INTRODUCTION TO ALGEBRAS OVER FIELDS

DARREN YAO

Abstract. In this paper, we introduce the four normed division algebras: the real numbers, complex numbers, quaternions, and octonions. We discuss how the normed division algebras are constructed, their properties, and how they relate to concepts of group, ring, and field theory. Of particular importance here is polynomials over the ring of quaternions, where we will prove some of the basic properties of quaternion polynomials, and compare them to the properties of real and complex polynomials. We also briefly introduce the split composition algebras.

1. Introduction

As is usual for an expository paper, we begin by confusing the reader with an extensive list of nested definitions. Since this paper is about algebras over fields, it should be quite obvious what we will define first:

Definition 1.1. [Bae] Let K be a field, and A be a vector space over K with a binary operation for the product, denoted by the $\cdot$ symbol, or also by juxtaposition with no explicit symbol. Then, A is an **algebra** over K if the following criteria are satisfied:

- Left distributivity: $z \cdot (x + y) = z \cdot x + z \cdot y$
- Right distributivity: $(x + y) \cdot z = x \cdot z + y \cdot z$
- Compatibility with scalars: $(ax) \cdot (by) = (ab)x \cdot y$

Some special cases of algebras that we'll focus on:

Definition 1.2. An algebra A is called a **division algebra** if for any element a and and nonzero element b, there is only one element x in A with $a = bx$ and only one element y in A with $a = yb$. Note that since division algebras don't have to be commutative, x and y do not have to be the same element.

Definition 1.3. [Dix94] A division algebra is **normed** if it takes place over a normed vector space, such that the norm satisfies $|x \cdot y| = |x||y|$ for all $x, y \in A$.

Definition 1.4 (Properties of algebras)**.** Not every algebra satisfies all of these properties; in fact, most don't:

- Commutativity: For any $a, b \in A$, $ab = ba$.
- Associativity (or full associativity): For any $a, b, c \in A$, $a(bc) = (ab)c$
- Alternativity: A weaker form of associativity. For any $a, b \in A$, $(aa)b = a(ab)$, $(ab)a = a(ba)$, and $b(aa) = (ba)a$.
- Power associativity: An even weaker form of associativity. When an element $a \in A$ is performed an operation $\cdot$ by itself, it doesn't matter what order the operations are done. In other words, it means that exponentiation is well-defined.

Similarly to how the kernel and image of a group homomorphism measure the failure of bijectivity, in algebras, we have the associator, which measures the degree to which an algebra fails to be associative. This allows us to determine which of the levels of associativity a given algebra satisfies.

Definition 1.5. The **associator** is a trilinear map $A^3 \to A$: $[a, b, c] = (ab)c - a(bc)$.

Definition 1.6. Some properties of the associator:

- If the associator $[a, b, c]$ is always zero, then the operation in question is associative.
- If the associators $[a, a, b]$, $[a, b, a]$, and $[b, a, a]$ are always zero, then the operation is alternative.
- If the associator $[a, a, a]$ is always zero, then the operation is power associative.

Proposition 1.7. *The associator is alternating (switching the order of two elements changes its sign) if and only if the algebra A is alternative.*

2. The Cayley-Dickson Construction

$\mathbb{R}$ *to* $\mathbb{C}$*.* We are all familiar with the real numbers $\mathbb{R}$, which are a division algebra of dimension 1, and the complex numbers $\mathbb{C}$, a division algebra of dimension 2. However, a lesser known property is how the complex numbers can be generated from the reals. Usually, we express complex numbers in the form $a + bi$, but they can also be written as ordered pairs of real numbers (a, b). Addition of complex numbers is simply done component-wise. Now, there are two other operations that we'll need to define: multiplication and conjugation.

- Multiplication: $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$.
- Conjugation: $(a, b)^* = (a, -b)$.

$\mathbb{C}$ *to* $\mathbb{H}$*.* The quaternions, as implied from the name, are an algebra of dimension 4 generated from the complex numbers in a similar manner to the complex numbers being generated from the real numbers. We write quaternions as pairs of complex numbers (a, b) and (c, d), where $a, b, c, d \in \mathbb{C}$. Once again, addition is done component-wise. Multiplication and conjugation are defined slightly differently. It's important to note that when going from complex numbers to quaternions, commutativity is lost, so the order of multiplication is important in here and in further algebras.

