DIVISION ALGEBRAS

LOUIS H. ROWEN

1. Introduction

A *division ring*, or *skew-field*, satisfies all the axioms of a field except (possibly) commutativity of multiplication. The center of a division algebra D is a field, which we always denote as F. Thus D is a vector space over F. This paper focuses on the case $[D : F] < \infty$; then we call D a *division algebra*. Division rings arise in several ways:

(1) By Schur's lemma, the endomorphism ring of an arbitrary simple module is a division ring.
(2) Goldie proved every noncommutative Noetherian domain is Ore, and thus has a classical ring of quotients which is a division ring. This applies for example to enveloping algebras of finite dimensional Lie algebras, and group algebras of torsion-free polycyclic-by-finite groups, rings of differential operators of nonsingular complex algebraic varieties, and other rings of current research interest in mathematics and physics.
(3) Many non-Noetherian domains also can be embedded in division rings, e.g. the free ring, and enveloping algebras of arbitrary Lie algebras.
(4) By the Wedderburn-Artin theorem, every simple Artinian ring is isomorphic to a matrix ring over a division ring. In particular, any finite dimensional semisimple algebra R can be written as a direct product of matrix rings $M_{t_i}(D_i)$, for suitable division algebras D_i (determined uniquely up to isomorphism). Thus division algebras arise in group representation theory, via Maschke's theorem.
(5) Quadratic forms give rise to *Clifford algebras*, which are simple algebras, and more generally division algebras come up in the study of homogeneous forms over non-algebraically closed fields.
(6) Division algebras tie in to algebraic geometry through Brauer-Severi varieties.
(7) The Steinberg symbols of K-theory are intimately connected with cyclic algebras.
(8) Division algebras arise in forms of algebraic groups defined over nonalgebraically closed fields.
(9) Any Desarguian projective plane can be coordinatized in terms of a suitable division ring.

The purpose of this talk is to give a brief account of the structure of division algebras, from the point of view of the role of cyclic algebras. After reviewing the early history, we shall focus on a recent development, the "essential dimension," which has been of considerable recent interest, largely because of the efforts of Z.

The author's research was supported in part by the Israel Science Foundation Center of Excellence. Also, the author would like to thank the referee for many helpful comments.

Y. Fong et al. (eds.), Proceedings of the Third International Algebra Conference, 221–233.

Reichstein. We review its effectiveness in studying division algebras of degree 4, indicating at the end how it fits into the overall structure theory (although much remains to be done there). A more thorough historical survey is given in [7].

According to the Hollywood version[1], the theory of division algebras was born on 16 October 1843. Hamilton had been trying for years to construct a 3-dimensional algebra over $\mathbb{R}$ satisfying all the axioms of a field except for commutativity. However, his efforts had been fruitless. His breakthrough in 1843 was to pass to dimension 4, where one can take

$$\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k,$$

made into an algebra by means of the relations

$$i^2 = j^2 = k^2 = -1, \tag{1}$$

$$ij = -ji = k \tag{2}$$

Unlike most mathematical constructions, Hamilton's has been preserved in stone, on the Brougham bridge, where in his moment of inspiration he reputedly carved out the formulas,

$$i^2 = j^2 = k^2 = ijk = -1.$$

The algebra $\mathbb{H}$ has indeed provided the base for much of modern physics.

Hamilton, the inventor of vectors, might have recognized there is no three-dimensional division algebra. Any noncommutative division algebra will have subfields K properly containing F; just take $F[d]$ for any $d \in D \setminus F$. In case $F = \mathbb{R}$, K must be isomorphic to $\mathbb{C}$. But clearly

$$[D : F] = [D : K][K : F], \tag{3}$$

so in our case $[D : F] = 2[D : K]$ is even.

Jumping ahead a bit, recall that a ring is called *simple* if it has no proper ideals $\neq 0$; then its center is a field F. If R is any simple (finite dimensional) algebra over its center F, then letting $\bar{F}$ denote the algebraic closure of F, one has

$$R \otimes \bar{F} \approx M_n(\bar{F}) \tag{4}$$

for suitable n, from which one concludes

$$[R : F] = [M_n(\bar{F}) : \bar{F}] = n^2,$$

which is always a square. We call n the *degree* of R. Thus $\deg \mathbb{H} = 2$.

One can cull much more information from (4). Indeed, identifying each element d of D with the matrix $d \otimes 1$ having entries in $\bar{F}$, we can define $\mathrm{tr}_{\mathrm{red}}\, d$, $\mathrm{N}_{\mathrm{red}}\, d$ as the respective trace and determinant of $d \otimes 1$; actually these take values in F. Furthermore, fixing a base $b_1, \ldots, b_{n^2}$ of D over F, and thereby writing any element of D of the form $\sum_{i=1}^{n^2} \alpha_i b_i$, we can use the usual formula of determinant of a matrix to view the reduced norm as a form of degree n in n^2 variables, which is nonisotropic since every nonzero element of D is invertible.

[1]Hamilton's work, published in [19], was anticipated both in the published literature by Rodriguez [33] and also in unpublished work by Gauss [17]; this information is contained in [4]. Nevertheless, Hamilton recognized the fundamental algebraic structure of quaternions, and spent most of the remainder of his mathematical career studying them.

