THE WEDDERBURN FACTORIZATION THEOREM AND VALUED DIVISION ALGEBRAS

BHARATH SETHURAMAN AND ABHAY SOMAN

1 Introduction

The purpose of this expository article is to describe a charming and entirely elementary theorem of Wedderburn, known as the *Wedderburn Factorization Theorem.* It describes how certain polynomials over a field F factor completely into linear factors over a division algebra D whose center is F. This theorem merits being better known than it appears to be, especially given how easy it is to prove, and our hope, indeed, is that this article will contribute to that goal.

We use this opportunity to also describe the notion of valuations on division algebras, and show how Wedderburn's theorem allows us to prove a key result about the uniqueness of such valuations. We end by giving a construction of an infinite family of division algebras, using the properties of valuations.

First recall that if K/F is a finite extension of fields, K is said to be *normal* over F if the minimal polynomial over F of every element $k \in K$ splits completely over K. Normality is thus a measure of algebraic "fullness" over F, and yields desirable characteristics. For instance, if L/F is an extension of fields containing K/F as a subextension, then any element of the group of symmetries of L/F carries K to K. As another example, the group of symmetries of K/F is as large as it can possibly be, after factoring out the elements purely inseparable over F: we have $|\mathrm{Gal}(K/F)| = [K : F^{ins}]$, where F^{ins} is the set of elements purely inseparable over F. (In general, without the normality assumption, we would only have $|\mathrm{Gal}(K/F)| \leq [K : F^{ins}]$).

Now let D be an F-central division algebra, finite-dimensional over F. Any nonzero element $d \in D$ generates over F a commutative subring $F[d]$ of D, which as a set is just $\{f_0 + f_1 d + \cdots + f_k d^k \mid k \geq 0, f_i \in F\}$. The subring $F[d]$ is necessarily finite-dimensional as a vector space over F, since D itself is finite-dimensional over F. Hence, the set $\{1, d, d^2, \dots\}$ cannot be F-linearly independent, and exactly as in the case of field extensions, there exists some (say monic) polynomial $m_{d,F}$ of least degree with coefficients in F satisfied by d (see for instance [Lang, Chapter V, §1]). This polynomial is necessarily irreducible, for exactly the same reasons as in the field case: Assume that $m_{d,F} = fg$ for polynomials $f, g \in F[x]$ of lower degree than $m_{d,F}$. The evaluation map from $F[x]$ to $F[d]$ that arises from substituting $x = d$ is a ring homomorphism (this would not be true if F were a more general ring, as we will see in Remark 2.2 Part 1 ahead). Hence, $0 = m_{d,F}(d) = f(d)g(d)$. Since D is a division ring, either $f(d)$ or $g(d)$ must be zero. But this violates the minimality of $m_{d,F}$.

In analogy with the case of field extensions, it is reasonable to ask if $m_{d,F}$ factors completely in D.

Let us study a simple example, the first and most well-known example of a division algebra. This is Hamilton's Quaternions, denoted by $\mathbb{H}$. This is the four-dimensional $\mathbb{R}$-vector space with basis $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$, so $\mathbb{H} = \{p(= p \cdot 1) + q \cdot \mathbf{i} + r \cdot \mathbf{j} + s \cdot \mathbf{k},\ p, q, r, s \in \mathbb{R}\}$. Here, $\mathbf{i}$, $\mathbf{j}$, and $\mathbf{k}$ are symbols, and multiplication is given $\mathbb{R}$-bilinearly, subject to the following rules: $\mathbf{ij} = \mathbf{k}$, $\mathbf{ji} = -\mathbf{k}$, $\mathbf{i}^2 = \mathbf{j}^2 = -1$ (from which one derives the rules $\mathbf{k}^2 = -1$, $\mathbf{jk} = \mathbf{i}$, $\mathbf{ki} = \mathbf{j}$, $\mathbf{kj} = -\mathbf{i}$ and $\mathbf{ik} = -\mathbf{j}$), and, $p\mathbf{i} = \mathbf{i}p$, $p\mathbf{j} = \mathbf{j}p$ for all $p \in \mathbb{R}$ (which yields the rule $p\mathbf{k} = \mathbf{k}p$ as well). It is easy to see that this is a division algebra: we have the identity

$$(p + q\mathbf{i} + r\mathbf{j} + s\mathbf{k})(p - q\mathbf{i} - r\mathbf{j} - s\mathbf{k}) = p^2 + q^2 + r^2 + s^2 := N(d),$$

so if $d = p + q\mathbf{i} + r\mathbf{j} + s\mathbf{k}$ is nonzero, then $(p, q, r, s) \neq (0, 0, 0, 0)$, and we may divide the second factor on the left above by the nonzero real number $N(d)$ to determine the inverse of d as

$$d^{-1} = \frac{p}{N(d)} - \frac{q}{N(d)}\mathbf{i} - \frac{r}{N(d)}\mathbf{j} - \frac{s}{N(d)}\mathbf{k}.$$

