NONASSOCIATIVE ALGEBRAS

PETE L. CLARK

Contents

1. Introduction to Non-Associative Algebras

1.1. First definitions.

Let F be a field. By an **algebra** $A_{/F}$, we mean an F-vector space endowed with an F-bilinear product $\cdot : A \cdot A \rightarrow A$. We usually denote the product of x and y as xy.

If A, A' are F-algebras, then a morphism $\varphi : A \rightarrow A'$ is simply an F-linear map such that for all $x, y \in A$, $\varphi(xy) = \varphi(x)\varphi(y)$. In this way, we obtain a category of F-algebras. We have the usual constructions of direct sums and tensor products.

An F-algebra A is **commutative** if for all $x, y \in A$, we have $xy = yx$. More on commutativity in §1.5.

An F-algebra A is **associative** if for all $x, y, z \in A$, we have $(xy)z = x(yz)$. More on associativity in §1.6.

Thanks to Jeroen Schillewaert for catching an error in an exercise.

An F-algebra is **unital** if there exists $e \in A$ such that e such that for all $x \in A$, $ex = xe = x$, i.e., a two-sided multiplicative identity.[1] In the sequel we will mainly be concerned with unital F-algebras, but let us entertain the general case for a little while. Anyway, in some circumstances the lack of unit can be overcome as follows:

Let A be any F-algebra, and let $A_1 = F \times A$ as an F-vector space, endowed with the following product: for $(\alpha, a), (\beta, b) \in F \times A$, put

$$(\alpha, a) \cdot (\beta, b) = (\alpha\beta, \beta a + \alpha b + ab).$$

Then A_1 is an F-algebra with identity element $e = (1, 0)$. Moreover, $0 \times A$ is an ideal in A_1 that is isomorphic as an F-algebra to A itself. Moreover, A_1 is commutative (resp. associative, resp. finite-dimensional) iff A is.

Exercise 1.1. *Let A be a one-dimensional F-algebra. Show that either $\{xy \mid x, y \in A\} = 0$ or $A \cong F$. In particular, A is commutative and associative.*

Exercise 1.2. *For any field F, exhibit a 2-dimensional F-algebra which* has none of *the following properties: unital, commutative, associative.*

For an F-algebra A, we define its **opposite algebra** A^{op}, which has the same underlying F-vector space as A but with a new bilinear product: $x \bullet y := yx$.

1.2. Structure constants.

We are especially interested in the case in which A is finite-dimensional as an F-vector space. In such a situation, it is useful to fix a single n-dimensional vector space $V = \bigoplus_{i=1}^n e_i F$ over F and consider all possible algebra structures on V. Obviously any n-dimensional F-algebra is isomorphic to some F-algebra with underlying vector space F, although possibly in many different ways. For $n \in \mathbb{Z}^+$, let $\mathcal{A}_n(F)$ be the set of all F-algebras with underlying vector space V.

We claim that $\mathcal{A}_n(F)$ has the natural structure of an affine space over F of dimension n^3. Indeed, to specify an F-algebra structure A on $V = \bigoplus_{i=1}^n Fe_i$ it is enough to consider its effect on basis elements: specifically, for all $i, j, k \in [1, n]$, there exist unique constants $c_{ij}^k \in F$ such that

$$e_i e_j = \sum_{k=1}^n c_{ij}^k e_k.$$

These n^3 constants c_{ij}^k are called the **structure constants** of the algebra A. Moreover they are freely determined, since bilinear maps $V \times V \to V$ correspond bijectively to F-linear maps from $V \otimes V \to V$ (or, if you like, tensors of type $(2, 1)$ on V), which is clearly an F-vector space of dimension n^3.

1.3. Base extension.

Let A be an F-algebra and K/F a field extension. Then we may form the algebra $A_K := A \otimes_F K$, which we may then regard as an algebra over K, with $\dim_K(A_K) = \dim_F(A)$. In particular, tensoring with K gives an injective map

[1] Any F-algebra has at most one identity e. These notes are intended for readers whose intelligence would be insulted if this were set as a formal exercise.

$\mathcal{A}_n(F) \hookrightarrow \mathcal{A}_n(K)$, which may be regarded as the usual extension of scalars construction on $\mathbb{A}^{n^3}$.

Note that in the case that A is finite-dimensional, the base extension $A_{/K}$ can be described as the bilinear product on $V_K = \bigoplus_{i=1}^n e_i K$ with the *same* structure constants as A, i.e., for all i, j, k, $c_{i,j}^k(A_K) = c_{i,j}^k(A)$. This makes it useful to try to express certain algebra properties in terms of structure constants: often doing so makes it obvious that they are preserved under base extension.

1.4. **Unital algebras.**

Suppose that A is an n-dimensional F-algebra with a multiplicative identity 1. Then we may choose the vector space isomorphism $A \to \bigoplus_{i=1}^n e_i F$ such that 1 maps to the first basis element e_1. In this way, the unital n-dimensional F-algebras with underlying space V become a subset of $\mathbb{A}^{n^3}$. Let us call this subset $\mathrm{Alg}_n(F)$. It is easy to identify it explicitly: e_1 is a unit for a bilinear product on V iff both of the following hold:

- for all $j, k \in [1, n]$, $c_{1j}^k = \delta(j, k)$ and
- for all $i, k \in [1, n]$, $c_{i1}^k = \delta(i, k)$,

where $\delta(i, j)$ is the "Kronecker delta": equal to 1 if the arguments are equal, otherwise 0. From this it follows easily that $\mathrm{Alg}_n(F)$ is a linear subspace of $\mathcal{A}_n(F)$ of dimension $n(n-1)^2$.

1.5. **Commutativity.**

An F-algebra A is **commutative** if for all $x, y \in A$, $xy = yx$. In this section we wish to give a simple analysis of the condition of commutativity and, in particular, show that it can be usefully recast in terms of commutators.

To start from the beginning: given an F-algebra A, we would like to be able to verify whether it is commutative. On the face of it, this involves verifying $\#A \times A$ different equalities, i.e., infinitely many if A is infinite (as it usually will be). Evidently we want a simpler way to proceed. In fact it suffices to verify commutativity on basis elements, which at least in the case of a finite dimensional F-algebra, reduces us to a finite problem. To establish this claim, we begin by introducing the following formalism.

For elements x, y in any F-algebra A, we define their **commutator**

$$[x, y] = xy - yx. \tag{1}$$

Thus x and y commute – i.e., $xy = yx$ – iff $[x, y] = 0$, and therefore an algebra is commutative iff all its commutators are zero.

One may wonder what we have gained here. The answer is that by introducing the commutator we have *linearized* our situation. Indeed, viewing the commutator as a map $A \times A \to A$, one immediately verifies that it is F-bilinear: that is, for all $x, y, z \in A$ and $\alpha \in F$, we have

$$[\alpha x + y, z] = \alpha[x, z] + [y, z] \tag{2}$$

and

$$[x, \alpha y + z] = [x, z] + \alpha[y, z]. \tag{3}$$

For instance, the following calculation verifies (2):

$$[\alpha x + y, z] = (\alpha x + y)z - z(\alpha x + y) = \alpha(xz - xz) + (yz - zy) = \alpha[x, z] + [y, z].$$

Equation (3) can be checked just as easily. However, it is probably more insightful to observe that it follows from (2) and the fact that the commutator is an **alternating** multilinear map: recall that a multilinear map $L : V^n \rightarrow W$ is alternating if $L(v_1, \ldots, v_n) = 0$ whenever there exist indices $i \neq j$ such that $v_i = v_j$. In this case we are simply asserting that for all $x \in A$,

$$[x, x] = xx - xx = 0.$$

Note that an alternating multilinear map is necessarily skew-symmetric, i.e., if we interchange two of the arguments, we introduce a minus sign in the answer. The verification of this reduces to the case of an alternating bilinear form $L : V^2 \rightarrow W$ (any n-linear form with $n \geq 3$ becomes a bilinear form when we evaluate at any fixed elements the other $n - 2$ places): for all $x, y \in V$,

$$0 = L(x + y, x + y) = L(x, x) + L(x, y) + L(y, x) + L(y, y) = L(x, y) + L(y, x),$$

so

$$L(y, x) = -L(x, y).$$

The converse holds so long as the characteristic of F is not 2: if $L : V^2 \rightarrow W$ is skew-symmetric, then for any $x \in V$, $L(x, x) = -L(x, x)$, so $2L(x, x) = 0$. Conversely, in characteristic 2, skew-symmetric is the same as symmetric, which is strictly weaker than being alternating.

