Division Algebras*

Konrad Voelkel

2015-01-27

Contents

1 Big Picture 1

2 Algebras 2
- 2.1 Finite fields . . . 2
- 2.2 Algebraically closed fields . . . 2
- 2.3 $\mathbb{R}$-division algebras . . . 3

3 Cayley-Dickson construction 4

4 Spheres 6

5 Exceptional Groups 7

1 Big Picture

Slogan: "$\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$ are special"

If we consider $\mathbb{R}$-algebras with some extra property or structure, like being a finite dimensional division algebra or admitting a norm or a composable quadratic form, very often all you can have are the classical four algebras of dimensions $1, 2, 4, 8$.

They arise from the real numbers by the Cayley-Dickson construction, which is algebraic.

As a consequence, the numbers $1, 2, 4, 8$ show up elsewhere in mathematics. One example is the Hopf invariant one problem, whose solution shows that the unit spheres in $\mathbb{R}^1, \mathbb{R}^2, \mathbb{R}^4, \mathbb{R}^8$ are the only ones which admit a multiplication, even up to homotopy.

Another prominent example of the classical division algebras showing up is the construction of exceptional groups.

*More than enough notes for a talk in the "Basic Notions" seminar, Freiburg

2 Algebras

Definition. *Let A be a k-algebra with k a field.*

- *A is* associative *if its multiplication is.*
- *A is* simple *if the multiplication is not uniformly* 0 *and there are no non-trivial two-sided ideals.*
- *A is* central simple *or a* csa *if it is associative, simple and k is the center.*
- *A is a* division algebra *if one can solve equations $ax = b$ and $xa = b$ for x. An associative division algebra can be characterized by having inverse elements for any $x \neq 0$.*
- *A is a* composition algebra *if it has a quadratic form N which is* composable*, i.e. $N(xy) = N(x)N(y)$.*
- *A is a* Banach algebra *if it has a multiplicative norm and it complete for this norm.*

Proposition. *Every simple algebra A is a csa over its center $Z(A)$, which is a commutative ring without nontrivial ideals, hence a field. Every associative k-division algebra A is simple, hence a k'-csa for k'/k a field extension.*

2.1 Finite fields

Theorem (Wedderburn's little theorem 1905)**.** *For a division algebra A over a field k, the following are equivalent:*

- *k is a finite field and A is finite dimensional over k*
- *A is a finite field.*

This follows from the Skolem-Noether theorem, which states that every automorphism of a finite dimensional csa over a field is inner.

2.2 Algebraically closed fields

Proposition. *Over an algebraically closed field $k = \overline{k}$, the only finite-dimensional associative division algebra is k itself.*

Proof. If you have D over k, any $a \in D$ is the root of a monic polynomial f, since the powers a^n are linearly dependent over k. Choose f of minimal-degree, let λ be a root in k, then $f(x) = g(x)(x - \lambda)$ and minimality of f yields $g(a) \neq 0$, hence $\lambda = a$. □

From this, one can show the interesting

Proposition. *The dimension of a k-csa is either infinite or a square.*

Proof. If a k-csa A its not infinite-dimensional, extend A to the algebraic closure $\overline{k}$. By another theorem of Wedderburn, There is a skew field D such that $A_{\overline{k}}$ is a matrix algebra $Mat(D)^{n\times n}$. We count $[A_{\overline{k}} : \overline{k}] = n^2[D : \overline{k}]$. By the previous proposition $D = \overline{k}$, therefore $[A : k] = [A_{\overline{k}} : \overline{k}] = n^2$. □

Remark. *While $\mathbb{R}$ and $\mathbb{H}$ have center $\mathbb{R}$ and therefore are $\mathbb{R}$-csa (and have square dimensions $1, 4$), this is not the case for $\mathbb{C}$, which has center $\mathbb{C}$ and $\mathbb{O}$, which is not associative. The Brauer group of $\mathbb{R}$, which classifies $\mathbb{R}$-csa's up to Morita equivalence, contains just one nontrivial element, corresponding to $\mathbb{H}$.*

Over an arbitrary field k, four-dimensional k-csa's are also called quaternion algebras*.*

2.3 $\mathbb{R}$-division algebras

Example. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$ *are $\mathbb{R}$-division algebras with complete norm (defined by a composable quadratic form). While $\mathbb{R}$ and $\mathbb{C}$ are commutative, $\mathbb{H}$ is non-commutative and $\mathbb{O}$ is not even associative.*

Example. *The* split complex numbers *are $\mathbb{R} \oplus j\mathbb{R}$ with $j^2 = 1$, so*

$$(a + jb)(c + jd) = (ac + bd) + j(ad + bc).$$

There are zero divisors:

$$(1 - j)(1 + j) = (1 - 1) + j(1 - 1) = 0$$

hence we have an associative algebra on $\mathbb{R}^2$ which is not a division algebra.