In this simple example, it is easy to see that for any nonzero $d \in \mathbb{H}$, $m_{d,\mathbb{R}}$ splits completely in $\mathbb{H}$. In fact, it splits completely in $\mathbb{R}[d]$ itself. This is of course trivial if $d \in \mathbb{R}$, since $m_{d,\mathbb{R}}$ in that case is just $x - d$. For $d \notin \mathbb{R}$, first note that more generally, for any division algebra D finite-dimensional over its center F and nonzero $d \in D$, the subring $F[d]$ is necessarily a field. For, if

$$m_{d,F} = x^m + f_{m-1}x^{m-1} + \cdots + f_1 x + f_0,$$

then $f_0 \neq 0$, for otherwise, $m_{d,F}$ would admit the nontrivial factor x. We may write

$$d(d^{m-1} + f_{m-1}d^{m-2} + \cdots + f_1) = -f_0$$

and exactly as in the field case and in the case of $\mathbb{H}$ above, we may divide the second factor on the left by $-f_0$ to find that the inverse of d lies in $F[d]$ itself. Applying this same reasoning to any $e \neq 0$ in $F[d]$ shows that the inverse of e lies in $F[e] \subseteq F[d]$. Thus, $F[d]$ is a field.

Now, in our particular case of the Quaternions $\mathbb{H}$, for $d \notin \mathbb{R}$, the field $\mathbb{R}[d]$ has to be an isomorphic copy of $\mathbb{C}$, as $\mathbb{C}$ is the only nontrivial finite-dimensional field extension of $\mathbb{R}$. Thus, $m_{d,\mathbb{R}}$ has to split completely in $\mathbb{R}[d]$ as $\mathbb{C}$ is algebraically closed. (Alternatively, as $\deg(m_{d,\mathbb{R}}) = [\mathbb{C} : \mathbb{R}] = 2$ and $x - d$ is already a factor in $F[d]$, the other factor of $m_{d,\mathbb{R}}$ has to be linear.)

But what about more complicated examples of division algebras? This is where the Wedderburn Factorization Theorem comes in. It shows that if F is *any* field, and if D is *any* division algebra finite-dimensional over its center F, then D/F is normal in the same sense as in field theory: $m_{d,F}$ factors completely in D for any $d \in D$! Wedderburn's proof of this rather elegant theorem is elementary. We give his original proof of this theorem, and then describe a nontrivial application of this theorem to valued division algebras due to Wadsworth [Wa]: we describe how this theorem can be used to show that if F has a valuation v defined on it, and if this valuation extends to D, then the extension is completely determined by the valuation on F! We give examples of valuations on division algebras extending a given valuation on the center, describing, in the process, a natural genaralization of Hamilton's quaternions that yields division algebras of dimension n^2 for any integer $n = 2, 3, \ldots$.

2 Factorization theorem

We describe the Wedderburn Factorization theorem in this section. The theorem appears in Wedderburn's paper [We], where he uses it to study division algebras whose dimension over their centers is 9. Wedderburn's proof of his theorem, which we give below, is also described in the texts [Row1] and [Lam], among others. As already noted in Section 1, the proof is quite elementary; a more conceptual proof was given later by Jacobson, and can be found in [Row2].

For any ring R (always with 1), let $R[t]$ denote the polynomial ring in one variable t over R, where t commutes elementwise with R. For a polynomial

$$f(t) = \sum_{i=0}^{n} a_i t^i$$

and an element $r \in R$, we define the *evaluation of f at r* by $f(r) := \sum_{i=0}^{n} a_i r^i \in R$. Note that $(f + g)(d) = f(d) + g(d)$ for two polynomials $f, g \in R[t]$. Note, too, that to evaluate $f = gh \in R[t]$ at $r \in R$ we must first multiply out g and h and write f in the form $\sum a_i t^i$, and then substitute r for t. (See Remark 2.2, Part 1 below.)

Definition 2.1. *An element $r \in R$ is said to be a right root of $f \in R[t]$ if $f(r) = 0$.*

Remark 2.2.

1. In general, if $f = gh$ it does not follow that $f(r) = g(r)h(r)$. Indeed, consider a division algebra D with center F, and $d, d_1 \in D \setminus \{0\}$ are such that $dd_1 \neq d_1 d$. Put $g(t) = (t - d)$, and $h(t) = (t - d_1)$. Then $g(d)h(d) = 0$, while
$$\begin{aligned} gh(d) &= (t^2 - (d + d_1)t + dd_1)|_{t=d} \\ &= d^2 - d^2 - d_1 d + dd_1 \\ &= dd_1 - d_1 d \\ &\neq 0. \end{aligned}$$

2. Given f, h in $R[t]$, we say that h is a *right factor* of f if $f = gh$ for some $g \in R[t]$. An analogous definition holds for left factors.