The bilinearity of the commutator map is the key to the following result.

Proposition 1.1. *Let $A_{/F}$ be an F-algebra, with basis $\{e_i\}_{i \in I}$. Then A is commutative iff for all $i, j \in I$, $e_i e_j = e_j e_i$.*

Proof. Let $x, y \in A$, and write them in terms of the given F-basis: $x = \sum_{i \in I} x_i e_i$, $y = \sum_{i \in I} x_i e_i$ (of course x_i and y_i are both zero except for finitely many indices). Then

$$[x, y] = [\sum_i x_i e_i, \sum_j y_j e_j] = \sum_{i,j} x_i y_j [e_i, e_j] = 0,$$

by our assumption that basis elements commute. □

In case A is an n-dimensional algebra with underlying vector space V, the previous result amounts to the fact that the commutativity of F is equivalent to the following symmetry relations on the structure coefficients: $\forall i, j, k$, $c_{ij}^k = c_{ji}^k$.

Exercise 1.3. *Show: the loci of commutative algebra structures on V is a linear subspace of $\mathcal{A}_n$, and compute its dimension. Do the same for unital algebra structures.*

Corollary 1.2. *Let A be an F-algebra and K/F a field extension. Then A is commutative iff $A_{/K}$ is commutative.*

Proof. One can choose an F-basis of $\{e_i\}$ of A, note that under scalar extension $\{e_i \otimes 1\}$ is a K-basis of A_K and apply Proposition 1.1. Alternately and perhaps more directly, this amounts to the fact that a bilinear map on an F-vector space is identically zero iff its scalar extension to K is identically zero, which is clear. □

Center: For any F-algebra A, define the **center** $Z(A)$ to be the set of all $x \in A$ which commute with every element of A: equivalently, the set of $x \in A$ such that the associated F-linear map $\operatorname{ad} a : x \mapsto [a, x]$ is identically zero.

Proposition 1.3. *The center $Z(A)$ of A is a commutative F-subalgebra of A.*

Exercise 1.4. *Prove Proposition 1.3.*

Exercise 1.5. *Use commutators to show that any two-dimensional F-algebra with identity is commutative.*

Exercise 1.6. *a) Show that every commutative F-algebra is isomorphic to its opposite algebra.*
b) Is the converse true?

1.6. **Associativity.**

The constructions of the previous section are quite familiar, to the extent that their interpretation via commutators and multilinear algebra may seem heavy-handed. However the merits of this approach is that it has analogues for several other important classes of algebras, including associativity.

An algebra $A_{/F}$ is **associative** if for all $x, y, z \in F$, $(xy)z = x(yz)$.

Proposition 1.4. *Let $A_{/F}$ be an algebra $x_1, \ldots, x_n \in F$ with $n \geq 2$.*
a) There are $C_{n-1} = \frac{(2n-1)!}{n!(n-1)!}$ syntactically correct ways of inserting parentheses into the expression $x_1 \cdots x_n$ so as to resolve this into a product of binary multiplications.
b) If A is associative, then all C_{n-1} possible choices of parentheses evaluate to the same element of A.

Exercise 1.7. *a) Prove Proposition 1.4.*
b) Show: there are algebras in which these expressions yield C_{n-1} distinct elements.*

Again in direct analogy with commutativity, for any elements x, y, z in an F-algebra A, we define their **associator**

$$[x, y, z] = (xy)z - x(yz).$$

Exercise 1.8. *Let 1 be a two-sided multiplicative identity of A. Show: an associator $[x, y, z]$ in which at least one of x, y, z is equal to 1 evaluates to zero in A.*

Evidently x, y, z "associate" iff their associator is zero. More usefully, the associativity of A is equivalent to the identical vanishing of all associators. Again, the point of this construction is as follows:

Proposition 1.5. *For an F-algebra A, the associator is an F-trilinear map $A^3 \to A$.*

Exercise 1.9. *Prove Proposition 1.5.*

Corollary 1.6. *Let $A_{/F}$ be an F-algebra, with basis $\{e_i\}_{i \in I}$.*
a) A is associative iff for all $i, j \in I$, $(e_i e_j)e_k = e_i(e_j e_k)$.
b) Let K/F be a field extension. Then the scalar extension $A_{/K}$ is associative iff A is associative.

Exercise 1.10. *Prove Corollary 1.6.*

Exercise 1.11. *Use associators to show that any two-dimensional F-algebra with identity is associative.*

Exercise 1.12. *Let A be a two-dimensional F-algebra with identity element 1. By the above exercises, A is commutative and associative. Choose $x \in A \setminus F \cdot 1$, and let $a, b \in F$ be the unique constants such that $x^2 = ax + b \cdot 1$.*
a) Show that $A \cong F[t]/(t^2 - at + b)$.
b) Under what circumstances is A a field? An integral domain? An algebra without nilpotent elements?

Example 1.7. *(Quaternion Algebras): Let F be a field of characteristic different from 2, let $a, b \in F^\times$. We will define a 4-dimensional unital F-algebra $B = B(a,b)_{/F}$ on $V = \bigoplus_{i=1}^r e_i F$ explicitly in terms of structure constants. Namely, we put:*

$e_1 \cdot e_j = e_j$ *for all* j;
$e_2 \cdot e_2 = a$;
$e_3 \cdot e_3 = b$;
$e_4 \cdot e_4 = -ab$;
$e_2 \cdot e_3 = -e_3 \cdot e_2 = e_4$;
$e_2 \cdot e_4 = -e_4 \cdot e_2 = ae_3$.
$e_3 \cdot e_4 = -e_4 \cdot e_3 = -be_2$.

Note that any two basis elements e_i, e_j with $i, j > 1$ anticommute: $e_i e_j = e_j e_i$. (In particular, B is not *a commutative algebra.)*

Let us check by brute force that B is associative: this means checking that for all $4^3 = 64$ triples of basis elements we have $[e_i, e_j, e_k] = 0$. Well, let's cut down the computations a bit: since e_1 is indeed a two-sided identity, by Exercise 1.8 any of the associators involving e_1 will vanish. This leaves us to check the 27 associators involving only e_2, e_3, e_4. Obviously all the associators of the form $[e_i, e_i, e_i]$ are going to vanish, so that leaves us with 24 choices. That's not so bad:

$[e_2, e_2, e_3] = (e_2e_2)e_3 - e_2(e_2e_3) = ae_3 - e_2e_4 = ae_3 - ae_3 = 0.$
$[e_2, e_2, e_4] = (e_2e_2)e_4 - e_2(e_2e_4) = ae_4 - ae_2e_3 = ae_4 - ae_4 = 0.$
$[e_2, e_3, e_2] = (e_2e_3)e_2 - e_2(e_3e_2) = e_4e_2 - e_2e_4 = 0.$
$[e_2, e_3, e_3] = (e_2e_3)e_3 - e_2(e_3e_3) = e_4e_3 - be_2 = be_2 - be_2 = 0.$
$[e_2, e_3, e_4] = (e_2e_3)e_4 - e_2(e_3e_4) = e_4e_4 - be_2e_2 = -ab + ab = 0.$
$[e_2, e_4, e_2] = (e_2e_4)e_2 - e_2(e_4e_2) = -ae_3e_2 - ae_2e_3 = 0.$
$[e_2, e_4, e_3] = (e_2e_4)e_3 - e_2(e_4e_3) = ae_3e_3 - be_2e_2 = ab - ba = 0.$
$[e_2, e_4, e_4] = (e_2e_4)e_4 - e_2(e_4e_4) = ae_3e_4 + abe_2 = -abe_2 + abe_2 = 0.$
$[e_3, e_2, e_2] = (e_3e_2)e_2 - e_3(e_2e_2) = -e_4e_2 - ae_3 = ae_3 - ae_3 = 0.$
$[e_3, e_2, e_3] = (e_3e_2)e_3 - e_3(e_2e_3) = -e_4e_3 - e_3e_4 = e_3e_4 - e_3e_4 = 0.$
$[e_3, e_2, e_4] = (e_3e_2)e_4 - e_3(e_2e_4) = -e_4e_4 - ae_3e_3 = ab - ab = 0.$

