_i' = \prod_{j=0}^{r_i} (\beta^{\eta_{i,r_i-j}} \alpha^{\epsilon_{i,r_i-j}}),$$

for $1 \leq i \leq s$, and

$$u' = \sum_{i=1}^{s} u_i',$$

and claim that

$$u + u' \in L, \tag{1}$$

and that

$$u\gamma u' = 0, \tag{2}$$

for all $\gamma \in \langle \alpha \rangle \cup \langle \beta \rangle$. The first claim follows from d) and the fact that L is a group under addition. To prove the second claim we first note that

$$u\gamma u' = \sum_{i=1}^{s} u_i \gamma u_i' + \sum_{i<j} (u_i \gamma u_j' + u_j \gamma u_i').$$

The summands $u_i \gamma u_i'$ and $u_i \gamma u_j' + u_j \gamma u_i'$ lie in L by a) and d). Since L is a group under addition, it follows that $u\gamma u' \in L$. Since u is a zero divisor of R it doesn't lie in $\mathrm{GL}(V)$, so neither does $u\gamma u'$. Hence $u\gamma u' = 0$.

Let $\gamma \in \langle\alpha\rangle \cup \langle\beta\rangle$. In the case where $u+u'=0$, we have $\gamma u - u\gamma = \gamma u + u'\gamma$, which is in L, by d) and the fact that L is a group under addition. By (2), $(\gamma u - u\gamma)^2 = 0$. So $\gamma u - u\gamma \notin \mathrm{GL}(V)$, which forces $\gamma u - u\gamma = 0$. Thus $\gamma u = u\gamma$. Hence the image of u is $\gamma-$invariant for all $\gamma \in \langle\alpha\rangle \cup \langle\beta\rangle$. Thus the image of u is $\langle\alpha,\beta\rangle-$invariant. Since u is a zero divisor on R, the image of u is not V, and so it is $\{0\}$, and therefore $u = 0$.

In the case where $u+u' \neq 0$, we have $u+u' \in M$ and hence $u+u' \in \mathrm{GL}(V)$. By 2 with $\gamma = 1$, we get $uu' = 0$. Thus the image of u is contained in the kernel of u'. Since $u + u' \in \mathrm{GL}(V)$, the kernel of u and the kernel of u' meet just in $\{0\}$, so, by dimensions, the image of u equals to kernel of u'. But now (2) shows that the image of u is $\gamma-$invariant for all $\gamma \in \langle\alpha\rangle \cup \langle\beta\rangle$. Thus the image of u is $\langle\alpha,\beta\rangle-$invariant. Since u is a zero divisor on R, the image of u is not V, and so it is $\{0\}$, and therefore $u = 0$.

Thus R has no zero divisors. □

To help the exposition below, we introduce the name a **Glauberman-Heimbeck set** over the field F for a subset S of the n by n invertible matrices over F containing the identity matrix such that S is closed under inversion and $S \cup \{0\}$ is closed under both addition and multiplication by elements of F, for some n. We will also call n the **degree** of the Glauberman-Heimbeck set S. The **dimension** of a Glauberman-Heimbeck set S is the dimension of $S \cup \{0\}$ as a vector space over F. Glauberman-Heimbeck sets of degree equal to their dimension play a special role in the sequel.

4 An elementary proof of the Artin-Zorn theorem

We denote left multiplication by an element a of a (not necessarily associative) ring A by ℓ_a, and the set $\{\ell_a : a \in A\}$ by $L(A)$.

Theorem 4.1. *Let A be a (not necessarily associative) ring with identity. Then A is associative if and only if $L(A)$ is closed under composition.*

Proof. If A is associative, then $(ab)c = a(bc)$, for all $a, b, c \in A$, so $\ell_{ab} = \ell_a \ell_b$, for all $a, b \in A$, and hence $L(A)$ is closed under composition. Conversely, if $L(A)$ is closed under composition, then , for all $a, b \in A$, $\ell_a \ell_b = \ell_d$, for some $d \in A$, and hence $a(bc) = dc$, for all $c \in A$. Putting $c = 1$, we have $a(b1) = d1$, that is, $ab = d$. So $\ell_{ab} = \ell_a \ell_b$, for all $a, b \in A$, giving $(ab)c = a(bc)$, for all $a, b, c \in A$. □

Theorem 4.2. *Let A be an alternative division ring. Then $L(A)$ is closed under addition and under inverses of non-zero elements.*

Proof. The distributive law $(a + b)c = ac + bc$, for all $a, b, c \in A$, implies $\ell_{a+b} = \ell_a + \ell_b$, for all $a, b, c \in A$. Thus $L(A)$ is closed under addition. Let $a \in A$ with $a \neq 0$. Then ℓ_a is invertible with inverse $\ell_{a^{-1}}$, by Lemma 2.4. Hence $L(A)$ is closed under inverses of non-zero elements. □