3. Over a field, a polynomial of degree n has at most n distinct roots. Over a division ring, this is no longer true. For instance, in the Hamiltonian division algebra $\mathbb{H}$ over $\mathbb{R}$, both $\mathbf{i}$ and $-\mathbf{i}$ satisfy $t^2 + 1$, but so do $\pm\mathbf{j}$ and $\pm\mathbf{k}$. Further, any element of $\mathbb{H}$ of the form $z\mathbf{i}z^{-1}$ with $z \neq 0$ is also a root of $t^2 + 1$. Indeed, $(z\mathbf{i}z^{-1})^2 + 1 = z\mathbf{i}^2z^{-1} + 1 = z(\mathbf{i}^2 + 1)z^{-1} = 0$. It is easy to produce infinitely many distinct elements of the form $z\mathbf{i}z^{-1}$, so $t^2 + 1$ has infinitely many roots.

4. Let D and F be as in Part 1 of this remark. If $f = \sum a_i t^i \in F[t]$, and $d \in D$ is a root of f, then any conjugate zdz^{-1} is also a root. Indeed, $zf(t)z^{-1} = \sum za_i t^i z^{-1} = \sum a_i (ztz^{-1})^i$ (since $za_i = a_i z$). Also $zf(t)z^{-1} = f(t)$.

For our next definition, let D be a division algebra with center F, and D^* the set of its nonzero elements. A conjugacy class in D is the set of all conjugates zdz^{-1} of a fixed nonzero element d of D, as z varies through D^*.

Definition 2.3. *We say that a conjugacy class A is algebraic over F if one (and hence all) of its element is algebraic over F.*

Lemma 2.4. *Let D be a division ring and let $f = gh \in D[t]$. Let $d \in D$ be such that $a \coloneqq h(d) \neq 0$. Then*
$$f(d) = g(ada^{-1})h(d).$$
In particular, if d is a root of f but not of h, then ada^{-1} is a root of g.

Proof. Let $g = \sum b_i t^i$ and $h = \sum c_j t^j$. Then $f = \left(\sum b_i t^i\right)\left(\sum c_j t^j\right) = \sum\sum b_i c_j t^{i+j}$, so
$$\begin{aligned} f(d) &= \sum\sum b_i c_j d^{i+j} = \sum b_i \left(\sum c_j d^j\right) d^i \\ &= \sum b_i \left(h(d)\right) d^i = \sum b_i a d^i \\ &= \sum b_i a d^i a^{-1} a \\ &= \sum b_i (ada^{-1})^i a \\ &= g(ada^{-1})h(d). \end{aligned}$$

The last statement of the lemma follows because D is a division ring and has no zero divisors. □

Lemma 2.5. *For $f(t) \in D[t]$ and $d \in D$, we have*

$$f(t) = q(t)(t-d) + f(d).$$

In particular, d is a root of f if and only if $t-d$ is a right factor of f.

Proof. We proceed by induction on $\deg f(t)$. If $\deg f(t) = 1$, $f(t) = at + b$, then $f(t) = a(t - d) + ad + b$, i.e., we can take $q(t) = a$. Suppose $\deg f = n > 1$ and let $d_n \in D$ be the leading coefficient of $f(t)$. Put $g(t) = f - d_n t^{n-1}(t-d) = f - d_n t^n + d_n d t^{n-1}$, then $\deg g < \deg f$, and $g(d) = f(d) - d_n d^n + d_n d d^{n-1} = f(d)$. Thus, by the induction there exists $q_1 \in D[t]$ such that $g(t) = f(t) - d_n t^{n-1}(t-d) = q_1(t-d) + g(d)$. Hence, $f(t) = (q_1 + d_n t^{n-1})(t-d) + f(d)$. □

Proposition 2.6. *Let D be a central division algebra over F and A a conjugacy class of D which is algebraic over F with minimal polynomial $f \in F[t]$. If a polynomial $h \in D[t] \setminus \{0\}$ vanishes identically on A, then* $\deg h \geq \deg f$.

Proof. We may assume that h is monic, since if $h = e_m t^m + e_{m-1} t^{m-1} + \cdots + e_0$, then d is a root of h if and only if d is a root of $t^n + e_m^{-1} e_{m-1} t^{m-1} + \cdots + e_m^{-1} d_0$. Let $h = t^m + d_1 t^{m-1} + \cdots + d_m \in D[t]$ be such that $h(A) = 0$ and $m = \deg h < \deg f$ is as small as possible. Observe that $h \notin F[t]$, as f is the polynomial of least degree from $F[t]$ that vanishes on A. Hence some coefficient d_i is not in F, and therefore there is an $s \in D$ such that $d_i s \neq s d_i$. For any $a \in A$, $h(a) = a^m + d_1 a^{m-1} + \cdots + d_m = 0$. Hence

$$0 = (sas^{-1})^m + d_1 (sas^{-1})^{m-1} + \cdots + d_m.$$

On the other hand, using $s d_j a^{m-j} s^{-1} = s d_j s^{-1} s a^{m-j} s^{-1} = (s d_j s^{-1})(sas^{-1})^{m-j}$ we also have

$$0 = (sas^{-1})^m + (s d_1 s^{-1})(sas^{-1})^{m-1} + \cdots + (s d_m s^{-1}).$$

Hence the polynomial

$$\sum_{j=1}^{m} (d_j - s d_j s^{-1}) t^{m-j}$$

vanishes on $sAs^{-1} = A$. Since $d_i s \neq s d_i$, the above polynomial is nonzero, and its degree $< m$. This contradicts the choice of m. □