Given any set $A \subset D$, we define the *centralizer*

$$C_D(A) = \{d \in D : da = ad \text{ for all } a \in A\}.$$

For example, $C_D(D) = F$ and $C_D(F) = D$. A subfield K is maximal iff $C_D(K) = K$, iff $[D : K] = [K : F] = \deg D$. Furthermore D always has maximal subfields separable over F.

2. Cyclic algebras

We return to the early history. After Frobenius [16] proved $\mathbb{H}$ is the only noncommutative division algebra over $\mathbb{R}$, the question remained whether other noncommutative division algebras exist. Wedderburn [47] proved any finite dimensional simple algebra R is isomorphic to a matrix ring $M_m(D)$ for some division algebra D unique up to isomorphism; we define the *index* of R to be $\deg D$. Thus

$$\deg(R) = m \operatorname{index}(R).$$

However, conceivably D could always be F.

In 1899 Hilbert had displayed examples of infinite dimensional division rings, by using Laurent series twisted by the automorphism of $\mathbb{C}$ given by complex conjugation. Only in 1906 did Dickson see how to find a finite dimensional analog of Hilbert's construction, and published the details later, in [13]:

Let K be a field with an automorphism σ of order n and fixed field F, and choose an element $\beta \in F$. Let A be an n-dimensional K-vector space with base designated $1, z, z^2, \ldots, z^{n-1}$, and endowed with multiplication

$$(a_1 z^i)(a_2 z^j) = \begin{cases} a_1 \sigma^i(a_2) z^{i+j} & \text{if } i + j < n; \\ \beta a_1 \sigma^i(a_2) z^{i+j-n} & \text{if } i + j \geq n; \end{cases}$$

where $a_i \in K$. This is a simple algebra called the *cyclic algebra* (K, σ, β). It still remains to see when this is a division algebra. Dickson did this for dimension 9 and 16, but Wedderburn [48] provided a sufficient criterion for (K, σ, β) to be a division algebra, thereby yielding division algebras of arbitrary index.

If F contains a primitive n-th root ρ of 1, then by Kummer's theorem there is a in K such that $\sigma(a) = \rho a$ and $\alpha = a^n \in F$. Then (K, σ, β) is called the *symbol algebra* $(\alpha, \beta)_n$ or $(\alpha, \beta; F)_n$. Every element has the form $\sum_{i,j=0}^{n-1} \gamma_{ij} a^i z^j$, with multiplication determined by the easy rules

$$za = \rho az, \qquad a^n = \alpha, \qquad z^n = \beta.$$

(In other words one juxtaposes the two monomials and then applies these rules to move the occurrences of z to the right of the occurrences of a.) Thus $\mathbb{H} = (-1, -1)_2$. The choice of ρ is important whenever $n > 2$, but nevertheless is usually deleted from the notation.

Conversely, suppose D has a maximal subfield K which is cyclic Galois over F. It follows easily from the Skolem-Noether Theorem that $D \approx (K, \sigma, \beta)$ is cyclic for suitable $\beta \in F$.

Cyclic algebras have always assumed an important role in the subject, leading to:

General fundamental question: Which division algebras are cyclic? Write $\mathbb{Z}/n$ for the cyclic group of order n. Obviously all division algebras of degree 2 are cyclic, since any separable field extension of degree 2 is Galois with group $\mathbb{Z}/2$.

In another remarkable paper, Wedderburn [49] proved that the minimal polynomial f_d of any element d in D can be factored over D as

$$f_d = (\lambda - d_n)\dots(\lambda - d_1) \tag{5}$$

for suitable d_i which are conjugate to d (i.e. $d_i = a_i d a_i^{-1}$ for suitable $a_i \neq 0$ in D.) Furthermore, in degree 3, Wedderburn showed that all a_i may be taken to be equal. Using Wedderburn's factorization, here is a direct proof that any division algebra D of degree 3 is cyclic: Clearly

$$d_1 + d_2 + d_3 = \operatorname{tr}_{\mathrm{red}} d.$$

If we choose $d \in D$ with $\operatorname{tr}_{\mathrm{red}} d = 0$ then we conclude

$$\frac{d_3}{d_2} = -1 - \frac{d_1}{d_2}. \tag{6}$$

Letting $K = F[\frac{d_1}{d_2}]$, we see that conjugation by a sends $\frac{d_1}{d_2}$ to $\frac{d_2}{d_3} \in K$, by (6), implying K/F is Galois.

Any central simple algebra R is the tensor product of central simple algebras of prime power degree (and exponent). Thus the theory reduces to the case where R has prime power degree. In particular, all division algebras of degree 6 are cyclic.

On the other hand, Albert (1931) displayed a noncyclic division algebra of degree 4. Today such an example would be quite easy: Take $F = F_0(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$, a field in 4 commuting indeterminates over any field F_0 of characteristic $\neq 2$, and let

$$D = (\lambda_1, \lambda_2)_2 \otimes_F (\lambda_3, \lambda_4)_2,$$

the tensor product of two "generic" symbol algebras. This can be viewed as the ring of fractions of a skew polynomial ring in indeterminates μ_2 and μ_4 over the commutative ring $L = F(\sqrt{\lambda_1}, \sqrt{\lambda_3})$, where $\mu_i^2 = \lambda_i$. Examining leading coefficients (after adjoining a primitive 4-th root of 1 to F), one can show that D cannot be cyclic. Indeed, if there were an element r with $r^4 \in F$ but $r^2 \notin F$ then multiplying by a suitable element of the center we could assume r is a (noncommutative) polynomial in μ_2 and μ_4; taking leading coefficients one would conclude L is a cyclic extension of degree 4 over F, which is false.