There are also split quaternions and split octonions.

Example. *Another "splitting phenomenon" is the isomorphism*

$$\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \xrightarrow{\sim} Mat^{2\times 2}(\mathbb{C}).$$

Theorem (Frobenius 1877)**.** *The only finite-dimensional associative $\mathbb{R}$-division algebras are $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$.*

To prove this, one shows that in any finite-dimensional associative $\mathbb{R}$-division algebra D the subspace $V := \{a \in D \mid a^2 = \lambda \cdot 1,\ \lambda \leq 0\}$ is a direct summand of codimension 1 that generates D as algebra. Then $B(a, b) := -(ab + ba)/2$ is an inner product on V. Using a minimal length generating system for D inside V, one can see in a case-by-case analysis that the length can only be $0, 1, 2$ or D wouldn't be a division algebra.

There exist many infinite-dimensional associative division algebras:

Example. *Over $\mathbb{Q}(t)$, take formal Laurent series $\mathbb{Q}(t)((x))$ with new product induced by $x \cdot a(t) := a(2t)x$. This is not a field, but an infinite dimensional associative $\mathbb{Q}$-division algebra (due to Hilbert).*

Example. *For any Banach space X, the endomorphisms $End(X)$ with composition form an infinite dimensional associative Banach algebra, but not every element is invertible.*

Theorem (Gelfand-Mazur 1938)**.** *The only associative Banach $\mathbb{R}$-division algebras are $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$. The only associative Banach $\mathbb{C}$-division algebra is $\mathbb{C}$.*

Both statements follow from a rather elementary analysis of the spectrum of elements, but the first takes much more time than the second.

3 Cayley-Dickson construction

Definition. *If A is an algebra with involution $* : A \to A$ such that $(ab)^* = b^* a^*$, we call a subalgebra $A' \subset A$* real *if $*|_{A'} = A'$. For the identity involution on A, the whole A is real. This is how we consider $\mathbb{R}$ as an algebra with involution.*

Definition. *Given a unital algebra A with involution $* : A \to A$ such that $(ab)^* = b^* a^*$, on $B := A \oplus iA$ (with i an arbitrary new symbol) we define a new multiplication that satisfies $i^2 = -1$, by the formula*

$$(a + ib)(c + id) = (ac - \lambda d^* b) + i(da + bc^*),$$

where we put $\lambda = 1$. We define an involution on B by $(a + ib)^* := a^* - ib$.

Proposition. *The Cayley-Dickson construction "destroys" properties.*

- *If A is associative, commutative and real, B will be associative and commutative, but no longer real.*
- *If A is associative, commutative, but not real, B will be associative, but no longer commutative.*
- *If A is associative, but not commutative, B will no longer be associative, but alternative (a weak form of associativity).*

Example. *For $\mathbb{R}$ with the identity involution, we obviously get $\mathbb{C}$ with the complex conjugation as involution, while we loose the property of being "real". From $\mathbb{C}$ we get $\mathbb{H}$, which is no longer commutative, and then we get $\mathbb{O}$, which is no longer associative. The next step are the Sedenions $\mathbb{S}$, which are no longer a division algebra, but still power-associative. We can go on forever, doubling in each step the dimension of the algebra.*

Definition. *For a unital composition algebra A with quadratic form N, we define a bilinear form b by the polarization formula from the quadratic form:*

$$b(a, b) := \frac{1}{2}\left(N(a + b) - N(a) - N(b)\right)$$

if the field k has char$k \neq 2$, in which case we only have a definition of $2b$. In any case, we define an involution on A by

$$a^* = 2b(a, 1)1 - a.$$

In addition to the "external" Cayley-Dickson construction for a unital composition algebra, there is also an "internal" version:

Proposition. *Given a unital composition algebra A and a finite-dimensional composition subalgebra $A' \subset A$ with $A' \neq A$, there is a subalgebra $B' \subset A$ such that $A' \oplus B' \subset A$ is isomorphic to the Cayley-Dickson construction applied to A'.*

Proof. We have $A = A' \oplus A'^{\perp}$ and there is $a \in A'^{\perp}$ with $N(a) \neq 0$. Then $B' := Aa$ is a composition subalgebra of A with $B' \subset A'^{\perp}$ and on $A' \oplus B'$ we can verify the Cayley-Dickson formula with $\lambda := N(a)$, by calculations. □

Lemma. *Any proper, finite-dimensional subalgebra of a composition algebra is associative.*

Proof. Let $A' \subset A$ be a proper, finite-dimensional subalgebra. We test associativity with the bilinear form defined by the quadratic form, using the extra space of having a proper subalgebra.