Theorem 2.7 (Wedderburn's Factorization theorem)**.** *Let D be a division algebra with center F. Let A be a conjugacy class of D which is algebraic over F, with minimal (monic) polynomial $f \in F[t]$ of degree n. Then there exists $a_1, \ldots, a_n \in A$ such that $f = \prod_{i=1}^{n} (t - a_i) \in D[t]$. Also, f is product of the same linear factors, permuted cyclically. The element $a_1 \in A$ can be arbitrarily prescribed.*

Proof. Fix $a_1 \in A$, so a_1 is a root of f and hence $t - a_1$ is a right factor of f. Consider a factorization of f

$$f = g(t)(t - a_r) \cdots (t - a_1)$$

with $g \in D[t]$, $a_i \in A$, where r is chosen as large as possible. We claim that $h = (t - a_r) \cdots (t - a_1)$ vanishes identically on A. Indeed, for $a \in A$ we have $f(a) = 0$. If $h(a) \neq 0$ then by lemma 2.4, $g(a_{r+1}) = 0$ for a conjugate a_{r+1} of a. Then we can write $g = g_1(t)(t - a_{r+1})$ for some $g_1 \in D[t]$, and thus f has a right factor $(t - a_{r+1})(t - a_r) \cdots (t - a_1)$, which contradicts the choice of r. Hence $h(a) = 0$ for every $a \in A$. Hence by Lemma 2.6, $\deg h \geq \deg f$. Since $\deg f \geq \deg h$ by construction, we find $f(t) = \prod_{i=1}^{n} (t - a_i)$.

To prove the last assertion, we show that for $f \in F[t]$ if $f = gh \in D[t]$, then $f = hg \in D[t]$. Indeed, for $g \in D[t]$, we have $gf = fg$ since the coefficients of f are in F. Thus, $gf = fg = ghg$, i.e., $g(f - hg) = 0 \in D[t]$. Hence, $f = hg$. □

An interesting paper of Laffey and Meehan ([LM]) carries Wedderburn's computations much further. For an arbitrary ring R, the authors analyze the factorization over R of an arbitrary polynomial in $Z(R)[t]$, where $Z(R)$ is the center of R. They show that under a certain existence condition, the polynomial factors into conjugate linear factors, exactly as in the Wedderburn factorization. They apply their result then to matrix rings $M_n(F)$ over arbitrary fields F of characteristic zero, and show that any polynomial of degree n with coefficients in F factors over the matrix ring into conjugate linear factors.

3 Valuation on a division algebra

In this section, we consider valuations on fields and division algebras finite-dimensional over their centers.

Recall that an abelian group Γ is *totally ordered* if it is linearly ordered as a set, and if $g \leq h$ implies $g + k \leq h + k$ for all $g, h, k \in \Gamma$.

Definition 3.1. *[Jac, Chapter 9, Definition 9.4′] A valuation v on a field F is a map*

$$v\colon F \to \Gamma \cup \{\infty\},$$

where Γ is a totally ordered abelian group, and ∞ a symbol such that

$$\gamma < \infty \quad \text{and } \gamma + \infty = \infty + \infty = \infty \text{ for all } \gamma \in \Gamma, \tag{3.1}$$

subject to the following conditions: for all $x, y \in F$,

1. *$v(x) = \infty$ if and only if $x = 0$;*
2. *$v(x + y) \geq \min\{v(x), v(y)\}$;*
3. *$v(xy) = v(x) + v(y)$.*

We denote $v\big(F \setminus \{0\}\big)$ by Γ_F. It is called the value group of F and is indeed a subgroup of Γ. Note that by Part 3 of the definition, v is a group homomorphism from $F \setminus \{0\}$ to Γ_F. In particular, $v(1) = 0$, and the relation $-1 \cdot -1 = 1$ then shows that $v(-1) = 0$. The field and its valuation are often jointly referred to as (F, v).

It is useful to observe that if $x \in F$ has positive value, then $v(1 + x) = 0$. For, by Definition 3.1 Part 2, $v(1 + x) \geq \min(v(1), v(x)) = 0$. If $v(1 + x)$ were positive, we would find $v(1) = v\left((1 + x) - x\right) \geq \min\left(v(1 + x), v(-x)\right)$, and since $v(-x) = v(-1 \cdot x) = v(-1) + v(x) = v(x) > 0$, we would find $v(1) > 0$, a contradiction.