BIG QUESTION. Need division algebras of arbitrary prime degree ≥ 5 be cyclic?

The most promising way of attacking this question may be to find a field extension K of F and a cyclic division algebra D_1 of degree n over K which "descends" to a division algebra D over F, i.e. $D_1 = D \otimes_F K$. Even if $[K : F] = 2$, it is unknown whether D need be cyclic in general, although there are some partial results. This could cut either way - given D, one may try to find D_1 which will enable us to prove D is cyclic, or, alternatively, one might try to use D_1 to construct a noncyclic D.

3. The crossed product question and Amitsur's generic algebra

Albert did prove that every division algebra of degree 4 contains a maximal subfield Galois over the center (with group $\mathbb{Z}/2 \times \mathbb{Z}/2$), leading to other descriptions

of division algebras one to describe division algebras in terms of the following types of maximal subfields:

(1) Abelian Galois extensions of F, when they exist, [8], [14], [15];
(2) Galois extensions of F, when they exist (the "Noether" factor sets), [9]
(3) maximal separable subfields, which always exist (the "Brauer" factor sets).

These various constructions led to the question:

Crossed Product Question. Does every division algebra have a maximal subfield which is Galois over the center? (A division algebra with a maximal subfield Galois over F having Galois group G, is called a "crossed product" with respect to G. For prime degree, every crossed product is cyclic, so this distinction only is meaningful for composite degrees.)

Amitsur's crowning achievement in division algebras was his discovery in 1972 of a noncrossed product. As with many of Amitsur's finest results, the idea of proof is remarkably straightforward, although the computations needed at the time were quite intricate.

Given a field F_0, and commuting indeterminates $\{\xi_{ij}^{(k)} : 1 \leq i, j \leq n, 1 \leq k \leq m\}$ (where here m could be any ordinal number > 1), we define the *F_0-algebra of generic $n \times n$ matrices* to be the subalgebra R of $M_n\left(F_0[\xi_{ij}^{(k)}]\right)$ generated by the matrices $Y_k = \left(\xi_{ij}^{(k)}\right)$, called *generic* since the entries are distinct indeterminates. Amitsur proved R is a noncommutative domain satisfying a polynomial identity; hence by Posner's theorem (modified by the use of central polynomials), R is a central order in a division algebra, called $\mathrm{UD}(n, F_0)$. Since $\mathrm{UD}(n, F_0)$ satisfies the same polynomial identities as $n \times n$ matrices, it has degree n over its center, but the center is much larger than F_0, and very mysterious. For example its center encodes the classical theory of invariants, cf. [41, Chapter 14], and we still do not know if the center is purely transcendental over F_0.

Specialization lemma. *For any given element $f \neq 0$ in $UD(n, F_0)$ and any division algebra D of degree n over $F \supseteq F_0$, there is a specialization (i.e. partial homomorphism) from $UD(n, F_0)$ to D under which the image of $f \neq 0$ is defined and nonzero.*

By the specialization lemma, certain classes of first-order sentences in $\mathrm{UD}(n, F_0)$ pass down to D. In fact, enough sentences pass down so that in some sense $\mathrm{UD}(n, F_0)$ "contains" the theory of division algebras of degree n over F. In particular, Amitsur showed that if $\mathrm{UD}(n, F_0)$ is a crossed product with respect to G, then so is every division algebra D of degree n over $F \supseteq F_0$.

Thus $\mathrm{UD}(p^3, F_0)$ cannot be a crossed product, once one observes (over a field F containing a primitive p^3-root of 1 and indeterminates λ_i):

(1) The tensor product $(\lambda_1, \lambda_2)_p \otimes (\lambda_3, \lambda_4)_p \otimes (\lambda_5, \lambda_6)_p$ of generic symbols is a crossed product *only* with respect to $\mathbb{Z}/p \times \mathbb{Z}/p \times \mathbb{Z}/p$;
(2) the generic symbol $(\lambda_1, \lambda_2)_{p^3}$ is *not* a crossed product with respect to $\mathbb{Z}/p \times \mathbb{Z}/p \times \mathbb{Z}/p$.

The same argument shows noncrossed products exist for any degree n divisible by a cube > 1. This can also be done for n divisible by p^2 when F does not contain

a primitive p-th root of 1, but Amitsur's incompatibility method does not work in degree p^2 when F does contain a primitive p^2 root of 1; any symbol $(a,b)_{p^2}$ contains the subfield $F[\sqrt[p]{a}, \sqrt[p]{b}]$, and thereby is also a crossed product with respect to $\mathbb{Z}/p \times \mathbb{Z}/p$.