Theorem 4.3 (Artin-Zorn Theorem)**.** *A finite alternative division ring is a field.*

Proof. For any given finite alternative division ring A, $Z(A)$ is a field, and elements of $L(A)$ are linear over $Z(A)$, that is $L(A)$ is a finite vector space over $Z(A)$. Let S be the set of matrices of non-zero elements of $L(A)$ with respect to a fixed basis of A over $Z(A)$. By Theorem 4.2, the hypotheses of the Glauberman-Heimbeck Theorem are satisfied, so $S \cup \{0\}$ is a field under matrix addition and matrix multiplication, and hence $L(A)$ is a field under addition and composition. By Theorem 4.1, it follows that A is a field. □

Given a division ring A, the incidence structure with points the elements of $A \times A$ and lines the sets $\{(x, mx + b) : x \in A\}$, for all $m, b \in A$ and $\{(c, y) : y \in A\}$, for all $c \in A$, with incidence set membership is an affine plane, which we denote by $\mathrm{Aff}(A)$ whose projective completion is a projective plane, which we denote by $\Pi(A)$. A projective plane is *Pappian* if and only if it is isomorphic to $\Pi(A)$, where A is a field. A projective plane is *Desarguesian* if and only if it is isomorphic to $\Pi(A)$, where A is an associative division ring. It is a theorem of Moufang that a projective plane is *Moufang* if and only if it is isomorphic to $\Pi(A)$, where A is an alternative division ring [17, Theorem 6.15]).

Corollary 4.4 (Artin-Zorn-Levi theorem)**.** *A finite Moufang projective plane is Pappian.*

5 Extensions of the Glauberman-Heimbeck theorem to more general fields

We wish to reverse the connection between an alternative division ring A and the set $L(A)$ of left multiplications, given by Theorem 4.2. Each is a vector space over the centre of the alternative division ring (and the centre is a field) and they have the same dimension over the centre. Moreover, choosing a basis for the algebra over its centre and assigning to each left multiplication by a non-zero element of the algebra its matrix with respect to that basis, gives rise to a Glauberman-Heimbeck set of degree equal to its dimension. This is why Glauberman-Heimbeck sets of degree equal to their dimension play a special role in the sequel: there's no hope of reversing the connection between an alternative division ring and its ring of left multiplications unless we begin with a Glauberman-Heimbeck set of degree equal to its dimension. This also means that our extensions of the Glauberman-Heimbeck theorem to more general fields are restricted to this case.

Let S be a Glauberman-Heimbeck set over a field F of degree n and dimension n. Let e be a fixed non-zero element of F^n, and $\{C_1, \ldots C_n\}$ be a basis for $S \cup \{0\}$. Suppose $c_1(C_1e) + \cdots + c_n(C_ne) = 0$. Then $(c_1C_1 + \cdots + c_nC_n)e = 0$, but $c_1C_1 + \cdots + c_nC_n \in S \cup \{0\}$, so $c_1C_1 + \cdots + c_nC_n = 0$, which implies $c_1 = \cdots = c_n = 0$. Hence the subspace $W = \{Ce : C \in S \cup \{0\}\}$ has dimension n. Thus $W = F^n$. If $Ce = C'e$, then $(C - C')e = 0$ and $C - C' \in S$, so $C - C'$ not invertible implies $C - C' = 0$. Therefore, every element x of F^n can be written in a unique way as $x = Ce$, for some $C \in S$.

Denote that unique C by $C(x)$. Now define a multiplication on F^n by $xy = C(x)y$. Define $R(S)$ to be F^n under addition and this multiplication.

The left distributive law $x(y+z) = xy+xz$ in $R(S)$ follows from distributivity of matrix multiplication over vector addition. The right distributive law $(x + x')y = xy + x'y$ follows from $C(x + x') = C(x) + C(x')$, which, in turn follows from $C_1e = x$ and $C_2e = x'$ implying $(C_1 + C_2)e = x + x'$. Since $C(e) = I$, e is the left identity. Furthermore, $xe = C(x)e = x$, by definition of $C(x)$, so our left identity is the right identity. Let $a, b \in R(S)$ with $a \neq 0$. Then $ax = C(a)x = b$ if and only if $x = C(a)^{-1}b$, so $ax = b$ has a unique solution x. Moreover, $xa = b$ if and only if $C(x)a = b$. By the dimension argument above $\{Ca : C \in S \cup \{0\}\} = F^n$, so there exists $x \in R(S)$ with $xa = b$. If $Ca = C'a$, for $C, C' \in S$, then $C - C' \in S$ is not invertible, so $C = C'$. Thus there is a unique $x \in R(S)$ with $xa = b$. Then $R(S)$ is a (not necessarily associative) division ring.