It follows from this that if $v(x) < v(y)$ then $v(x + y) = v(x)$. For, $v(x + y) = v\left(x(1 + x^{-1}y\right)$. Now, from $xx^{-1} = 1$ we find $v(x^{-1}) = -v(x)$, so $v(x^{-1}y) = v(y) - v(x) > 0$. Hence by what we just showed, $v\left(x(1 + x^{-1}y)\right) = v(x) + v(1 + x^{-1}y) = v(x)$.

Example 3.2. Let $F = E(x)$ be the rational function field in one variable over a field E. Note that $\mathbb{Z}$ is naturally a totally ordered abelian group. We define a valuation $v_x\colon F \to \mathbb{Z} \cup \{\infty\}$ as follows: If $0 \neq f \in E[x]$ is such that $f = a_r x^r + a_{r+1}x^{r+1} + \cdots + a_{r+s}x^{r+s}$ where $a_r \neq 0$, then define

$$v_x(f) = r.$$

For any nonzero element $f/g \in F$ we define $v(f/g) = v(f) - v(g)$, and $v(0) = \infty$.

Example 3.3. Let $F = E(x, y)$ be the rational function field over E in two variables. Note that $\mathbb{Z} \times \mathbb{Z}$ is a totally ordered abelian group under the reverse lexicographic ordering: $(a, b) > (c, d)$ if $b > d$, or else, $b = d$ and $a > c$. Define a valuation $v\colon F \to (\mathbb{Z} \times \mathbb{Z}) \cup \{\infty\}$ as follows: Let $0 \neq f \in E(x)[y]$ and write f in the form $f = f_r y^r + f_{r+1}y^{r+1} + \cdots + f_{r+s}y^{r+s}$, where $f_i \in E(x)$ and $f_r \neq 0$. Define

$$v(f) \coloneqq \big(v_x(f_r), r\big).$$

For any nonzero element $f/g \in F$ we define $v(f/g) = v(f) - v(g)$, and $v(0) = \infty$. In particular, $v(x) = (1,0)$ and $v(y) = (0,1)$. Note that the zero element in $\mathbb{Z} \times \mathbb{Z}$ is $(0,0)$ and $v(e) = (0,0)$ for all $e \in E$.

In what follows, we restrict our attention to division algebras finite-dimensional over their centers.

Definition 3.4 (Valuation on a division algebra)**.** *Let D be a division algebra, finite-dimensional over its center. A valuation on D is a function*

$$v_D \colon D \to \Gamma \cup \{\infty\},$$

where Γ and ∞ are as in Definition 3.1, subject to the following conditions: for all $x, y \in D$,

1. *$v_D(x) = \infty$ if and only if $x = 0$;*
2. *$v_D(x + y) \geq \min\{v_D(x), v_D(y)\}$;*
3. *$v_D(xy) = v_D(x) + v_D(y)$.*

We denote $v_D\big(D \setminus \{0\}\big)$ by Γ_D. It is called the value group of D and is indeed a subgroup of Γ. Just as in the field case, v_D is a group homomorphism from $D \setminus \{0\}$ to Γ_D, so $v_D(1) = v_D(-1) = 0$. The division algebra and its valuation are often jointly referred to as (D, v_D).

Definitions 3.4 and 3.1 are clearly very similar. Indeed, if F is the center of D, then v_D restricts to a valuation on F in the sense of Definition 3.1. In the other direction, if (F, v) is a valued field and D is a division algebra with center F, we say a valuation v_D on D extends v if $v_D|_F = v$. In general, a valuation v on F need not extend to D, but the remarkable fact is that if it does extend, it does so *uniquely*, via a simple formula that determines it completely in terms of v. The derivation of this formula, which we describe in Proposition 3.5 below, is a lovely application of the Wedderburn Factorization Theorem.

To understand the ingredients in the formula, it is useful to know certain key facts about division algebras. While full proofs of these will take us deep into a study of a more general family of algebras known as simple algebras, the facts themselves can be described easily. We refer the reader to [Draxl, Part I, §5] or [Jac, Chapter 4, §4.6] for more details. A key result is that if $\overline{F}$ is an algebraic closure of F, then $D \otimes_F \overline{F}$ is isomorphic to the matrix algebra $M_t(\overline{F})$ for some t. Since the $\overline{F}$ dimension of $M_t(\overline{F})$ is t^2, we find from the tensor product description that the *dimension of any division algebra over its center is a perfect square.* The square root of this dimension is called the *index* of the division algebra.

Next, given $d \in D$, we may work with its matrix avatar $M_d = d \otimes 1$ in $M_t(\overline{F})$ under the embedding

$$D \xhookrightarrow{d \mapsto d \otimes 1} D \otimes_F \overline{F} \cong M_t(\overline{F}),$$

and consider its determinant. A second key result is that $\det(M_d)$ *lies in* F, not just in $\overline{F}$! The value of this determinant is called the *reduced norm of* d, and is denoted $\mathrm{Nrd}(d)$. It can be shown to be independent of the specific isomorphism $D \otimes_F \overline{F} \cong M_t(\overline{F})$ (there can be several) and is thus intrinsic to D. (In fact, the expression $N(d) = p^2 + q^2 + r^2 + s^2$ obtained in Section 1 from the quaternion $d = p + q\mathbf{i} + r\mathbf{j} + s\mathbf{k}$ is nothing more than $\mathrm{Nrd}(d)$, a tidy formula for the reduced norm in the case of the Quaternions!)