Let $a \in A'^{\perp}$ with $N(a) \neq 0$. Then for $x, y, u, v \in A'$ we have

$$N((x + ya)(u + va)) = N(x + ya)N(u + va)$$

so plugging in the definition of the bilinear form b (resp. $2b$) defined by N gives

$$b(xu, v^*y) - b(vx, yu^*) = 0$$

So one has

$$b((xu)y^*, v^*) = b(v, (yu^*)x^*) = b(x(uy^*)v^*)$$

for all v, hence for all v^*, actually

$$(xu)y = x(uy).$$

□

Theorem (Jacobson)**.** *A composition algebra over a field k can be only of dimensions $1, 2, 4, 8$. In particular there are no infinite-dimensional composition algebras.*

Proof. In characteristics 2, the proof (by Springer) is different, we don't discuss it, so let k be of characteristics $\neq 2$. Let A be a composition algebra, then in the center we have a 1-dimensional composition sub-algebra $k1$ from which Cayley-Dickson gives a 2-dimensional composition sub-algebra. If one gets to the third step, the 8-dimensional composition sub-algebra one gets is no longer associative (since Cayley-Dickson only gives something associative if the input is commutative, and the dimension 4 step is already non-commutative), so from the previous lemma it must be non-proper, i.e. the whole thing. □

Remark. *One can say something more about the properties of composition algebras:*

- *Composition algebras of dimension 1 and 2 are commutative and associative.*

- *Composition algebras of dimension 2 are either quadratic field extensions of k (like the complex numbers) or isomorphic to $k \oplus k$ (like the split complex numbers, which are not a division algebra).*
- *Composition algebras of dimension 4 are called quaternion algebras. They are associative but never commutative.*
- *Composition algebras of dimension 8 are called octonion algebras. They are neither associative nor commutative.*

Remark. *Over any field, in each dimension $2, 4, 8$ there is, up to isomorphism, exactly one split composition algebra, and no other composition algebra with zero divisors. The split composition algebras are the only ones where the quadratic form is isotropic, i.e. there exists x with $N(x) = 0$.*

Remark. *Over $k = \mathbb{R}$, one can show that every composition division algebra is (isometrically) isomorphic to one of $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$. As a consequence, one gets a result of Hurwitz from 1898 on composability of bilinear forms (sums of square formulas). Therefore the theorem is sometimes called "Hurwitz' Theorem". One can classify the composition algebras over more fields (e.g. algebraically closed fields or algebraic number fields).*

4 Spheres

Proposition. *For any $\mathbb{R}$-division algebra A, the additive structure $A \xrightarrow{\sim} \mathbb{R}^n$ induces a (not necessarily multiplicative) norm on A and the multiplication map $m : A \times A \to A$ induces a multiplication on the unit sphere $S(A) \xrightarrow{\sim} S^{n-1}$, which is an odd map*

$$m : S^{n-1} \times S^{n-1} \to S^{n-1}$$

where the oddity is $m(-x, y) = -m(x, y) = m(x, -y)$.

In particular, the division algebras $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$ induce multiplications on S^0, S^1, S^3, S^7.

Theorem (Hopf 1940)**.** *The dimension of a $\mathbb{R}$-division algebra is a power of 2.*

Proof. We look at the map induced by the multiplication m on the associated projective spaces

$$M : \mathbb{RP}^{n-1} \times \mathbb{RP}^{n-1} \to \mathbb{RP}^{n-1}$$

on the cohomology with finite coefficients $\mathbb{F}_2$:

$$M^* : H^\bullet(\mathbb{RP}^{n-1}; \mathbb{F}_2) = \mathbb{F}_2[t]/t^n \to \mathbb{F}_2[u, v]/(u^n, v^n) = H^\bullet(\mathbb{RP}^{n-1} \times \mathbb{RP}^{n-1}; \mathbb{F}_2)$$

where we obviously have $M^*(t) = u + v$, so from $t^n = 0$ we get

$$0 = M^*(t^n) = (u + v)^n = \sum_{k=0}^{n-1} \binom{n}{k} u^k v^{n-k}$$

over $\mathbb{F}_2$, which just means all the binomial coefficients are even. This means n has only even prime factors. $\square$

Definition. *For A a $\mathbb{R}$-division algebra of dimension n, the $2:1$ covering $S(A^2) \to \mathbb{P}(A)$ is called* Hopf fibration. *We study it as element of $\pi_{2n-1}(S^n)$.*