4. The Brauer Group

A more comprehensive theory is obtained by investigating the wider class of (finite dimensional) simple algebras with center F; these are closed under taking of tensor products, whereas the tensor product of division algebras is not necessarily a division algebra. Utilizing the Wedderburn-Artin theorem, we define an equivalence by saying $R_1 = M_{t_1}(D_1)$ and $R_2 = M_{t_2}(D_2)$ are *similar* if $D_1 \approx D_2$. The set of equivalence classes forms an Abelian monoid (under the operation of tensoring over F) denoted as $\operatorname{Br}(F)$. $\operatorname{Br}(F)$ points to the most important properties of central simple algebras. To begin with, define R^{op} to be the algebra with the same additive structure as R but multiplication taken in the opposite direction. Then one can prove

$$R \otimes R^{op} \approx M_{n^2}(F),$$

where $n = \deg(R)$, implying $\operatorname{Br}(F)$ is an Abelian group (where $[R]^{-1} = [R^{op}]$).

Examples:

(1) The Brauer group of an algebraically closed field is trivial.
(2) Wedderburn proved the Brauer group of a finite field is trivial.
(3) $|\operatorname{Br}(\mathbb{R})| = 2$ by Frobenius' theorem (the elements being $[\mathbb{H}]$ and $[\mathbb{R}]$). This is the only known example of a finite nontrivial Brauer group.
(4) Hasse showed $\operatorname{Br}(F) \approx (\mathbb{Q}/\mathbb{Z}, +)$, for any local field F; this follows from the fact that any division algebra of degree n over a local field F has the form (K, σ, π^k), where K is the unramified extension of dimension n, and π generates its value group.
(5) Brauer, Hasse, and Noether in Europe, at the same time (1931-1932) as Albert in the US, proved the famous Albert-Brauer-Hasse-Noether theorem, that every division algebra over an algebraic number field is cyclic, and also determined $\operatorname{Br}(\mathbb{Q})$.

We also get two important invariants associated with a central simple F-algebra $R = M_t(D)$. The first is the *index*, defined as $\deg(D)$. The second invariant is the *exponent*, defined as the period of $[R]$ in $\operatorname{Br}(F)$, i.e. the smallest number of times one must tensor R by itself in order to obtain a matrix algebra over F. The exponent and index are related by the two arithmetical properties:

(1) The exponent divides the index (so that in particular $\operatorname{Br}(F)$ is a torsion group);
(2) Any prime number dividing the index also divides the exponent.

When K and F are fields with $K \supset F$ there is a group homomorphism, called the *restriction* $\operatorname{res}_{K/F} \operatorname{Br}(F) \to \operatorname{Br}(K)$, given by $[D] \mapsto [D \otimes_F K]$. A more complicated map, called the *corestriction* $\operatorname{cor}_{K/F} \operatorname{Br}(K) \to \operatorname{Br}(F)$ can be defined in the other direction whenever the extension K/F is separable, and satisfies

$$\operatorname{cor}_{K/F} \operatorname{res}_{K/F}([D]) = [D]^{[K:F]}.$$

Rosset-Tate [24] proved the corestriction of a symbol is a product of at most $[K : F]$ symbols.

In 1982 Merkurjev-Suslin [28] demonstrated an important link between the Brauer group and K_2 groups, which shows that when F contains "enough" roots of 1, the Brauer group is generated by cyclic algebras. More explicitly, if D has exponent m, and F contains a primitive m-th root of 1, there exists t such that the matrix algebra $M_t(D)$ is isomorphic to a tensor product of cyclic algebras of degree $\leq n$. There must be an upper bound $t(n)$ for t, depending on $n = \deg D$, which we obtain by applying the Merkurjev-Suslin theorem to $\mathrm{UD}(n, F)$. However, there is no known algorithm to compute this bound, and as of now, there is no known upper bound for $t(n)$, for general n.

When n is a prime p, Rosset-Tate's theorem shows $t(p) \leq (p-1)!$, and using work of Rowen-Saltman [40] this can be lowered to $\frac{(p-1)!}{6}$, for $p \geq 5$, but this could be way too high, since perhaps $t(p) = 1$. So a major question is:

What is the Merkurjev-Suslin number $t(n)$ for various n? Tignol-Amitsur [45] provided lower bounds for nonprime n.

Interestingly, (with the exception of the next paragraph), much less is known about division algebras of exponent $m \geq 5$ when F does not contain a primitive m-th root of 1. One can still define the corestriction, but we do not have a workable analog of the Rosset-Tate theorem.

When $\mathrm{char}(F) = p \neq 0$ and $n = \deg D$ is a power of p then D is called a p-algebra, and a different situation takes hold. (For example F cannot have primitive p-roots of 1.) Surprisingly, the structure theory actually becomes more straightforward. For example, the part of the Merkurjev-Suslin theorem quoted was known years ago by Albert [3] in this case. However, we shall not treat that case here.

5. Essential dimension and C_m-fields

Amitsur's use of generic division algebras leads one to wonder how simply one can build them. More precisely, a division algebra U is called *generic for* a class of division algebras containing F, if the conclusion of the specialization lemma holds. The *essential dimension* $\mathrm{ed}(n)$ is the smallest possible transcendency degree of the center of a generic algebra for the class of division algebras of degree n. For example, $\mathrm{ed}(n) = 2$ whenever $\mathrm{UD}(n, F)$ is a symbol algebra.