A third key result relates the reduced norm of d to its norm from $F[d]$ to F as defined via field theory. If $[F[d] : F] = n$, the result is that

$$\mathrm{Nrd}(d) = \big(N_{F[d]/F}(d)\big)^{\mathrm{ind}\,(D)/n},$$

where $N_{F[d]/F}(d)$ stands for the field theoretic norm, and $\mathrm{ind}\,(D)$ denotes the index of D as defined above.

We can now describe the formula for the extension of v to D (assuming such an extension exists).

Proposition 3.5. *(Wadsworth [Wa]) Let D be a finite-dimensional central division algebra over a valued field (F, v). Assume that w is a valuation on D extending v. For all $a \in D^*$ we have*

$$w(a) = \frac{1}{\operatorname{ind}(D)} v(\operatorname{Nrd}(a)).$$

In particular, if v extends to D, then the extension is uniquely determined by v.

Proof. Let $0 \neq a \in D$ and $f(t) = t^n + \alpha_{n-1}t^{n-1} + \cdots + \alpha_0 \in F[t]$ be the minimal polynomial of a over F. Thus, $n = [F(a) : F]$, $N_{F[a]/F}(a) = (-1)^n \alpha_0$, so by the third key result described above, $\operatorname{Nrd}(a) = (-1)^{\operatorname{ind}(D)} \alpha_0^{\operatorname{ind}(D)/n}$. Hence, $v(\operatorname{Nrd}(a)) = \frac{\operatorname{ind}(D)}{n} v(\alpha_0)$. By Wedderburn's Factorization theorem (2.7), we may find conjugates of a,

$$a_i = d_i a d_i^{-1} \quad (1 \leq i \leq n)$$

such that $f(t) = (t-a_1)\cdots(t-a_n)$. In particular, $\alpha_0 = (-1)^n a_1 a_2 \ldots a_n$. Now $w(a_i) = w(d_i a d_i^{-1}) = w(d_i) + w(a) + w(d^{-1})$, and the relation $d_i d_i^{-1} = 1$ shows us that $w(d_i) = -w(d_i^{-1})$. Hence, $w(a_i) = w(a)$ for all i, from which it it follows that $w(\alpha_0) = n \cdot w(a)$; hence $v(\operatorname{Nrd}(a)) = \operatorname{ind}(D) w(a)$. □

Example 3.6. Let E be a field containing a primitive n-th root of unity ω. Let $F = E(x, y)$ be the rational function field over E in two variables. Let v be the valuation on F defined in (Example 3.3).

Define an F-algebra generated by i, j with the following relations:

$$i^n = x, j^n = y, ij = \omega ji.$$

We denote this algebra by $(x, y)_n$. It is easy to see that an arbitrary element of this algebra can be written uniquely in the form $\sum_{k,l=0}^{n-1} c_{kl}\, i^k j^l$, where $c_{kl} \in F$, so the various powers i^k, j^l, $k, l, = 0, \ldots, n-1$ form an F basis.

Note that $\frac{1}{n}(\mathbb{Z} \times \mathbb{Z})$ is a totally ordered abelian group under the reverse lexicographic ordering, just like its subgroup $\mathbb{Z} \times \mathbb{Z}$. Consider the mapping $v_D \colon (x, y)_n \to \frac{1}{n}(\mathbb{Z} \times \mathbb{Z}) \cup \{\infty\}$ given by

$$v_D\left(\sum_{k,l=0}^{n-1} c_{kl}\, i^k j^l\right) = \min_{k,l}\left(v(c_{kl}) + \frac{k}{n}(1,0) + \frac{l}{n}(0,1)\right). \tag{3.2}$$

In particular,

$$v_D(i) = \frac{1}{n}(1,0), \quad v_D(j) = \frac{1}{n}(0,1) \quad \text{and} \quad v_D(\alpha) = v(\alpha) \text{ for } \alpha \in F. \tag{3.3}$$

Notice that

$$v_D(i^k j^l) \in \Gamma_F \text{ if and only if } k \in n\mathbb{Z} \text{ and } l \in n\mathbb{Z}.$$

Furthermore, we can show, exactly as we did for valuations on fields above, that the function v_D on $(x, y)_n$ also satisfies $v_D(1 + e) = 0$ if $v_D(e)$ is positive, and $v_D(d + e) = v_D(d)$ if $v_D(d) < v_D(e)$ *and* if d is invertible in $(x, y)_n$.

We first show that v_D satisfies all properties listed in Parts 1, 2, and 3 of Definition 3.4.