$[e_3,e_3,e_2]=(e_3e_3)e_2-e_3(e_3e_2)=be_2+e_3e_4=be_2-be_2=0.$
$[e_3,e_3,e_4]=(e_3e_3)e_4-e_3(e_3e_4)=be_4+be_3e_2=be_4-be_4=0.$
$[e_3,e_4,e_2]=(e_3e_4)e_2-e_3(e_4e_2)=-be_2e_2+ae_3a_3=-ab+ab=0.$
$[e_3,e_4,e_3]=(e_3e_4)e_3-e_3(e_4e_3)=-be_2e_3-be_2e_2=0.$
$[e_3,e_4,e_4]=(e_3e_4)e_4-e_3(e_4e_4)=-be_2e_4+abe_3=-abe_3+abe_3=0.$
$[e_4,e_2,e_2]=(e_4e_2)e_2-e_4(e_2e_2)=-ae_3e_2-ae_4=ae_4-ae_4=0.$
$[e_4,e_2,e_3]=(e_4e_2)e_3-e_4(e_2e_3)=-ae_3e_3-e_4e_4=-ab+ab=0.$
$[e_4,e_2,e_4]=(e_4e_2)e_4-e_4(e_2e_4)=-ae_3e_4-ae_4e_3=0.$
$[e_4,e_3,e_2]=(e_4e_3)e_2-e_4(e_3e_2)=be_2e_2-e_4e_4=-ab+ab=0.$
$[e_4,e_3,e_3]=(e_4e_3)e_3-e_4(e_3e_3)=be_2e_3-be_4=be_4-be_4=0.$
$[e_4,e_3,e_4]=(e_4e_3)e_4-e_4(e_3e_4)=be_2e_4-be_4e_2=0.$
$[e_4,e_4,e_2]=(e_4e_4)e_2-e_4(e_4e_2)=-abe_2+ae_4e_3=-abe_2+abe_2=0.$
$[e_4,e_4,e_3]=(e_4e_4)e_3-e_4(e_4e_3)=-abe_3+be_4e_2=abe_3-abe_3=0.$

Exercise 1.13. *Show:* $Z(B)=e_1\cdot F$.

Exercise 1.14. *Suppose that either* $a=1$ *or* $b=1$. *Show that* $B\cong M_2(F)$.

Example 1.8. *(Quaternion algebras in characteristic* 2*): ...*

Nucleus: For an F-algebra A, define the **nucleus** $\mathrm{Nuc}(A)$ to be the set of all $x\in A$ such that $[x,A,A]=[A,x,A]=[A,A,x]=0$, i.e., the set of all x which "associate with every pair of elements of A".

Exercise 1.15. *Show: the nucleus of an* F*-algebra is an associative subalgebra.*

Exercise 1.16. *Show: an* F*-algebra* A *is associative iff its opposite algebra is associative.*

Exercise 1.17. *Show: a quaternion algebra is isomorphic to its opposite algebra.*

1.7. **Alternativity.** Previously we noted that the commutator $[x,y]$ was, in general, an alternating multilinear form. It is then natural to ask: does the same hold for the associator $[x,y,z]$?

This suggests that it may be worth singling out the class of algebras A for which the F-trilinear associator map $A^3\to A$ is alternating. This condition is equivalent to the conjunction of the following three identities:

(LA) For all $x,y\in A$, $[x,x,y]=0$, i.e., $(xx)y=x(yx)$.
(F) For all $x,y\in A$, $[x,y,x]=0$, i.e., $(xy)x=x(yx)$.
(RA) For all $x,y\in A$, $[x,y,y]=0$, i.e. $(xy)y=x(yy)$.

(LA) and (RA) stand for, respectively, **left alternative** and **right alternative**, whereas (F) stands for **flexible**.[2]

For later use, we introduce some more precise terminology. For distinct indices i,j in $\{1,\ldots,n\}$, say that an n-linear map $L(x)=L(x_1,\ldots,x_n)$ is (ij)-skew symmetric if interchanging the ith and jth indices of any vector x introduces a minus sign in the map. A trilinear map is evidently skew-symmetric in the above sense iff it is (12)-skew symmetric and (23)-skew symmetric. Now we claim that property

[2]No, I don't why an algebra satisfying this identity is called flexible, but it is standard.

(LA) implies the alternator is (12)-skew symmetric and property (RA) implies the alternator is (23)-skew symmetric. Indeed, for $x, y, z \in A$, (LA) implies

$$0 = [x + y, x + y, z] = [x, x, z] + [x, y, z] + [y, x, z] + [y, y, z] = [x, y, z] + [y, x, z],$$

so $[y, x, z] = -[x, y, z]$. Similarly (RA) implies

$$0 = [x, y + z, y + z] = [x, y, y] + [x, y, z] + [x, z, y] + [x, z, z] = [x, y, z] + [x, z, y],$$

so $[x, z, y] = -[x, y, z]$.

Lemma 1.9. *An F-algebra A which satisfies any two of the properties (LA), (RA), (F) also satisfies the third. Such an algebra is called **alternating**.*

Proof. Let x, y be any elements of A.
If A satisfies (LA) and (RA) it is skew symmetric, so $[x, y, x] = -[x, x, y] = 0$.
If A satisfies (LA) and (F) it is (12)-skew symmetric, so $[x, y, y] = -[y, x, y] = 0$.
If A satisfies (RA) and (F) it is (23)-skew symmetric, so $[x, x, y] = -[x, y, x] = 0$. □

Exercise 1.18. *Let F be a field. Exhibit three algebras over F each satisfying exactly one of the three properties of Lemma 1.9 above.*

Exercise 1.19. *Let A be an F-algebra.*
a) Suppose that the characteristic of F is not 2. Show that if the alternator is skew-symmetric, then it is alternating.
b) Give an example of an F-algebra A for which the alternator is skew-symmetric but not alternating.

Exercise 1.20. *a) Let $A = e_1F \oplus e_2F$ be the F-algebra with multiplication table $e_1e_1 = e_1e_2 = e_2e_1 = e_2$, $e_2e_2 = e_1$. Show that A is not alternative.*
b) By the previous exercises, every unital 2-dimensional F-algebra is associative, so certainly alternative. Use part a) to build a 3-dimensionial unital F-algebra which is not alternative.

Exercise 1.21. *Let V and W by K-vector spaces and $L : V^n \to W$ an n-linear map. Let $\sigma \in S_n$. For $x = (x_1, \ldots, x_n) \in V^n$, put $\sigma(x) = (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. We say that L is σ-skew symmetric if for all $x \in V^n$, $L(\sigma(x)) = \operatorname{sgn}(\sigma)L(x)$.*
a) Let $\{e_i\}_{i \in I}$ be any K-basis for V. Suppose that for all vectors x each of whose components is a basis element e_i we have $L(\sigma(x)) = \operatorname{sgn}(\sigma)L(x)$. Show that L is σ-skew symmetric.
b) Deduce that if K/F is a base extension, L is σ-skew symmetric iff its scalar extension $L_K : V^n \otimes K \to W \otimes K$ is σ-skew symmetric.
c) Let $A_{/K}$ be an F-algebra with a F-basis $\{e_i\}_{i \in I}$. Show that to check skew symmetry of the alternator map $A^3 \to A$, it is enough to check that for all $i, j, k \in I$,

$$[e_j, e_i, e_k] + [e_i, e_j, e_k] = [e_i, e_k, e_j] + [e_i, e_j, e_k] = 0.$$

In particular, if F has characteristic not 2, this shows that the alternating property can be checked on basis elements and thus that a scalar extension of an alternating algebra is alternating.
d) Let F be a field of characteristic 2. Exhibit an F-algebra A with an F-basis $\{e_i\}_{i \in I}$ such that for all $i, j \in I$, $[e_i, e_i, e_j] = [e_i, e_j, e_j] = 0$ but A is not alternating.

Nevertheless:

Proposition 1.10. *Let V and W be an F-vector spaces and $L : V^n \to W$ be an alternating n-linear map.*
a) For any field extension K/F, the scalar extension L_K is alternating.
b) It follows that if A is an alternating F-algebra and K/F is a field extension, then $A_{/K}$ is alternating.