Thus we have:

Theorem 5.1. *Let S be a Glauberman-Heimbeck set over a field F of degree of degree equal to its dimension. Then $R(S)$ is a (not necessarily associative) division ring.*

Theorem 5.2. *Let S be a Glauberman-Heimbeck set over a field F of degree equal to its dimension. Then $R(S)$ is associative if and only if S is closed under matrix multiplication. Moreover, $R(S)$ is an alternative division ring.*

Proof. Apply the identification $\ell_x \mapsto C(x)$ from $L(R(S))$ to S. It shows that S is closed under matrix multiplication if and only if $L(R(S))$ is closed under multiplication. Now apply Theorem 4.1.

To show that $R(S)$ is alternative, we apply the Skornyakov-San Soucie Theorem (Theorem 2.8). Thus we need only prove the left inverse property. Let $x \in R(S)$ with $x \neq 0$. Now, for all $y \in R(S)$, $x^{-1}(xy) = C(x^{-1})(C(x)y) = (C(x^{-1})C(x))y$, and $C(x)e = x$, so $e = C(x)^{-1}x$. Since $C(x)^{-1} \in S$, it follows that $C(x)^{-1} = C(x^{-1})$. Hence $x^{-1}(xy) = y$, for all $x, y \in R(S)$ with $x \neq 0$, which is the left inverse property for $R(S)$. □

Corollary 5.3. *Given an alternative division ring A, $L(A)$ is a subspace of the endomorphism ring of A over $Z(A)$ closed under inverses of non-zero elements and having the same dimension over $Z(A)$ as A does. Conversely, given a subspace L of the endomorphism ring of a vector space V over the field F closed under inverses of non-zero elements and having the same dimension over F as V does, V can be endowed with the structure of an alternative division ring with centre containing F in such a way that $L = L(V)$.*

Theorem 5.4. *Every Glauberman-Heimbeck set S over a field F of degree equal to its dimension is, together with 0, an associative division ring under matrix addition and multiplication if the dimension is not divisible by 8.*

Proof. By Theorem 5.2 and Bruck-Kleinfeld-Skornyakov Theorem (Theorem 2.7), $R(S)$ is either associative or an octonion algebra over its center (which contains F). Thus, if 8 does not divide the dimension, then $R(S)$ is associative. By Theorem 5.2 and Corollary 5.3, $S = L(R(S))$ is closed under multiplication, whence S is an associative division ring. □

Theorem 5.5. *Every Glauberman-Heimbeck set S over a field F of degree equal to its dimension is, together with 0, an associative division ring under matrix addition and multiplication if F is a complete, discretely valued field with finite residue class field, or a perfect field with cohomological dimension at most two.*

Proof. By Theorem 5.2, Bruck-Kleinfeld-Skornyakov Theorem (Theorem 2.7) and [28, pp.21-23], $R(S)$ is either an associative division ring or the split octonion algebra over its center. As the latter is not a division ring, then $R(S)$ is an associative division ring. The result then follows from Theorem 5.2 and Corollary 5.3. □

Remark 5.6. *Examples of perfect fields with cohomological dimension at most two are finite fields (which have dimension 1), p-adic fields and totally imaginary algebraic number fields .*

Theorem 5.7. *Every Glauberman-Heimbeck set S over a field F of degree equal to its dimension that is not, together with 0, an associative division ring under matrix addition and multiplication is isomorphic to the vector space $L(A)$ of left multiplications of an octonion algebra A whose centre Z contains a subfield F' isomorphic to F such that $|Z : F'|$ is finite, and conversely.*

Proof. This follows from Theorem 5.2, Corollary 5.3 and Theorem 2.7. □

Remark 5.8. In the preceding sections, there has been a subterranean undercurrent of ideas from geometry. The two key results connecting the properties of A and $L(A)$ in Theorem 4.2 and the construction of the ring $R(S)$ at the beginning of Section 5 both appeared in works of Bruck and Bose on representing translation planes by sets of square matrices, the former in Bruck-Bose [4, Section 11], and the latter in Bruck-Bose [3, Section 6]. In [22], another current of ideas from geometry was used to prove, without the use of deep results on finite groups, that a finite Bol quasifield of even order is a nearfield. It is desirable to find a similar proof for the case of odd order, which would give a combined algebraic result stronger than the Artin-Zorn theorem; a result previously obtained by six authors using the classification of finite simple groups during the period 1968-2006 (see the references in [22]).

Acknowledgments

The authors would like to thank the referee for his/her accurate report and for pointing out that the proof of Theorem 4.3 could be shortened by using the proof of [10, Lemma 4.6]. As the focus of our paper is on the connection between group theory, projective geometry and the theory of alternative division rings, we prefer to follow Glauberman's reasoning more closely for the purposes of comparison.