Suppose that $v_D\left(\sum_{k,l=0}^{n-1} c_{kl}\, i^k j^l\right) = \infty$. Then $v(c_{kl}) + \frac{k}{n}(1,0) + \frac{l}{n}(0,1) = \infty$ for every k, l, i.e., $v(c_{kl}) = \infty$ for every k, l. Since v is a valuation on F, we have $c_{kl} = 0$ for every k, l. Hence, $\sum_{k,l=0}^{n-1} c_{kl}\, i^k j^l = 0$, establishing Part 1.

We have

$$\begin{aligned}
v_D\Big(\sum_{k,l=0}^{n-1} c_{kl}\, i^k j^l + \sum_{k,l=0}^{n-1} d_{kl}\, i^k j^l\Big) &= v_D\Big(\sum_{k,l=0}^{n-1} (c_{kl}+d_{kl})\, i^k j^l\Big) \\
&= \min_{k,l}\Big(v(c_{kl}+d_{kl}) + v_D(i^k j^l)\Big) \\
&\geq \min_{k,l}\Big(\min\big(v(c_{kl}), v(d_{kl})\big) + v_D(i^k j^l)\Big) \\
&= \min_{k,l}\Big(\min\big(v(c_{kl}+v_D(i^k j^l)), v(d_{kl}+v_D(i^k j^l))\big)\Big) \\
&= \min\Big(\min_{k,l}\big(v(c_{kl})+v_D(i^k j^l), v(d_{kl})+v_D(i^k j^l)\big)\Big) \\
&= \min\Big(v_D\big(\sum_{k,l=0}^{n-1} c_{kl}\, i^k j^l\big), v_D\big(\sum_{k,l=0}^{n-1} d_{kl}\, i^k j^l\big)\Big),
\end{aligned}$$

establishing Part 2

To establish Part 3 needs a little more work. First, let us refer to an expression such as $c_{kl}i^k j^l$ for $0 \leq k < n$, $0 \leq l < n$ as a *monomial*. Note that any monomial is invertible: this follows from the fact that the inverse of i^k is $x^{-1}i^{n-k}$ for $1 \leq k < n$, and the inverse of j^l is $y^{-1}j^{n-l}$ for $1 \leq l < n$. First, we will show that if m_1 and m_2 are two monomials, then $v_D(m_1 m_2) = v_D(m_1) + v_D(m_2)$. Note that if $m_1 = c_{kl}i^k j^l$ and $m_2 = d_{k'l'}i^{k'} j^{l'}$, then, setting $\zeta = \omega^{k'l}$ we have the following relations:

$$m_1 m_2 = \begin{cases} (c_{kl}d_{k'l'}\,\zeta) i^{k+k'} j^{l+l'} & \text{if } k+k' < n \text{ and } l+l' < n \\ (c_{kl}d_{k'l'}\,\zeta x) i^{k+k'-n} j^{l+l'} & \text{if } k+k' \geq n \text{ and } l+l' < n \\ (c_{kl}d_{k'l'}\,\zeta y) i^{k+k'} j^{l+l'-n} & \text{if } k+k' < n \text{ and } l+l' \geq n \\ (c_{kl}d_{k'l'}\,\zeta xy) i^{k+k'-n} j^{l+l'-n} & \text{if } k+k' \geq n \text{ and } l+l' \geq n \end{cases}$$

Notice that from the expressions for $m_1 m_2$ above that if m_1 and m_2 are monomials, then $m_1 m_2$ is also a monomial.

We will show that $v_D(m_1 m_2) = v_D(m_1) + v_D(m_2)$ in the second of the four cases above; the proof for the other cases is similar. We apply the formula for v_D for a single monomial, which is implicit in Definition 3.2:

$$\begin{aligned}
v_D(m_1 m_2) &= v(c_{kl}d_{k'l'}\,\zeta x) + \tfrac{k+k'-n}{n}(1,0) + \tfrac{l+l'}{n}(0,1) \\
&= v(c_{kl}) + v(d_{k'l'}) + v(\zeta) + v(x) + \tfrac{k+k'-n}{n}(1,0) + \tfrac{l+l'}{n}(0,1) \\
&= v(c_{kl}) + v(d_{k'l'}) + (0,0) + (1,0) + (\tfrac{k+k'}{n} - 1)(1,0) + \tfrac{l+l'}{n}(0,1) \\
&= v(c_{kl}) + \tfrac{k}{n}(1,0) + \tfrac{l}{n}(0,1) + v(d_{k'l'}) + \tfrac{k'}{n}(1,0) + \tfrac{l'}{n}(0,1) \\
&= v_D(m_1) + v_D(m_2).
\end{aligned}$$

Here we have used the fact that $v(\zeta) = (0,0)$, this is because $\zeta^n = 1$, so $nv(\zeta) = v(1) = (0,0)$.