Proof. Let $1 \leq i < j \leq n$. Say that L is (ij)-alternating if for any vector $x = (x_1, \ldots, x_n)$ with $x_i = x_j$, $L(x) = 0$. Clearly L is alternating iff it is (ij)-alternating for all pairs $i < j$. Let $E = \{e_i\}_{i \in I}$ be an F-basis for V. Suppose that $L(x) = 0$ for all vectors x with $x_i = x_j$ and for all $k \notin \{i, j\}$, $x_k \in E$ is a basis element. Then it is easy to see that L is (ij)-alternating. Thus we reduce to the case of $n = 2$.

For this, we calculate explicitly: any $x \in V_K$ may be written as $\sum_i x_i e_i$ with $x_i \in K$. Thus

$$[x, x] = [\sum_i x_i e_i, \sum_i x_i e_i] = \sum_i x_i^2 [e_i, e_i] + \sum_{i \neq j} x_i x_j [e_i, e_j].$$

The first term is zero since $L : V^2 \to W$ is alternating. As for the second, upon putting a total ordering on I, we may rewrite it as $\sum_{i<j} x_i x_j ([e_i, e_j] + [e_j, e_i])$. Since L is alternating, hence skew-symmetric, this latter term is also zero. □

Exercise 1.22. *Show: an algebra A is alternative iff its opposite algebra is alternative.*

Proposition 1.11. *In any alternative F-algebra A, the* ***Moufang identities*** *hold: for all $a, x, y \in A$, we have*

$$(xax)y = x(a(xy)), \tag{4}$$

$$y(xax) = ((yx)a)x, \tag{5}$$

$$(xy)(ax) = x(ya)x. \tag{6}$$

Moreover, in any F-algebra A, (6) holds iff for all $a, x, y \in A$ we have

$$[y, xa, x] = -[y, x, a]x. \tag{7}$$

Remark: Since alternative algebras are flexible, the expression xax is unambiguous.

Proof. Let $a, x, y \in A$. Then

$$\begin{aligned}(xax)y - x(a(xy)) &= [xa, x, y] + [x, a, xy] = -[x, xa, y] - [x, xy, a] \\ &= -(x(xa))y + x((xa)y) - (x(xy))a + x((xy)a) \\ &= -[x^2, a, y] - [x^2, y, a] - x^2(ay) - x^2(ya) + x((xa)y) + (xy)a) \\ &= x(-x(ay) - x(ya) + (xa)y + (xy)a) \\ &= x([x, a, y] + [x, y, a]) = 0,\end{aligned}$$

establishing (4). By Exercise 1.22, A^{op} is also alternating, and the identity (4) in A^{op} is equivalent to the identity (5) in A. Using (4) we have

$$\begin{aligned}(xy)(ax) - x(ya)x &= [x, y, ax] + x(y(ax) - (ya)x) \\ &= -[x, ax, y] - x[y, a, x] = -(xax)y + x((ax)y - [y, a, x]) \\ &= -x(a(xy) - (ax)y + [y, a, x]) = -x(-[a, x, y] + [y, a, x]) = 0,\end{aligned}$$

establishing (6). Finally, assuming (4) we get

$$[y, xa, x] = (y(xa))x - y(xax) = (y(xa))x - ((yx)a)x = -[y, x, a]x$$

and conversely assuming (7) gives (4). □

Lemma 1.12. *Let A be an F-algebra in which (7) holds: i.e., for all $a, x, y \in A$,*

$$[y, xa, x] = -[y, x, a]x.$$

Then for all $a, x, y, z \in A$ we have

$$[y, xa, z] + [y, za, x] = -[y, x, a]z - [y, z, a]x. \tag{8}$$

Proof. Observe that the identity (7) is *quadratic* in x. In such cases there is a corresponding **linearized** identity: i.e., we replace the identity $\forall x \in V$, $P(x) = 0$ with the identity $\forall x, z \in V^2$, $P(x+z) - P(x) - P(z) = 0$. Applying this to (7) we get

$$0 = [y, xa+za, x+z]+[y, x+z, a](x+z)-[y, xa, x]-[y, x, a]x-[y, za, z]-[y, z, a]z$$

$$= [y, xa, z] + [y, za, x] + [y, x, a]z + [y, z, a]x = 0.$$

□

Theorem 1.13. *(E. Artin) Let A be an alternative F-algebra and $x, y \in A$. Then the F-subalgebra generated by x and y is associative.*

Proof. We denote by $p(x, y), q(x, y), r(x, y)$ any products of t elements $z_1 \cdots z_t$ – i.e., possibly a diferent element for each of the C_{t-1} possible choices of parentheses – with each z_i equal to either x or y. For such an expression $p(x, y)$ we define its degree δp to be t, i.e., the number of terms in the product: we assume that $t \geq 1$. It is enough to show that all of the associators $[p, q, r]$ vanish.

We go by induction on $N = \delta p + \delta q + \delta r$. The result holds vacuously for $N < 3$. By induction, we suppose that it holds for all triples with degree sum less than N. In particular then $\delta p < N$, so that by induction the insertion of the parentheses in $p(x, y)$ is immaterial. Now some two of p, q, r must begin with the same letter, say x. Since associators alternate, we may assume that $q(x, y)$ and $r(x, y)$ both begin with x.

Case 1: $\delta q = \delta r = 1$. Then $[p, q, r] = [p, x, x] = 0$.

Case 2: $\delta q > 1$, $\delta r = 1$. Then, by (7), $[p, q, r] = [p, xq', x] = -[p, x, q']x = 0$ by induction.

Case 3: If $\delta q = 1$, $\delta r > 1$, then using (23)-skew symmetry of alternators we reduce to Case 2.

Case 4: Finally, suppose $\delta q, \delta r > 1$, and put $q = xq'$, $r = xr'$.

$$[p, q, r] = [p, xq', xr'] = -[xr', xq', p]$$

$$= [xr', pq', x] + [xr', x, q']p + [xr', p, q'] = -[pq', xr', x] = [pq', x, r']x = 0.$$

Here we have used, in order, (13)-skew symmetry, (8), the induction hypothesis, (12)-skew symmetry, and (7), and the induction hypothesis once again. □

An F-algebra A is **power-associative** if for all $x \in A$ and any $n \in \mathbb{Z}^+$, any of the C_{n-1} different ways of parenthesizing x^n give rise to the same answer. Equivalently, A is power-associative if for each $x \in A$, the F-subalgebra generated by x is associative. In lieu of the previous sentence, we get an immediate corollary to Artin's Theorem.

Corollary 1.14. *An alternative algebra is power-associative.*

Example (Octonion Algebras in characteristic not 2): ...

Example (Octonion Algebras in characteristic 2): ...

2. Composition Algebras

To fix ideas we assume throughout most of this section that F is a ground field with characteristic different from 2. At the end of the section we discuss modifications for the characteristic 2 case.

The following is our preliminary definition of composition algebra.

Definition: A **composition algebra over F** is a pair (C, N), where C is a unital F-algebra[3] and $N : C \to F$ is a nondegenerate quadratic form on C such that for all $x, y \in C$, $N(xy) = N(x)N(y)$.

2.1. **Hurwitz's Theorem.**

Many of the algebras we met in §1 are composition algebras. Indeed:

Example 2.1: F is a composition F-algebra.

Example 2.2: Binion algebras $(\frac{\alpha}{F})$.

Example 2.3: Quaternion algebras $(\frac{\alpha,\beta}{F})$.

Example 2.4: Octonion algebras $(\frac{\alpha,\beta,\gamma}{F})$.

Remarkably, every composition algebra over a field F (of characteristic not 2) is isomorphic to one of the algebras given in the above examples. Namely, we have the following theorem, whose proof will be given later in the section.