- Multiplication: $(a, b) \cdot (c, d) = (ac - db^*, a^*d + cb)$.
- Conjugation: $(a, b)^* = (a^*, -b)$.

$\mathbb{H}$ *to* $\mathbb{O}$*.* If we define an octonion to be a pair of quaternions, we can apply the same multiplication and conjugation operations that were defined in the Quaternions section above. Thus, the octonions are an algebra of dimension 8. Unlike the quaternions, the octonions do not satisfy associativity; only alternativity.

$\mathbb{O}$ *to* $\mathbb{S}$ *and Beyond.* We can continue this process by defining an element of an algebra to be a pair of elements of the previous algebra, and using the same multiplication and conjugation operations. This is called the **Cayley-Dickson construction**, and can be repeated indefinitely. Following the octonions, the next algebra has dimension 16 and is called the sedenions. The sedenions and all further algebras retain power associativity, but division sometimes behaves unusually due to the existence of nontrivial zero divisors.

Definition 2.1. For an element a of an algebra A, if there exists and x such that $ax = 0$ or $xa = 0$, then x is called a **left zero divisor** or **right zero divisor** of a, respectively. If $x \neq 0$, then x is called a **nontrivial zero divisor** of a.

Theorem 2.2. *$\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, and $\mathbb{O}$ are the only normed division algebras.*

Theorem 2.3. *$\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, and $\mathbb{O}$ are the only alternative division algebras.*

While these are the only normed and alternative division algebras, there exist other division algebras that don't necessarily satisfy these properties. However, we do have the following theorem:

Theorem 2.4. *All division algebras have dimension 1, 2, 4, or 8.*

The proof of this theorem is extremely complicated and requires far too much background knowledge to be included here. The full proof is in John Baez's paper [Bae].

3. Quaternions and the Quaternion Group

We reference the following: [Eim] [Bal]

The quaternions, denoted by $\mathbb{H}$, are usually written in the form $a + bi + cj + dk$, where a, b, c, d are real numbers, and i, j, k are the nonreal quaternion units. The quaternions are a 4-dimensional vector space, with basis $\{1, i, j, k\}$. Let's look at the multiplication table of quaternions:

x	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

This is not a group. However, we can make the quaternions into a group, Q_8, by including the negatives of each basis element.

x	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	i	1	-1	-k	k	j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	j	k	-k	1	-1	-i	i
k	k	-j	j	-j	-i	i	-1	1
-k	-k	k	-j	j	i	-i	1	-1

It should be easy to check from this table that the set $\{1, -1, i, -i, j, -j, k, -k\}$ satisfies all the group axioms: closure, identity, associativity, and invertibility, and is thus a group.

Some additional properties of the quaternion group:

- The center (the normal subgroup of elements that commute with all) of the quaternion group is $\{1, -1\}$.
- The subgroups are as follows: the trivial subgroup $\{1\}$, the center subgroup $\{1, -1\}$, the 4-element subgroups $\{1, -1, i, -i\}$, $\{1, -1, j, -j\}$, $\{1, -1, k, -k\}$, and the group itself $\{1, -1, i, -i, j, -j, k, -k\}$. Each of the 4-element subgroup is isomorphic to the group of complex units. All subgroups are normal.
- The quaternion group is the minimal example of a **Hamiltonian group**, which is a non-abelian group such that all of its subgroups are normal.

4. Quaternion Polynomials

Polynomials over $\mathbb{H}$ behave somewhat differently from polynomials over $\mathbb{R}$ or $\mathbb{C}$, because of $\mathbb{H}$'s noncommutativity. Let's first look at some properties of polynomials over $\mathbb{R}$ and $\mathbb{C}$, which are largely similar, and then we can compare these to polynomials over $\mathbb{H}$.