Now consider arbitrary elements $d = \sum_{k,l} c_{kl}\, i^k j^l$ and $e = \sum_{k,l} d_{kl}\, i^k j^l$ of $(x,y)_n$. Since $v_D(i^k j^l)$ and $v_D(i^{k'} j^{l'})$ are in different cosets of $\mathbb{Z}\times\mathbb{Z}$ in $\frac{1}{n}\big(\mathbb{Z}\times\mathbb{Z}\big)$ if $(k,l) \neq (k'l')$, $v_D(c_{kl}i^k j^l) \neq v_D(d_{k'l'}i^{k'} j^{l'})$. Hence we find that there is a *unique* monomial m_0 in d that has the lowest value of v_D, so by definition, $v_D(d) = v_D(m_0)$. Similarly, there is a unique monomial n_0 in e that has the lowest value of v_D and $v_D(e) = v_D(n_0)$. Let us write $d = m_0 + m_1 + \cdots$, where $m_1, \cdots$ are the other monomials in d: all of these have higher value of v_D than m_0. Similarly, let us write $e = n_0 + n_1 + \cdots$. Then $m_1 m_2 = m_0 n_0 + \sum_{(i,j)\neq(0,0)} m_i n_j$. Note that the various monomial products $m_s n_t$ need not be in distinct cosets of $\mathbb{Z}\times\mathbb{Z}$ in $\frac{1}{n}(\mathbb{Z}\times\mathbb{Z})$, but that will not concern us. Since we have already

seen that $v_D(m_i m_j) = v_D(m_i) + v_D(m_j)$, we see that all the monomial products other than $m_0 n_0$ have values of v_D higher than $v_D(m_0 n_0)$. Thus we write, $m_1 m_2 = m_0 n_0 + w$, and it follows from Part 2 of Definition 3.4, which we have already established, that $v_D(w) > v_D(m_0 n_0)$. Now $m_1 m_2$ is invertible (since we have observed that $m_1 m_2$ is a monomial and that every monomial is invertible), so it follows from what we have noted above that $v_D(m_1 m_2 + w) = v_D(m_1 m_2)$. Thus, $v_D(de) = v_D(m_1 m_2) = v_D(m_1) + v_D(m_2) = v_D(d) + v_D(e)$. This establishes Part 3.

Note that Parts 1 and 3 show that $(x, y)_n$ has no zero divisors, since if $d \neq 0$ and $e \neq 0$, then $v_D(d) \neq \infty$ and $v_D(e) \neq \infty$, so $v_D(de) = v_D(d) + v_D(e) \neq \infty$. The arguments in Section 1 which show that $m_{d,F}$ is irreducible and from this that d is invertible in $F[d]$ only relied on the finite-dimensionality of D and the fact that it has no zero divisors. Applying this to $(x, y)_n$, we find that every nonzero element d of $(x, y)_n$ is invertible, with inverse in $F[d]$, showing that $(x, y)_n$ is a division algebra.

By Proposition 3.5, v_D is the unique valuation on $(x, y)_n$ that extends the valuation v on F.

Notice that the algebras $(x, y)_n$ form a very nice generalization of $\mathbb{H}$. These algebras are clearly of index n, and thus furnish examples of division algebras of arbitrary index.

References

[Draxl] Draxl, P. K., *Skew fields*, London Mathematical Society Lecture Note Series, 81, Cambridge University Press, Cambridge, 1983.

[Jac] Jacobson, Nathan, *Basic algebra. II*, W. H. Freeman and Co., San Francisco, Calif., 1980.

[LM] Laffey, Thomas J., Meehan, Eleanor, *An extension of a factorization theorem of Wedderburn to matrix rings*, Second NIU Conference on Linear Algebra, Numerical Linear Algebra and Applications (DeKalb, IL, 1991), Linear Algebra Appl., (1992), 243 – 260.

[Lam] Lam, T. Y., *A first course in noncommutative rings*, Graduate Texts in Mathematics, 131, Springer-Verlag, New York, 1991.

[Lang] Lang, Serge, *Algebra*, Revised third edition, Graduate Text in Mathematics, 211, Springer-Verlag, New York, 2002.

[Row1] Rowen, Louis Halle, *Polynomial identities in ring theory*, Pure and Applied Mathematics, 84, Academic Press, Inc. New York-London, 1980.

[Row2] Rowen, Louis Halle, *Graduate Algebra: noncommutative view*, Graduate Studies in Mathematics, 91, American Mathematical Society, Providence, RI, 2008.

[Wa] Wadsworth, A. R., *Extending valuations to finite-dimensional division algebras*, Proc. Amer. Math. Soc. 98(1), 20 – 22 (1986).

[We] Wedderburn, J. H. M., *On division algebras*, Trans. Amer. Math. Soc. 22, (1921), no. 2, 129 – 135.

Bharath Sethuraman
al.sethuraman@csun.edu
Indian Statistical Institute,
Bengaluru Center, Mysore Road,
India.

Abhay Soman
somanabhay@gmail.com
Indian Statistical Institute,
Bengaluru Center, Mysore Road,
India.