Theorem 2.1. *(Hurwitz Classification of Composition Algebras)*
Let $C_{/F}$ be a composition algebra. Then $\dim C \in \{1, 2, 4, 8\}$. Moreover:
a) If $\dim C = 1$, then $C = F$. With respect to the basis 1 of C, the norm form is

$$N(x) = x^2.$$

b) If $\dim C = 2$, there exists $\alpha \in F^\times$ such that $C \cong \left(\frac{\alpha}{F}\right) = F[t]/(t^2 - \alpha)$. With respect to the basis $1, \alpha$ of C, the norm form is

$$N = N(x_1, x_2) = x_1^2 - \alpha x_2^2.$$

c) If $\dim C = 4$, there exist $\alpha, \beta \in F^\times$ such that C is isomorphic to the quaternion algebra $B(\alpha, \beta) = \left(\frac{\alpha,\beta}{F}\right)$. With respect to the standard quaternion basis e_1, e_2, e_3, e_4, the norm form is

$$N(x_1, x_2, x_3, x_4) = x_1^2 - \alpha x_2^2 - \beta x_3^2 + \alpha\beta x_4^2.$$

d) If $\dim C = 8$, there exist $\alpha, \beta, \gamma \in F^\times$ such that C is isomorphic to the octonion algebra $O(\alpha, \beta, \gamma) = \left(\frac{\alpha,\beta,\gamma}{F}\right)$. With respect to the standard octonion basis

[3]In particular, we assume an embedding $F \hookrightarrow 1F \subset C$.

$e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8$, *the norm form is*

$$N(x_1, \ldots, x_8) = x_1^2 - \alpha x_2^2 - \beta x_3^2 - \gamma x_4^2 + \alpha\beta x_5^2 + \alpha\gamma x_6^2 + \beta\gamma x_7^2 - \alpha\beta\gamma x_8^2.$$

Conversely, each of the algebras exhibited above is a composition algebra.

Note in particular that although a composition algebra is *a priori* allowed to be infinite-dimensional over F, it turns out that the only possible dimensions are 1, 2, 4 and 8.

2.2. **Composition Algebras are Quadratic and Alternative.**

Recall the process of linearizing a quadratic form to get a bilinear form. Namely, if $q : V \to F$ is a quadratic form (or, more generally, is quadratic in one of its arguments while the other arguments are held fixed), then the associated bilinear form is

$$\langle x, y \rangle = q(x + y) - q(x) - q(y).$$

At least that is our convention here. In the algebraic theory of quadratic forms (in characteristic not 2), it is customary to insert a factor of $\frac{1}{2}$ in the definition of the associated bilinear form. Thus, with our convention, we find $\langle x, x \rangle = 2q(x)$ (rather than the more familiar $\langle x, x \rangle = q(x)$). The advantages of this convention are first, that as we shall see at the end, it makes some sense even in characteristic 2, and in characteristic different from 2 leads to some simpler formulas, whereas with the other convention many of our formulas would have $\frac{1}{2}$'s in them. In particular we have the basic linearization identity $\forall x, y \in C$,

$$N(x + y) = N(x) + N(y) + \langle x, y \rangle.$$

A homomorphism of composition algebras $(C, N) \to (C', N')$ is an F-algebra homomorphism $\varphi : C \to C'$ which is also an isometric embedding with respect to the induced bilinear forms. In particular, a composition subalgebra (C', N') amounts to (i.e., is, up to isomorphism) an F-subalgebra of C that is nondegenerate with respect to N.

We define the **trace map** $T : C \to F$ by $T(x) = \langle x, 1 \rangle$.

We now deduce some identities valid in any composition algebra (C, N). Denoting the multiplicative identity of C by 1, we have that for all $x \in C$,

$$N(x) = N(1 \cdot x) = N(1)N(x).$$

Since N is nondegenerate, there exists $x \in X$ with $N(x) \neq 0$, whence

$$N(1) = 1$$

and the quadratic form N is **principal** (i.e., represents 1).

For all $x_1 x_2, y \in C$,

$$N(x_1 y + x_2 y) = N(x_1 y) + N(x_2 y) + \langle x_1 y, x_2 y \rangle = N(x_1)N(y) + N(x_2)N(y) + \langle x_1 y, x_2 y \rangle$$

and also

$$N(x_1 y + x_2 y) = N((x_1 + x_2)y) = N(x_1 + x_2)N(y) = (N(x_1) + N(x_2) + \langle x_1, x_2 \rangle)\, N(y).$$

Comparing these gives

$$\langle x_1 y, x_2 y \rangle = \langle x_1, x_2 \rangle N(y) \tag{9}$$

and similarly

(10) $$\langle xy_1, xy_2\rangle = N(x)\langle y_1, y_2\rangle.$$

Notice that equation (9) is quadratic in y. Its linearized form is

(11) $$\langle x_1y_1, x_2y_2\rangle + \langle x_1y_2, x_2y_1\rangle = \langle x_1, x_2\rangle\langle y_1, y_2\rangle.$$

Taking $x_1 = x$, $y_1 = y$, $x_2 = z$, $y_2 = 1$ in (11) gives

(12) $$\langle xy, z\rangle + \langle x, zy\rangle = \langle x, z\rangle\langle y, 1\rangle = T(y)\langle x, z\rangle.$$

Taking $x_1 = y_2 = x$, $x_2 = y$, $y_2 = 1$ in (11) gives

(13) $$\langle x, yx\rangle + \langle x^2, y\rangle = \langle x, y\rangle\langle 1, x\rangle = T(x)\langle x, y\rangle.$$

Taking $x_1 = x$, $y_1 = y$, $x_2 = y_2 = 1$ gives

(14) $$\langle xy, 1\rangle + \langle x, y\rangle = \langle x, 1\rangle\langle y, 1\rangle.$$

Theorem 2.2. *Let (C, N) be a composition algebra and $x \in C$. Then*

(15) $$x^2 - T(x)x + N(x)1 = 0.$$

Thus every element of C satisfies a quadratic equation over F.

Proof. Let $y \in C$ be arbitrary and form the inner product of LHS(15) with y:

$$\langle x^2, y\rangle - \langle x, 1\rangle\langle x, y\rangle + \langle 1, y\rangle N(x) = \langle x^2, y\rangle - \langle x, 1\rangle\langle x, y\rangle + \langle x, yx\rangle = 0.$$

Here the first equality is by (9) and the second is by (13). Since this holds for all $y \in C$ and the bilinear form is nondegenerate, this establishes (15). □

Remark: An algebra $A_{/F}$ in which each element satisfies a quadratic polynomial with F-coefficients is called a **quadratic algebra**. (Similarly, one can define cubic algebras and algebras of degree $d < \infty$).) Thus every composition algebra is a quadratic algebra.

Again (15) is quadratic in x and its linearized version is

(16) $$xy + yx - \langle x, 1\rangle y - \langle y, 1\rangle x + \langle x, y\rangle 1 = 0.$$

We define the **pure subspace** of C to be $1^\perp$. Note that N restricted to $F \cdot 1$ is just the quadratic form $x \mapsto x^2$, so certainly $F \cdot 1$ is a nondegenerate subspace. By [**?**, Prop. I.6], it follows that as a quadratic space we have $C = F \cdot 1 \oplus 1^\perp$ and further, by [**?**, Cor. I.8], the pure subspace $1^\perp$ is also nondegenerate. In this regard, (16) has the following pleasant consequence: for all $x, y \in 1^\perp$ with $\langle x, y\rangle = 0$, $xy = -yx$. That is, any two perpendicular elements in the pure subspace anticommute. The attentive reader should now be reminiscing about the basis elements e_2, e_3, e_4 in a quaternion algebra B! (More on this shortly.)

Corollary 2.3. *Let (C, N) be a composition algebra and $x \in C \setminus F \cdot 1$. If the subspace $C_x = F \cdot 1 \oplus F \cdot x$ is nondegenerate for N, then it is a composition subalgebra.*

Proof. From (15) it follows that $C_x \cong F[t]/(t^2 - \langle x, 1\rangle t + N(x))$ is a commutative, associative unital F-subalgebra of C. Therefore, if N restricted to C_x is nonsingular, C_x is a composition subalgebra of C. □

The following important corollary shows that our definition of a composition algebra as a pair is unnecessarily complicated:

Corollary 2.4. *Let C be a unital F-algebra, and let N, N' be two quadratic forms on C such that (C,N) and (C,N') are each composition algebras. Then $N = N'$.*

Proof. As we have seen, for any element x of the form $\alpha \cdot 1$, we must have $N(\alpha \cdot 1) = N'(\alpha \cdot 1) = \alpha^2$. Otherwise, the minimal polynomial of x over F has degree at least 2, and in view of (15) must be both $x^2 - \langle x, 1\rangle_N + N(x) \cdot 1$ and $x^2 - \langle x, 1\rangle_{N'} + N'(x) \cdot 1$, so $N(x) = N'(x)$. □

Corollary 2.5. *Let (C,N) and (C',N') be composition algebras, and let $\varphi : C \rightarrow C'$ be an isomorphism of F-algebras. Then φ is necessarily an isometry.*

Exercise 2.1. *Deduce Corollary 2.5 from Corollary 2.4.*

Because of Corollaries 2.4 and 2.5, it makes sense to speak of "the composition algebra C", as well as "the quadratic form N associated to the composition algebra C". For reasons which will become clear presently, we refer to N as the **norm form** of C.