- The **evaluation** of a polynomial $f(x) = \sum_{i=0}^{n} a_i x^i$ at $x = r$ is $\sum_{i=0}^{n} a_i r^i$.
- Remainder theorem: The value r is a root of the polynomial $f(x)$ if $f(x) = g(x)(x-r)$ for some polynomial $g(x)$
- Factor theorem: If $f(x) = g(x)h(x)$ is a polynomial, than an element r is a root of $f(x)$ if and only if it is a root of either $g(x)$ or $h(x)$.
- Fundamental theorem of algebra: Every polynomial with real or complex coefficients of degree d has a maximum of d real or complex roots (exactly d roots up to multiplicity).

There is an analogue in the division algebras for each of the above properties and theorems, but obviously, they differ from their real and complex counterparts. Here, we introduce these theorems over a (not necessarily commutative) division algebra. This is primarily because the quaternions are noncommutative, which breaks many assumptions we usually rely on.

Definition 4.1. Let A be a division algebra, then $A[x]$ is the **polynomial algebra** with indeterminate variable x and coefficients from A, such that x commutes with the coefficients. This means that each polynomial $f(x) \in A[x]$ is of the form $f(x) = \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n} x^i a_i$.

Polynomials over the quaternions work much differently than polynomials over the reals and complex numbers. Similarly to how normal polynomials, we can evaluate a quaternion polynomial at a value of x.

Definition 4.2. Let $f(x) \in A[x]$, then for elements $r \in A$, the **(right) evaluation** of f is the map $A[x] \to A$ that maps $f(x)$ to $f(r)$. As expected, we call an element r a **(right) root** of $f(x)$ if $f(r) = 0$. Left evaluations and left roots are very similar, but we ignore them here because they are essentially equivalent, just on the other side.

Theorem 4.3 (Remainder theorem)**.** *Over an algebra A, an element $r \in A$ is a right root of a nonzero polynomial if $f(x) = g(x)(x - r)$ for some polynomial $g(x) \in R[x]$.*

Note that since the quaternions are noncommutative, $g(x)(x - r) \neq (x - r)g(x)$, so this only works in one direction.

Proof. $\leftarrow$ Let $f(x) = \sum_{i=0}^{n} a_i x^i (x - r) = \sum_{i=0}^{n} a_i x^{i+1} - \sum_{i=0}^{n} a_i r x^i$. Then we plug in $x = r$ to get $f(r) = \sum_{i=0}^{n} a_i r^{i+1} - \sum i = 0^n a_i r r^i = 0$, so r is a root of $f(x)$.

$\rightarrow$ We write $f(x) = g(x)(x - r) + s$, for constant s, by properties of polynomial division. From the first direction, we know that $r | g(x)(x - r)$, so $f(r) = s = 0$. ■

Theorem 4.4 (Factor theorem)**.** *Over an algebra A, an element $r \in A$ is a root of $f(x) = g(x)h(x)$ iff either r is a root of $h(x)$, or a conjugate of r is a root of $g(x)$.*

This differs from the factor theorem over complex numbers in that the quaternions are not commutative, but rather anticommutative, hence the roots of $g(x)$ must be conjugated.

Proof. Let $g(x) = \sum_{i=0}^{n} b_i x^i$, then $f(x) = (\sum_{i=0}^{n} b_i x_i)h(x) = \sum_{i=0}^{n} b_i h(x) x^i$. If $h(r) = 0$, then $f(r) = 0$. Now suppose $f(r) = 0$ and $h(r)$ is nonzero, let's call it a. Then $f(r) = \sum_{i=0}^{n} b_i h(r) r^i = \sum_{i=0}^{n} b_i a r^i a^{-1} a = \sum_{i=0}^{n} b_i (a r a^{-1})^i a = g(a r a^{-1}) h(r)$. Since $f(r) = 0$ and $h(r) \neq 0$, $g(a r a^{-1}) = 0$. ■

Theorem 4.5 (Fundamental theorem of algebra)**.** *For a polynomial $f(x)$ over $A[x]$ of degree d, there is no upper bound on the number of roots, but the roots must come from at most d distinct conjugacy classes.*

Proof. We use proof by induction. The base case $d = 1$ is trivial. For $d \geq 2$, let r be a root of $f(x)$, then $f(x) = g(x)(x - r)$. Then let s be a distinct root of $f(x)$. Then a conjugate of s is a root of $g(x)$. By the induction hypothesis, r lies in one of the $\leq d - 1$ distinct conjugacy classes of roots of $g(x)$. ■

Let's look at some examples. In the division ring of quaternions, $x^2 + 1 = 0$ has three roots: i, j, k. However, for any two roots r_1, r_2, within the same conjugacy class, there exists an element a such that $ar_1a^{-1} = r_2$. Applying this, we see that the roots of $x^2 + 1 = 0$ fall into two or fewer conjugacy classes, satisfying Theorem 4.5.