A field is called a *C_m-field* if every (homogeneous) form of degree d in $> d^m$ variables has a nontrivial zero. Thus F is algebraically closed iff F is C_0-field, and it is known that every finite field is a C_1-field. Furthermore, if F is a finitely generated field of transcendence degree t over a C_m-field then F is a C_{m+t}-field.

So, if F_0 is algebraically closed and $\mathrm{ed}(n) = m$, then there is a generic division algebra U whose center is a C_m-field. Let us see what can be said for small m.

(1) (Tsen-Lang) The Brauer group over any C_1-field is trivial. Indeed, the reduced norm has a nontrivial zero whenever $n^2 > n$, which is true for all $n > 1$.
(2) If λ_1, λ_2 are indeterminates over an algebraically closed field F_0, then we have the symbol division algebra (λ_1, λ_2) defined over the C_2-field $F = F_0(\lambda_1, \lambda_2)$.
(3) (Artin-Bloch-Harris-Tate) If F is a C_2-field and $\mathrm{index}(D)$ is a power of 2 or 3 then $\mathrm{index}(D) = \exp(D)$. Here is the idea of the proof: First one assumes

$\exp(D) = p$, and adjoins a cube root of 1 to F if $p = 3$. By the Merkurjev-Suslin theorem D is similar to a tensor product of symbols, so it suffices to prove the tensor product of two symbols has index $\leq p$, i.e. is not a division algebra. In fact they show by an easy counting argument that any two symbols of degree p have elements with a common minimal polynomial, and thus have a common subfield. Indeed, to check the minimal polynomials have the same characteristic coefficients involves matching forms of degree $1, \dots, p$, and we have $2p^2$ variables (p^2 for each element), so to solve these over a C_2-field we need

$$2p^2 > 1^2 + \cdots + p^2,$$

which holds for $p < 5$.

The general case is handled by applying induction on exponent to $D^{\otimes p}$.

(4) Although it is unknown whether exp = index for any division algebra over an arbitrary C_2-field, de Jong [12] has shown recently that $\exp(D) = \operatorname{index}(D)$ when F is the function field of a surface.

(5) Any division algebra of degree 4 over a C_3-field is cyclic. This follows from a lovely theorem of Rost-Serre-Tignol [36] that when $\sqrt{-1} \in F$ the trace quadratic form q defined by $\{\operatorname{tr} d^2 : d \in D\}$ is Witt equivalent to $q_2 \oplus q_4$, where q_2, q_4 are respective two-fold and 4-fold Pfister forms; furthermore D is cyclic iff q_4 is isotropic. However in [39] a short proof was obtained by constructing a 9-dimensional linear space V of elements whose squares were quadratic over F: Since

$$9 > 2^3 = 8,$$

V contains an element $d \neq 0$ with $\operatorname{tr} d^2 = 0$; it follows $d^4 \in F$ but $d^2 \notin F$, implying D is cyclic when $\sqrt{-1} \in F$.

In particular $\operatorname{ed}(4) \geq 4$, since we saw noncyclic division algebras of degree 4. On the other hand, the generic tensor product of two symbols can be defined over a C_4-field, so there is no hope for a cyclicity result in this case. Note that the proof relies solely on the trace quadratic form on D, which thus also has $\operatorname{ed} \geq 4$ (suitably defined). We shall consider these issues in the next section.

(6) Reichstein-Youssin [32] have found noncrossed products over C_6-fields.

6. Structure of division algebras of degree 4

We continue to study a division algebra D of degree 4, assuming characteristic $\neq 2$. Albert proved D contains a maximal subfield $K = F[a_1, a_2]$ where $\alpha_i = a_i^2 \in F$. We continue with the Dickson-Amitsur-Saltman construction. Taking $z_1, z_2 \in D$ such that

$$z_i a_i = -a_i z_i; \qquad z_i a_j = a_j z_i \text{ for } j \neq i, \tag{7}$$

or equivalently

$$z_i k = \sigma_i(k) z_i \tag{8}$$

for $i = 1, 2$, one puts

$$u = z_1 z_2 z_1^{-1} z_2^{-1} \in K, \qquad b_i = z_i^2 \in K. \tag{9}$$

Then

$$D = K + Kz_1 + Kz_2 + Kz_1z_2 \tag{10}$$

and, writing $N_i(k)$ for $k\sigma_i(k)$, we have

$$\sigma_1(b_2) = N_2(u)b_2; \qquad \sigma_2(b_1) = N_1(u)^{-1}b_1, \tag{11}$$

implying

$$N_1N_2(u) = 1. \tag{12}$$

Furthermore, (7) through (12) define multiplication on D.

Conversely, given $u \in K$ satisfying (10), one can solve for b_1, b_2 in (11) via Hilbert's Theorem 90, so one can write D as (K, G, u, b_1, b_2). Note that a_1, a_2 could be chosen as

$$a_1 = b_2 - \sigma_1(b_2); \qquad a_2 = b_1 - \sigma_2(b_1),$$

so are redundant in describing D.