Theorem 2.6. *Every composition algebra is an alternative algebra.*

Proof. Let (C,N) be a composition algebra. As special cases of the identity (11) we have that for all $x, y, z \in C$,

$$\langle xy, z\rangle + \langle y, xz\rangle = t(x)\langle y, z\rangle \tag{17}$$

and

$$\langle xy, z\rangle + \langle x, zy\rangle = T(y)\langle x, z\rangle. \tag{18}$$

It follows from (17) and (10) that for all $x, y, z \in C$,

$$\langle x(xy), z\rangle = T(x)\langle xy, z\rangle - \langle xy, xz\rangle = \langle (T(x)x - N(x)1)y, z\rangle = \langle x^2 y, z\rangle.$$

Since z is arbitary and the bilinear form is nondegenerate, this gives that for all $x, y \in C$, $x(xy) = (xx)y$, i.e., the left alternative identity (LA). Similarly, using (18) and (9) we deduce the right alternative identity. By Lemma 1.9, C is therefore alternative. □

Applying Theorem 2.6 to Example X.X, we immediately deduce a result that we have claimed before but did not wish to prove by direct computation.

Corollary 2.7. *An octonion algebra is alternative.*

2.3. **The involution.**

An **involution** on an F-algebra A is an F-linear map $\iota : A \rightarrow A$ such that:

(I1) for all $x, y \in A$, $\iota(xy) = \iota(y)\iota(x)$, and
(I2) for all $x \in A$, $\iota(\iota(x)) = x$.

Note that (I1) says precisely that $x \mapsto \iota(x)$ gives an isomorphism $A \stackrel{\sim}{\rightarrow} A^{\text{op}}$. It is common to use the bar notation to denote involutions, i.e., to write $\overline{x}$ for $\iota(x)$. We shall do so here.

I claim that any composition algebra C admits an involution, namely $x \mapsto \overline{x} =$

$\langle x,1\rangle 1 - x$. Note that if τ_1 is reflection through the orthogonal complement $1^\perp$ of the anisotropic vector 1 in the sense of quadratic form theory (c.f. [**?**, §I.8.2]), then

$$\overline{x} = -\tau_1(x). \tag{19}$$

Thus under the natural identification of the subalgebra $F \cdot 1$ of C with F, we have $T(x) = x + \iota(a)$.

Proposition 2.8. *Let x, y be elements of a composition algebra C with norm map N and associated bilinear form $\langle , \rangle$. Then:*
a) $\overline{x+y} = \overline{x} + \overline{y}$.
b) $x\overline{x} = \overline{x}x = N(x) \cdot 1$.
c) $\overline{\overline{x}} = x$.
d) $\overline{xy} = \overline{y}\,\overline{x}$.
e) $N(\overline{x}) = N(x)$.
f) $\langle \overline{x}, \overline{y}\rangle = \langle x, y\rangle$.

Proof. Part a) is immediate. Indeed the map $x \mapsto \overline{x}$ is visibly F-linear.
b) It is clear from the definition that x and $\overline{x}$ commute. Using (15), we compute $x\overline{x} = x(\langle x,1\rangle 1 - x) = -(x^2 - \langle x,1\rangle x)1 = N(x)1$.
c) We have $\overline{\overline{x}} = \overline{-\tau_1(x)} = -\overline{\tau_1(x)} = \tau_1(\tau_1(x)) = x$, since τ_1 is a reflection. (Or just compute directly.)
d) We compute

$$\overline{y}\,\overline{x} = (\langle x,1\rangle 1 - x)(\langle y,1\rangle 1 - y) = \langle x,1\rangle\langle y,1\rangle 1 - \langle x,1\rangle y - \langle y,1\rangle x + yx$$
$$= \langle x,1\rangle\langle y,1\rangle 1 - xy - \langle x,y\rangle 1 = \langle xy,1\rangle 1 - xy = \overline{xy}.$$

The third equality comes from (16) and the fourth equality from (14).
e) $N(\overline{x})1 = \overline{\overline{x}}\,\overline{x} = x\overline{x} = N(x)1$, so $N(\overline{x}) = N(x)$.
f) We have

$$\langle \overline{x}, \overline{y}\rangle = N(\overline{x} + \overline{y}) - N(\overline{x}) - N(\overline{y})$$
$$= N(\overline{x+y}) - N(\overline{x}) - N(\overline{y}) = N(x+y) - N(x) - N(y) = \langle x, y\rangle.$$

□

And now, more identities!

Lemma 2.9. *Let x, y, z be elements of a composition algebra C. Then:*

$$\langle xy, z\rangle = \langle y, \overline{x}z\rangle. \tag{20}$$

$$\langle xy, z\rangle = \langle x, z\overline{y}\rangle. \tag{21}$$

$$\langle xy, \overline{z}\rangle = \langle yz, \overline{x}\rangle. \tag{22}$$

$$x(\overline{x}y) = N(x)y. \tag{23}$$

$$(x\overline{y})y = N(y)x. \tag{24}$$

$$x(\overline{y}z) + y(\overline{x}z) = \langle x, y\rangle z. \tag{25}$$

$$(x\overline{y})z + (x\overline{z})y = \langle y, z\rangle x. \tag{26}$$

Proof. We have

$$\langle y, \overline{x}z\rangle = \langle y, (\langle x, 1\rangle 1 - x)z\rangle = \langle x, 1\rangle\langle y, z\rangle - \langle y, xz\rangle.$$

Using 11, the above expression is equal to

$$\langle xy, z\rangle + \langle xz, y\rangle - \langle y, xz\rangle = \langle xy, z\rangle,$$

establishing (20). Now applying (20) twice, we get

$$\langle xy, z\rangle = \langle y, \overline{x}z\rangle = \langle \overline{y}, \overline{z}x\rangle = \langle \overline{z}x, \overline{y}\rangle = \langle x, z\overline{y},$$

establishing (21). Similarly, using (20) we get

$$\langle xy, \overline{z}\rangle = \langle \overline{yx}, z\rangle = \langle \overline{x}, yz\rangle = \langle yz, \overline{x}\rangle,$$

establishing (22).
Next, take the inner product of $x(\overline{x}y)$ with any $z \in C$ and apply (20) followed by (10) to get

$$\langle x(\overline{x}y), z\rangle = \langle \overline{x}y, \overline{x}z\rangle = N(x)\langle y, z\rangle = \langle N(x)y, z\rangle.$$

Since the bilinear form is nondegenerate, (23) follows. Applying the involution to (23) yields (24). Finally, the identities (25) and (26) are the linearizations of (23) and (24) respectively. □

Proposition 2.10. *Let C be a composition algebra and $x \in C$. Then x has a multiplicative inverse if and only if $N(x) \neq 0$, and then $x^{-1} = N(x)^{-1}\overline{x}$.*

Proof. Suppose x has a multiplicative inverse, i.e., there exists $y \in C$ such that $xy = yx = 1$. Then $1 = N(1) = N(xy) = N(x)N(y)$, so $N(x) \neq 0$. Conversely, if $N(x) \neq 0$, then – since $N(x)$, x and $\overline{x}$ all lie in the commutative, assocative subalgebra C_x, we may unambiguously multiply the identities $x\overline{x} = \overline{x}x = N(x)$ by $N(x)^{-1}$ to see that $x(N(x)^{-1}\overline{x}) = (N(x)^{-1}\overline{x})x = 1$. □

Exercise 2.2. *Use Theorem 2.6, Theorem 1.13 and the multiplicativity of the quaternion norm to give a less computational proof of the associativity of quaternion algebras.*

Corollary 2.11. *For any $\alpha_1, \alpha_2, \alpha_3 \in F^\times$, the octonion algebra $\left(\frac{\alpha_1, \alpha_2, \alpha_3}{F}\right)$ is alternative.*

Proof. Indeed in §1 we showed that an octonion algebra is a composition algebra by writing down an explicit norm form ("generalized eight squares identity"). □

2.4. **The Internal Cayley-Dickson-Albert Process.**

Let C be a composition algebra, and let $D \subset C$ be a finite-dimensional proper composition subalgebra. Then $C = D \oplus D^\perp$ and $D^\perp$ is also nondegnerate. Since C is proper, $D^\perp \neq \{0\}$ and thus we may choose an anisotropic vector $i \in D^\perp$, i.e., $\alpha = N(i) \neq 0$. Since D contains $1 \cdot F$, $D^\perp \subset 1^\perp$, and thus $\overline{i} = -i$.