Definition. *For $\varphi : S^{2n-1} \to S^n$ the mapping cone $C_\varphi := S^n \cup_\varphi D^{2n-1}$ has a basepoint, a n-cell α and a $2n$-cell β. The* Hopf invariant *$h(\varphi)$ is defined by the equation $\alpha \cup \alpha = h(\varphi)\beta \in H^\bullet(C_\varphi)$.*

Remark. *The Hopf invariant measures how much the preimages of two points are "linked". For the Hopf fibrations, the Hopf invariant is 1.*

Theorem (Adams, Hopf Invariant One Problem, 1960)**.** *The only maps with Hopf invariant 1 are the Hopf fibrations in dimensions $1, 2, 4, 8$.*

The original proof used delicate analysis of Steenrod operations. A shorter proof of Adams' Theorem was given 1966 by Atiyah, using Adams operations and the (eight-fold) Bott periodicity in real K-theory, which in turn comes from the classification of real Clifford algebras (again an eight-fold symmetry).

Corollary. *The only finite dimensional $\mathbb{R}$-division algebras are of dimensions $1, 2, 4, 8$. The only spheres with multiplication (up to homotopy) are $S^0,\ S^1,\ S^3,\ S^7$, and these are also the only spheres which are parallelizable.*

There is no algebraic proof of this fact!

Remark. *While there are infinitely many finite dimensional $\mathbb{R}$-divison algebras, up to isomorphy, the only commutative associative ones are $\mathbb{R}$ and $\mathbb{C}$, the only non-commutative associative one is $\mathbb{H}$ and the only non-associative one is $\mathbb{O}$.*

5 Exceptional Groups

We remember that one can take a semisimple algebraic group G or a compact Lie group G and associate to it the semisimple Lie algebra of invariant derivations $\mathfrak{g}$, then to any semisimple Lie algebra its root system Φ and to every root system a Dynkin diagram D. The classification of root systems show how to build a root system out of a Dynkin diagram, but a very hard question is how to get a Lie algebra $\mathfrak{g}$ or a group G with prescribed root system Φ. For the "classical groups" this is readily solved, but for exceptional root systems it is not obvious.

The exceptional root systems are $G_2,\ F_4,\ E_6,\ E_7,\ E_8$. They are related to the division algebras $\mathbb{R},\ \mathbb{C},\ \mathbb{H},\ \mathbb{O}$.

One can show that $Aut(\mathbb{O})$ is a group of type G_2 and the automorphisms of $\mathbb{OP}^2$ are a group of type F_4, and that a "complexified version" of $\mathbb{OP}^2$ has automorphism group E_6. The definition of anything like $\mathbb{OP}^2 \otimes \mathbb{H}$ and $\mathbb{OP}^2 \otimes Octonion$ is not straightforward, but it would morally give us groups of type E_7 and E_8. The right way to do this is via Moufang loops and Rosenfeld projective planes.

A very beautiful way of constructing Lie algebras with exceptional type are the Freudenthal-Tits magic squares.

Definition. *A* Jordan algebra *is a (commutative) algebra over a field (of characteristics $\neq 2$) in which the Jordan identity holds:*

$$x^2(xy) = x(x^2y)$$

For a finite-dimensional $\mathbb{R}$-division algebra A denote by $J_3(A)$ the Jordan algebra of 3×3-hermitian matrices, by A_0 the trace-free part and by $\mathfrak{Der}(A)$ the Lie algebra of derivations.

Theorem. *For finite-dimensional $\mathbb{R}$-division algebras A, B we define*

$$L(A, B) := \mathfrak{Der}(A) \oplus \mathfrak{Der}(J_3B) \oplus (A_0 \otimes J_3(B)_0).$$

Then one can observe $L(A, B) = L(B, A)$, which is why this construction is called "magic". Furthermore,

- $L(\mathbb{O}, \mathbb{R})$ *is type* F_4
- $L(\mathbb{O}, \mathbb{C})$ *is type* E_6
- $L(\mathbb{O}, \mathbb{H})$ *is type* E_7
- $L(\mathbb{O}, \mathbb{O})$ *is type* E_8

There are other constructions for L which are obviously symmetric.

Remark. *If one plugs in the split versions of the division algebras (e.g. the split complex numbers), one gets split real forms of exceptional groups.*

Sources: mostly Springer-Veldkamp "Octonions, Jordan Algebras and Exceptional Groups", occasionally: Lam "Noncommutative Algebra", Ebbinghaus et al. "Numbers", Wikipedia, nLab, John Baez' TWF on the Cayley numbers (=octonions).