More explicitly,

$$b_1' = N_1(u) + 1, \qquad b_2' = N_2(u)^{-1} + 1 \tag{13}$$

satisfy (11), and clearly $\frac{b_i'}{b_i}$ is fixed by G and thus is in F. Hence one can build the generic division algebra of degree 4 as follows:

Take a generic field extension with respect to having an action of $G = \mathbb{Z}/2 \times \mathbb{Z}/2$ and element u such that $N_1N_2(u) = 1$. For example, let u_1, u_2, u_3 be indeterminates over the base field $F_1 = F_0(\lambda_1, \lambda_2)$, and define the action of G on $K = F_1(u_1, u_2, u_3)$ by fixing λ_1, λ_2 and

$$\sigma_1(u_1) = u_2; \qquad \sigma_2(u_1) = u_3; \qquad \sigma_1\sigma_2(u_1) = \frac{1}{u_1u_2u_3}. \tag{14}$$

Then $u = u_1$ satisfies (12), and taking b_i' as in (13) we see easily

$$UD = (K, G, u, b_1'\lambda_1, b_2'\lambda_2) \tag{15}$$

is generic. Its maximal subfield K has transcendence degree 5, so this shows $\operatorname{ed}(4) \leq 5$. In fact Rost [35] showed $\operatorname{ed}(4) = 5$, but his proof requires intersection theory from algebraic geometry. Ironically, although attempts to find simple proofs have failed so far, they have led to a full description of division algebras of degree 4, as we shall now see. Full details are in [26].

Theorem 1. *Assume $\sqrt{-1} \in F$. Any division algebra of degree 4 is similar to a tensor product of two symbols, one of degree 4 and one of degree 2. (In particular the Merkurjev-Suslin number $t(4) = 2$.)*

Proof. Write $D = (K, G, u, b_1, b_2)$. If $\operatorname{tr} b_1 = 0$ then $z_1^4 \in F$ and D is cyclic, so we assume $\operatorname{tr} b_1 \neq 0$. Pick $\gamma \in F$ to be determined shortly, and let

$$Q = (\alpha, \gamma)_2.$$

Then $(\alpha, \gamma)_2 \sim (K, G, 1, \gamma, b_2)$ so

$$D \otimes Q \sim (K, G, u, b_1\gamma, b_2).$$

Take z_1', z_2' as above, i.e. ${z_1'}^2 = b_1\gamma$, ${z_2'}^2 = b_2$; (7)-(12) hold with z_i' in place of z_i. Then

$$(z_1' + a_1)^2 = b_1\gamma + \alpha_1 \in F[a_2].$$

Picking

$$\gamma = -\frac{\alpha_1}{\operatorname{tr} b_1},$$

yields $\operatorname{tr}((z_1' + a_1)^2) = 0$, so $(z_1' + a_1)^4 \in F$ and $(K, G, u, b_1\gamma, b_2)$ is cyclic. This proves the theorem. □

Viewing $\operatorname{ed}(n)$ intuitively as the number of parameters needed to define a generic division algebra of degree n, it is not difficult to define the ed of many other kinds of algebraic structures, and in fact Buhler-Reichstein [11] initiated ed as a way of studying field extensions, which was carried out by Reichstein [30] (and other papers) in other situations. More precisely, the essential dimension is defined in [27], in terms of a functor Λ from the category of field extensions of a given field F_0 to the category of sets. For some field $F \supset F_0$, the essential dimension $\operatorname{ed}(\Lambda(F))$, of $\Lambda(F)$ is the minimal possible $\operatorname{tr}\deg(L)$ where $F_0 \subseteq L \subseteq F$, and $\lambda(F)$ lies in the image of the natural map $\Lambda(L) \to \Lambda(F)$. The sup of all these $\operatorname{ed}(\Lambda(F))$ is called the *essential dimension* of Λ, denoted $\operatorname{ed}(\Lambda)$.

Theorem 1 implies the *Brauer class* of index 4 has essential dimension 4, although $\operatorname{ed}(4) = 5$.

Another failed attempt to reprove Rost's theorem has led to another interesting theorem, about the trace quadratic form of the generic division algebra of degree 4. Reviewing the above discussion, one sees easily that the number of parameters needed for (15) is two more than the number needed to define K, i.e. the generic solution of a field extension K/F with a $\mathbb{Z}/2 \times \mathbb{Z}/2$-action and a generic element with respect to (12) has ed 3. So the obvious approach is to assume that there is a generic solution K' which could be defined with 2 parameters. Since we do not know much about division algebras of index 4 over C_4-fields, we would then modify (15) to $(K', G, u', b_1'\lambda_1, b_2')$, which we call *semi-generic*. This algebra, defined over a C_3-field, must be cyclic, implying $(K, G, u, b_1'\lambda_1, b_2')$ would be cyclic, so perhaps one could show this is false. On the contrary, it turns out that the semigeneric algebra *is* cyclic, and furthermore the trace quadratic form q for the generic division algebra of degree 4 is defined using only 4 parameters.

These results imply there is an example of a division algebra of degree 4, defined over a C_4-field, which is neither cyclic nor a tensor product of quaternion algebras, and an interesting question is to find some additional structural property distinguishing division algebras of degree 4 defined over C_4-fields.