To D and the anisotropic vector i in $D^\perp$ we associate the nondegenerate subspace

$$D_1 = D + Di.$$

Let $y, z \in D$. Then

$$\langle z, yi\rangle = \langle \overline{z}, \overline{i}\overline{y}\rangle = -\langle \overline{z}, i\overline{y}\rangle = -\langle \overline{z}y, i\rangle = 0,$$

since $\overline{z}y \in D$. This shows

$$Di \subset D^{\perp}. \tag{27}$$

In particular $i = 1i \in D^{\perp} \subset 1^{\perp}$, so $\overline{i} = -i$.

Also, since $D \subset i^{\perp}$, for all $y \in D$ we have

$$yi = -\overline{yi} + \langle y, i \rangle 1 = -\overline{i}\overline{y} = i\overline{y}. \tag{28}$$

Since D is nondegenerate, $Di \cap D = 0$ and thus $D_1 = D \oplus Di$ (*direct* sum).

Theorem 2.12. *(Internal Cayley-Dickson-Albert Process) Let $D \subset C$ be a proper, finite dimensional nondegenerate subalgebra and let $i \in D^{\perp}$ be such that $\alpha = -N(i) \neq 0$. Then $D_1 = D \oplus Di$ is a nondegenerate subalgebra of C with* $\dim D_1 = 2 \dim D$. *Moreover, for all $x, y, u, v \in D$,*

$$(x + yi)(u + vi) = (xu + \alpha\overline{v}y) + (vx + y\overline{u})i, \tag{29}$$

$$N(x + yi) = N(x) - \alpha N(y), \tag{30}$$

$$\overline{x + yi} = \overline{x} - yi. \tag{31}$$

Proof.
Step 0: We know that D_1 is an F-subspace of C. Since $N(i) \neq 0$, $i \in C^{\times}$ and thus the linear endomorphism $R_i : C \to C$, $x \mapsto xi$ is an isomorphism. So $\dim D_1 = \dim D + \dim Di = 2 \dim D$.
Step 1: We prove (29). For this it is enough to derive the following three special cases: for all $x, y, u, v \in D$, we have

$$x(vi) = (vx)i, \tag{32}$$

$$(yi)u = (y\overline{u})i, \tag{33}$$

$$(yi)(vi) = -\alpha\overline{v}y. \tag{34}$$

To establish (32), we form the inner product with $z \in C$ and recall that since $vi \in 1^{\perp}$, $\overline{vi} = -vi$:

$$\langle x(vi), z \rangle = \langle vi, \overline{x}z \rangle = -\langle vi, \overline{z}x \rangle.$$

Applying (11) and using $\langle i, x \rangle = 0$, the above expression is equal to

$$\langle vx, \overline{z}i \rangle = -\langle vx, xi \rangle + \langle z, 1 \rangle \langle vx, a \rangle = -\langle vx, zi \rangle$$
$$= \langle vx, z\overline{i} \rangle = \langle (vx)i, z \rangle,$$

where in the last equality we have used (21). This establishes (32). Similarly, for any $z \in C$,

$$\langle (yi)u, z \rangle = \langle yi, z\overline{u} \rangle = -\langle y\overline{u}, zi \rangle = \langle y\overline{u}, z\overline{i} \rangle = \langle (y\overline{u})i, z \rangle.$$

Finally, observe that for $y \in D$,

$$yi = -\overline{i}\overline{y} + \langle yi, 1 \rangle = i\overline{y}.$$

Thus, applying the Moufang identity (4),

$$(yi)(vi) = (i\overline{y})(vi) = i((\overline{y}v)i) = i(i(\overline{v}y)) = -\alpha\overline{v}y.$$

Step 2: From (29) it follows that D_1 is an F-subalgebra.
Step 3: As we saw just above, for all $x, y \in D$, $\langle x, yi \rangle = 0$, and thus

$$N(x + yi) = N(x) + N(y)N(i) = N(x) - \alpha N(y),$$

verifying (30). Thus the norm form on D_1 is the orthogonal direct sum of the norm form on D with a nonzero scalar multiple of the norm form on D. (Or better yet, N on D_1 is the tensor product of N on D with $\langle 1, -\alpha\rangle$!) Thus it is visibly nondegenerate on D_1.
Step 4: We have $\overline{x+yi} = \overline{x} + \overline{i}\overline{y} = \overline{x} - i\overline{y} = \overline{x} - yi$, proving (31). □

2.5. **Proof of Hurwitz's Theorem.**

Let C be any finite-dimensional composition algebra over F. Let $C_0 = F \cdot 1$. If $C_0 \subsetneq C$, choose $i_1 \in C_0^\perp$ with $N(i_1) = -\alpha_1 \neq 0$. Then

$$C_1 = C(\alpha_1) = C_0 \oplus C_0 i_1$$

is a two-dimensional composition subalgebra of C. If it is proper, choose $i_2 \in C_1^\perp$ with $N(i_2) = -\alpha_2 \neq 0$, so

$$C_2 = C(\alpha_1, \alpha_2) = C_1 \oplus C_1 i_2$$

is a 4-dimensional composition subalgebra of C. If C_2 is proper, then choose $i_3 \in C_3^\perp$ with $N(i_3) = -\alpha_3 \neq 0$, so

$$C_3 = C(\alpha_1, \alpha_2, \alpha_3) = C_2 \oplus C_2 i_3$$

is an 8-dimensional composition subalgebra of C. And then, *a priori* this construction can be continued: if $\dim C$ is infinite, it can be continued indefinitely. If $\dim C$ is finite, then this shows that it must be of the form 2^d and then we get a sequence of subalgebras $C_1, \ldots, C_d$ with $\dim C_k = 2^k$ for all k.

Theorem 2.13. *With notation as above:*
a) The algebra $C(\alpha_1)$ is isomorphic to the binion algebra $\left(\frac{\alpha}{F}\right)$.
b) The algebra $C(\alpha_1, \alpha_2)$ is isomorphic to the quaternion algebra $\left(\frac{\alpha,\beta}{F}\right)$.
c) The algebra $C(\alpha_1, \alpha_2, \alpha_3)$ is isomorphic to the octonion algebra $\left(\frac{\alpha,\beta,\gamma}{F}\right)$.

Proof. By choosing natural F-bases on both sides, one simply checks that the multiplication laws agree. We leave the details to the reader as a good exercise. □

We have now verified Theorem 2.1 for composition algebras of dimension $1, 2, 4, 8$. It remains to be shown that these are the only possible dimensions of composition algebras (recall that this includes ruling out the possibility of an infinite-dimensional algebra). The internal Cayley-Dickson process shows that any composition algebra C with $\dim C > 8$ must have an octonion subalgebra, and so what remains is to show that if $O \subset C$ is an octonion subalgebra of a composition algebra than we must have $O = C$. This is accomplished in the following result.