Definition 4.6. A division algebra is **(right) algebraically closed** if every nonconstant polynomial has a (right) root.

Theorem 4.7. *The quaternions $\mathbb{H}$ are right algebraically closed.*

The proof of this theorem is rather long, so it will not be presented here, but you can view it at [Ghi]

5. Octonions and Moufang Loops

[GM] [Alb]

The $\pm$ basis vectors of the octonions don't form a group, due to their nonassociativity. However, they do form what is called a Moufang loop. Unfortunately, this means that we need to introduce more definitions.

Definition 5.1. A **quasigroup** is a set with a binary operation such that for each a and b in the set, there exist unique elements x and y in the set such that $a \cdot x = b$ and $y \cdot a = b$.

Definition 5.2. A **loop** is a quasigroup with an identity element.

Definition 5.3. A **Moufang loop** is a loop that satisfies the following four identities for any elements x, y, z in the loop:

- $z(x(zy)) = ((zx)z)y$
- $x(z(yz)) = ((xz)y)z$
- $(zx)(yz) = (z(xy))z$
- $(zx)(yz) = x((xy)z)$

In fact, a Moufang loop can be thought of as a group that only satisfies alternativity; a Moufang loop that satisfies full associativity is a group.

If we take all the octonions of unit norm, they form a hypersphere of dimension 8. This follows from the definition of unit norm; it consists of all points that are a distance of 1 away from the center.

6. Split composition algebras

The split complex numbers are a number system similar to that of the regular complex numbers, but written as $z = a + bj$ where $j^2 = 1$. The split complex numbers form a commutative, associative algebra over the real numbers. The split complex numbers are not a division algebra nor a field.

Addition is simply done termwise. Other operations are defined as follows:

- Multiplication: $(a+bj)(c+dj) = (ac+bd, bc+ad)$.
- Conjugation: $z^* = a - bj$.

Applying the Cayley Dickson construction to the split complex numbers yields the split quaternions:

x	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	1	-i
k	k	j	i	1

The split quaternions are a 4-dimensional associative algebra. However, unlike the regular quaternions, the split quaternions contain nontrivial zero divisors, and nilpotents, which are nonzero elements that when raised to some positive integer power, equal zero. For example, $(i-j)^4 = 0$.

Continuing on with this process of generating new algebras gives the split octonions, the split sedenions, and so on, indefinitely. However, since we've already lost many useful properties by going to the split quaternions, we will stop here.

7. Conclusion

The four normed division algebras are the reals, complex numbers, quaternions, and octonions. Most people are familiar with the real numbers and the complex numbers, but less so with the other two; yet they have applications to many fields. For example, the unit quaternions are used to represent rotations, to prove Lagrange's four-square theorem, in addition to many applications in physics and computer graphics. Both the quaternions and octonions are used in the construction of mathematical objects like exceptional Lie groups and projective planes. The octonions are related to the 26 sporadic simple groups, and many problems in physics. In general, the concept of algebras over fields provides a framework for understanding other concepts in mathematics and physics.

References

[Alb] A. A. Albert. On nonassociative division algebras. *American Mathematical Society.*

[Bae] John C. Baez. The octonions. *American Mathematical Society.*

[Bal] Serge Baliff. Polynomial functions and the quaternions. *Pennsylvania State University.*

[Dix94] Geoffrey M. Dixon. *Division Algebras: Octonions, Quaternions, Complex Numbers and the Algebraic Design of Physics.* Springer, 1994.

[Eim] Rob Eimerl. The quaternions and their applications. *University of Puget Sound.*

[Ghi] Riccardo Ghiloni. The classification of algebraically closed alternative division rings of finite central dimension.

[GM] B. Gordon and T. S. Motzkin. On the zeros of polynomials over division rings. *American Mathematical Society.*

Email address: darren.yao@gmail.com