7. Essential dimension of division algebras of degree > 4

The results for degree 4 are so striking that one may ask whether they can be extended to arbitrary prime power degree $n = p^t$. There is some hope for $p = 2$, using induction, although presently only partial results are available. For example, the same sort of argument given above is used in [26] to show that any crossed product with respect to $\mathbb{Z}/m \otimes \mathbb{Z}/2$ is similar to a tensor product of two symbol algebras (of respective degrees m and $2m$). One could write this more generally as:

Theorem 1′. *Suppose an arbitrary division algebra D has an element a such that $C_D(a)$ contains a symbol (α, b) of degree 2^t where $\alpha \in F$, $b \in F[a]$. Then D contains an element whose 2^{t+1} power is central (but whose 2^t power is not central)*

One wonders whether this could be used to compute the Merkurjev-Suslin number for degrees which are higher powers of 2. For $p > 2$ these methods become much less useful. For one thing, the approach using Dickson-Amitsur-Saltman only works on Abelian crossed products, and also it is harder to define the analogous field extension to (14). Furthermore, the trace argument used in Theorem 1 does not produce enough linear equations for $p > 2$.

On the other hand, one can still cut down the number of parameters needed in building the generic division algebra. This is done using lattice theory in [26], but we would like to describe a more naive procedure here. In Amitsur's construction one needs 2 matrices X, Y each with n^2 generic entries, thereby requiring $2n^2$ entries altogether. Since the diagonalizable matrices are dense, we get a generic object if X is generic diagonal, i.e., 0 off the diagonal. Write $Y = (y_{ij})$. A trick of Procesi is to conjugate X, Y by the diagonal matrix $\operatorname{diag}(1, y_{12}, \ldots, y_{1n})$ to get 1 on the first row of Y except for the diagonal. Moreover, for any separable maximal subfield K of D, one has

$$D = K \oplus [D, K]$$

as vector spaces, where $[D, K]$ is the space generated by the additive commutators $dk - kd$. (Indeed, writing $K = F[a]$, one sees that $[D, a]$ has dimension $n^2 - n$, so it suffices to prove $K \cap [D, a] = 0$. But if $k = [d, a]$ then taking $k' \in K$ of trace 1, one sees

$$k' = kk^{-1}k' = [d, a]k^{-1}k' = [dk^{-1}k', a]$$

which has trace 0, a contradiction.)

Hence one may take $a = X$, and thus assume Y is 0 on the diagonal. One can continue to cut down parameters through tricks of this sort, although a more systematic approach is by means of *Brauer factor sets.* Unfortunately all of these tricks succeed only in yielding an upper bound which is still on the order of n^2; the best general bound known so far is $n^2 - 3n + 1$ for $n \geq 4$, cf. Lemire [25]. (This is sharp for $n = 4$, as we shall see, but not for $n = 6$; the generic division algebra of degree 6 is cyclic, and a symbol is defined by two parameters.)

One can do somewhat better in odd index. First, one may normalize the Brauer factor set as in [38]. The trace bilinear form then becomes the same as for matrices. Secondly, normalized Brauer factor sets yield $\operatorname{ed}(n) \leq \frac{1}{2}(n-1)(n-2)$. Good estimates concerning the asymptotic behavior of $\operatorname{ed}(n)$ would be very interesting. In particular, one would like a subquadratic bound for $\operatorname{ed}(n)$ for some infinite class of n.

Counting the number of parameters needed to define Abelian crossed products gives a much lower estimate for the class of Abelian crossed products.

References

[1] Albert, A.A., New results on associative division algebras, *J. Algebra* **5** (1967), 110–132.
[2] Albert, A.A., On associative division algebras, *Bull. Amer. Math. Soc.* **74** (1968), 438–454.
[3] Albert, A.A., *Structure of algebras.* Amer. Math. Soc. Colloq. Pub. **24**, 1961