References

[1] A.A. Albert, On nonassociative division algebras, *Trans. Amer. Math. Soc.* 72 (1952) 256–309.

[2] J. Bamberg, T. Penttila, Completing Segre's proof of Wedderburn's little theorem, *Bull. London Math. Soc.* 47 (2015) 483–492.

[3] R.H. Bruck, R.C. Bose, The construction of translation planes from projective spaces, *J. Algebra* 1 (1964) 85–102.

[4] R.H. Bruck, R.C. Bose, Linear representations of projective planes in projective spaces, *J. Algebra* 4 (1966) 117–172.

[5] R.H. Bruck, E. Kleinfeld, The structure of alternative division rings, *Proc. Amer. Math. Soc.* 2 (1951) 878–890.

[6] A. Cayley, On Jacobi's elliptic functions, in reply to the Rev. B. Bronwin; and on quaternions", *Philos. Mag.* 26 (1845) 208–211

[7] C. Cerroni, Non-Desarguian geometries and the foundations of geometry from David Hilbert to Ruth Moufang, *Historia Math.* 31 (2004), 320–336.

[8] H.P. Dembowski, *Finite geometries.* Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44, (Springer-Verlag, Berlin-New York, 1968).

[9] L.E. Dickson, *Linear Algebras* (Cambridge University Press, Cambridge, 1914).

[10] J. Faulkner, *The role of nonassociative algebra in projective geometry.* Graduate Studies in Mathematics, 159 (American Mathematical Society, Providence, RI, 2014).

[11] G. Glauberman, Weakly closed elements of Sylow subgroups, *Math. Z.* 107 1968 1–20.

[12] G. Glauberman, A sufficient condition for $p-$stability. *Proc. London Math. Soc.* 25 (1972) 253–287.

[13] A.M. Gleason, Finite Fano planes. *Amer. J. Math.* 78 (1956) 797–807.

[14] E.G. Goodaire, E. Jespers, C. Polcino Milies, *Alternative loop rings.* North-Holland Mathematics Studies, 184 (North-Holland Publishing Co., Amsterdam, 1996).

[15] W.R. Hamilton, On Conjugate Functions, or Algebraic Couples, as tending to illustrate generally the Doctrine of Imaginary Quantities, and as confirming the Results of Mr Graves respecting the Existence of Two independent Integers in the complete expression of an Imaginary Logarithm. *Report of the Fourth Meeting of the British Association for the Advancement of Science; held at Edinburgh in 1834.* John Murray, London, 1835, pp. 519–523.

[16] G. Heimbeck, Bemerkung zu einem Satz von Glauberman, *Elem. Math.* 39 (1984) 95–98.

[17] D.R. Hughes, F.C. Piper, *Projective planes.* Graduate Texts in Mathematics, Vol. 6. (Springer-Verlag, New York-Berlin, 1973).

[18] E. Kleinfeld, Alternative division rings of characteristic 2, *Proc. Nat. Acad. Sci. U.S.A.* 37 (1951) 818–820.

[19] F.W. Levi, *Finite Geometrical Systems* (University of Calcutta, Calcutta, 1942).

[20] K. McCrimmon, Finite power-associative division rings, *Proc. Amer. Math. Soc.* 17 (1966) 1173–1177.

[21] R. Moufang, Alternativkörper und der Satz vom vollständigen Vierseit (D_9), *Abh. Math. Sem. Univ. Hamburg* 9 (1933) 207–222.

[22] T. Penttila, A. Siciliano, Bol quasifields, Mathematical Communications, *Math. Commun.* 25, (2020), 1–12.

[23] R.L. San Soucie, Right alternative division rings of characteristic two. *Proc. Amer. Math. Soc.* 6, (1955). 291–296.

[24] R.D. Schafer, An introduction to nonassociative algebras. Pure and Applied Mathematics, Vol. 22 (Academic Press, New York-London 1966).

[25] J.-P. Serre, *Galois cohomology.* Springer Monographs in Mathematics. (Springer-Verlag, Berlin, 1997).

[26] L.A. Skornyakov, Alternative fields, *Ukrain. Mat. Žurnal* 2 (1950) 70–85.

[27] L.A. Skornyakov, Right-alternative fields. *Izvestiya Akad. Nauk SSSR. Ser. Mat.* 15 (1951) 177–184.

[28] T.A. Springer and F.D. Veldkamp *Octonions, Jordan algebras and exceptional groups.* Springer Monographs in Mathematics. (Springer-Verlag, Berlin, 2000).

[29] J.H.M. Wedderburn A theorem on finite algebras *Trans. Amer. Math. Soc.* 6 (1905) 349–352.

[30] M.A. Zorn Theorie der alternativen Ringe. *Abh. Math. Sem. Hamburg* 8 (1930) 123–147.