[4] Altmann, S.L., Hamilton, Rodriguez, and the quaternion scandal, *Math. Mag.* **62** (1989), 291–308.
[5] Amitsur, S.A., On central division algebras, *Israel J. Math.* **12** (1972), 408–420.
[6] Amitsur, S.A., Galois splitting fields of a universal division algebra, *J. Algebra* **143** (1991), 236–245.
[7] Amitsur, S.A., Highlights in the history of finite dimensional central division algebras, in *Israel Math. Conference Proceedings, vol. 1.* Amer Math. Soc., 1989.
[8] Amitsur, S.A. and Saltman D., On central division algebras, *Israel J. Math.* **12** (1972), 408–420.
[9] Brauer, R., Uber Systeme hyperkomplexer Zahlen *Math Z.* **30** (1929), 79–107.
[10] Brauer, R., Uber den index und den expotenten von divisionsalgebren, *Tohuko Math J.* **37** (1933), 77–87.
[11] Buhler J. and Reichstein Z., On the Essential Dimension of a Finite Group, *Compositio Math.* **106** (1997), 159–179.
[12] De Jong, A.J., The period-index problem for the Brauer group of an algebraic surface. Available from `http://www.math.mit.edu/~dejong`
[13] Dickson, L.E., Associative algebras and abelian equations, *Trans. Amer. Math. Soc.* **15** (1914), 31–46.
[14] Dickson, L.E., New division algebras, *Trans. Amer. Math. Soc.* **28** (1926), 207–234.
[15] Dickson, L.E., Construction of division algebras, *Trans. Amer. Math. Soc.* **32** (1932), 319–314.
[16] Frobenius, G., Uber die Darstellung der endlichen Gruppen durch linearen Substitutionen, *Berlin Akad.* (1897).
[17] Gauss, C.F. *Werke.* Konigliche Gesellschaft der Wissenschaften, vol. 8., Gottingen 1863–1929. (pp. 357–362).
[18] Greenberg, M. *Lectures on forms in many Variables.* Benjamin, New York, 1969.
[19] Hamilton, W.R., On quaternions; or a new system of imaginaries in algebra, *Phil. Mag. 3rd ser.* **25** (1844), 424–434.
[20] Jacob, B. and Wadsworth, A., Division algebras over Henselian fields, *J. Algebra* **128** (1990), 126–179.
[21] Jacobson, N., Brauer factor sets, Noether factor sets, and crossed products, in *Emmy Nother, a Tribute to her Life and Work* (eds. J. Brewer, M. Smith). 1981.
[22] Jacobson, N. *Finite-dimensional division algebras over fields.* Springer, 1996.
[23] Lang, S., On the quasi-algebraic closure, *Annals of Math.* **55** (1952), 373–390.
[24] Knus M.-A., Merkurjev A., Rost M. and Tignol J.-P., *The Book of Involutions.* Amer. Math. Soc. Colloq. Pub. **44**. Amer. Math. Soc. 1998.
[25] Lemire, N., In preparation.
[26] Lorenz, M., Rechstein, Z., Rowen, L., and Saltman, D. *The field of definition of a division algebra.* Submitted.
[27] Merkuriev A., *Essential dimension.* UCLA lecture notes 2000.
[28] Merkuriev and Suslin, A., K-cohomologies of Sevri-Brauer varieties and norm residue homomorphisms, *Izv. Akad. Nauk. SSSR* **46**, 1011–1046.
[29] Reichstein, Z., On a theorem of Hermite and Joubert, *Canad. J. Mathematics* **51** (1999), 69–95.
[30] Reichstein, Z., On the notion of essential dimension for algebraic groups, *Transformation groups* **5** (2000), 265–304.
[31] Reichstein, Z. and Youssin, B., Essential dimensions of algebraic groups, and a resultion theorem for G-varieties, with an appendix by J. Kollar and E. Szabo, *Canad. J. Mathematics* **52** (2000), 1018–1056.
[32] Reichstein Z. and Youssin, B., Splitting fields of G-varieties, *Pacific Journal of Mathematics* **200** (2001), 207–249.
[33] Rodriguez, O., Des lois geometriques qui regissent les deplacements d'une systeme solide dans l'espace, et la variation des coordonnees provenant de ses deplacements consideres independamment des causes quiveuvent les produire, *Journal de Math. Pure et Appliquees* **5** (1840), 380–440.

[34] Rosset, S, and Tate, J., A reciprocity law for K_2-traces, *Comment. Math. Helv.* **58**, 38–47.
[35] Rost, M., Computations of some essential dimensions. Preprint.
[36] Rost, M., Serre, J.P., and Tignol, J.P., The trace form of a central simple algebra of degree 4. Preprint.
[37] Rowen, L.H., *Polynomial Identities in Ring Theory.* Pure and Applied Mathematics **83**. Academic Press, Boston, 1980.
[38] Rowen, L.H., Brauer factor sets, *Trans. Amer. Math. Soc.* **282** (1984), 765–772.
[39] Rowen, L.H., Division algebras over C_2 and C_3-fields, *Proc. Amer. Math. Soc.* (2001).
[40] Rowen, L.H. and Saltman, D., Semidirect product division algebras, *Israel J. Math.* **96** (1996), 527–552.
[41] Saltman, D.J., *Lectures on division algebras.* Amer. Math. Soc. CBS Reg. Conf. Ser. in Math. vol. 94, 1999.
[42] Serre J.-P., *Corps Locaux.* Hermann 1962.
[43] Serre J.-P., *Galois Cohomology.* Springer 1997.
[44] Tate, J., Relations between K_2 and Galois cohomology, *Invent. Math.* **36** (1976), 257–274.
[45] Tignol, J.P. and Amitsur, S.A., Totally ramified splitting fields of central simple algebras over Henselian fields, *J. Algebra* **98** (1986), 95–101.
[46] Tsen, C., Zur Stufentheorie der Quasi-algebraisch-Abgeschloosenheit kommutativer Korper, *J. Chinese Math. Soc.* **1** (1936), 81–92 .
[47] Wedderburn, H.M.S., On hypercomplex numbers *Proc. London Math. Soc. (2)* **6** (1907), 77–118.
[48] Wedderburn, H.M.S., A type of primitive algebra *Trans. Amer. Math. Soc.* **15** (1914), 162–166.
[49] Wedderburn, H.M.S., On division algebras, *Trans. Amer. Math. Soc.* **22** (1921), 129–135.

BAR-ILAN UNIVERSITY, RAMAT-GAN 52900, ISRAEL
E-mail address: rowen@macs.biu.ac.il