Proposition 2.14. *Let D be a composition subalgebra of a composition algebra C. If $D \subsetneq C$, then D is associative.*

Proof. The key idea is that if D is proper, we can choose an anisotropic $i \in D^\perp$ and form $D_1 = D \oplus Di$, which is itself a composition subalgebra of C, with norm given as in Theorem 2.12 above. Thus, for any $x, y, u, v \in D$, we have

$$N((x+yi)(u+vi)) = N(x+yi)N(u+vi).$$

Expanding this and simplifying leads to

$$\langle xu, \overline{v}y\rangle = \langle vx, y\overline{u}\rangle,$$

hence

$$\langle (xu)\overline{y}, \overline{v}\rangle = \langle xu, \overline{v}y\rangle = \langle vx, y\overline{u}\rangle = \langle v, (y\overline{u})\overline{x}\rangle = \langle x(u\overline{y}), \overline{v}\rangle.$$

Thus by nondegeneracy of the norm form, we have $(xu)\overline{y} = x(u\overline{y})$, i.e., the multiplication in D is associative. □

This completes the proof of Theorem 2.1. In summary, the argument was this: inside any composition algebra we can repeatedly apply the Cayley-Dickson process, starting from $C_0 = F$, to get a sequence of composition subalgebras $C_0, \ldots, C_d$. However, each time we apply the process, we lose some of the nice properties of the algebra studied in §1. If we can apply the process three times, then we lose associativity and then Proposition 2.14 shows the process must terminate.

2.6. **More on the norm form of a composition algebra.**

Recall that we originally introduced a composition algebra as a pair (C, N), where C is a unital F-algebra and $N : C \to F$ is a nondegenerate quadratic form which is multiplicative with respect to C. Later we showed that in fact a given algebra C is a composition algebra with respect to at most one quadratic form, allowing us to speak of the "norm form" associated to "the composition algebra C".

In this section we establish the converse result: a composition algebra is determined up to isomorphism by the isometry class of its norm form N.

Theorem 2.15. *Let C, C' be composition algebras over F, with norm forms N, N'. If $N \cong N'$, then $O \cong O'$.*

Proof. Let t be an isometry of quadratic spaces $(C, N) \to (C', N')$: that is, for all $x \in C$, $N'(t(x)) = N(x)$. In particular $N'(t(1)) = 1$. In particular the element $t(1)$ of C' is invertible; let $t(1)^{-1}$ denote its left inverse. If we then define a new map $T : C \to C'$ by $T(x) := t(1)^{-1}t(x)$, then

$$N'(T(x)) = N'(t(1)^{-1}t(x)) = N(t(1)^{-1})N'(t(x)) = N(t(1))^{-1}N(x) = N(x),$$

so that T is again an isometry and $T(1) = 1$. Having established this we may as well just assume that $t(1) = 1$.
The case in which $\dim C = 1$ – i.e., $C = F$ – is trivial, and will be excluded. Otherwise, we know that $\dim C = 2^i$ for $i = 1, 2, 3$ and C is accordingly, a binion, quaternion or octonion algebra. Depending upon i, we run through the first i steps of the following argument.
Step 1: Choose $i \in 1^{\perp}$ with $N(i) \neq 0$, and put $i' = t(i)$. Thus $N'(i) = N(i)$ and $\langle i', 1\rangle = 0$. The two-dimensional composition subalgebras $K = F1 \oplus Fi$ and $K' = F1 \oplus Fi'$ are thus isomorphic: indeed, $\alpha_1 \cdot 1 + \alpha_2 i \mapsto \alpha_1 1 + \alpha_2 i'$ is an isomorphism. At this stage this assertion is probably obvious, but for analogous use let us mention that it is a consequence of the Cayley-Dickson-Albert process.
Step 2: Choose $j \in K^{\perp}$ with $N(j) \neq 0$ and put $j' = t(j)$. Extend φ to $K1 \oplus Kj$ by $\varphi(x + yj) = \varphi(x) + \varphi(y)j'$ for $x, y \in K$. Again, using the Cayley-Dickson-Albert process and the observation that $\varphi(\overline{x}) = \overline{\varphi(x)}$, we see that φ gives an isomorphism of quaternion algebras $B = K1 \oplus Kj \to B' = K \oplus Kj'$.
Step 3: Choose $k \in B^{\perp}$ with $N(k) \neq 0$ and put $k' = t(k)$. Extend φ to $B1 \oplus Bk$ by $\varphi(x + yk) = \varphi(x) + \varphi(y)k'$. This gives an isomorphism $C \to C'$. □

Thus the problem of classifying the composition algebras over F is reduced to that of classifying norm forms. From the perspective of quadratic form theory this problem has an immediately satisfactory answer: the norm form of a composition algebra is precisely a (0-fold, a trivial case, or) 1-fold, 2-fold or 3-fold Pfister form. More precisely: for a binion algebra

$$K = \left(\frac{\alpha}{F}\right),$$

the norm form is

$$\langle\langle \alpha \rangle\rangle := \langle 1, -\alpha \rangle.$$

For a quaternion algebra

$$B = \left(\frac{\alpha, \beta}{F}\right),$$

the norm form is

$$\langle\langle \alpha, \beta \rangle\rangle := \langle 1, -\alpha \rangle \otimes \langle 1, -\beta \rangle = \langle 1, -\alpha, -\beta, \alpha\beta \rangle.$$

For an octonion algebra

$$O = \left(\frac{\alpha, \beta, \gamma}{F}\right),$$

the norm form is

$$\begin{aligned} \langle\langle \alpha, \beta, \gamma \rangle\rangle &:= \langle 1, -\alpha \rangle \otimes \langle 1, -\beta \rangle \otimes \langle 1, -\gamma \rangle \\ &= \langle 1, -\alpha, -\beta, -\gamma, \alpha\beta, \alpha\gamma, \beta\gamma, -\alpha\beta\gamma \rangle. \end{aligned}$$

2.7. **Split Composition Algebras.**

Proposition 2.16. *For a composition algebra (C, N), the following are equivalent:*
(i) C is a division algebra (i.e., every nonzero element has both a left and a right inverse).
(ii) N is anisotropic: for all $x \in C^\bullet$, $N(x) \neq 0$.

Proof. (i) $\implies$ (ii): Suppose C is a division algebra and let $x \in C^\bullet$. Then there exists $y \in C$ such that $yx = 1$. Taking norms gives $N(y)N(x) = 1$, so $N(x) \neq 0$.
(ii) $\implies$ (i): This follows immediately from the identity $\overline{x}x = x\overline{x} = N(x) \cdot 1$. □

A composition algebra is **split** if it is not a division algebra.

Corollary 2.17. *a) The binion algebra $\left(\frac{1}{F}\right) \cong F \oplus F$ is split.*
b) The quaternion algebra $\left(\frac{1,1}{F}\right) \cong M_2(F)$ is split.
c) The octonion algebra $\left(\frac{1,1,1}{F}\right)$ is split.

Exercise 2.3. *Prove Corollary 2.17.*

Theorem 2.18. *For any field F and any $1 \leq i \leq 3$, there is up to isomorphism a unique split composition algebra $C_{/F}$ of dimension 2^i.*

One natural proof of Theorem 2.18 uses the basic theory of Pfister forms. Namely, a Pfister form is isotropic iff it is hyperbolic. In particular, there is up to isometry exactly one isotropic Pfister form of any given dimension 2^i. Applying Proposition 2.16 and Theorem 2.15 we conclude that there is up to isomorphism a unique split composition algebra of dimension 2^i, given by the i-fold tensor product of the hyperbolic plane $\langle\langle -1 \rangle\rangle = \langle 1, -1 \rangle$.

However, it is also of interest to give a more self-contained proof of Theorem 2.18, which we do now.

Proof. Since the norm form $N \cong x_1^2 + N^0(x_2, \ldots, x_n)$ is isotropic, there exists $i \in 1^\perp$ such that $N(i) = -1$. Indeed choose $x \in C^\bullet$ with $N(x) = 0$. If $x \in 1^\perp$, then pick $i' \in 1^\perp$ with $\langle i', x\rangle = 1$, and put $i := i' - (1 + N(i')x$. If $x \notin 1^\perp$, write $x = \alpha 1 + y$ with $\alpha \in F^\bullet$ and $y \in 1^\perp$. Since $0 = N(x) = \alpha^2 + N(y)$, $N(y) = -\alpha^2$, so put $a = \alpha^{-1} y$. (Or, using a little bit of quadratic form theory: $N(x) \cong x_1^2 + a_2 x_2^2 + \ldots + a_n x_n^2 = 0$. Let $x \in C^\bullet$ be an iostropic vector. If $x_1 \neq 0$, then $i = (0, \frac{x_2}{x_1}, \ldots, \frac{x_n}{x_1})$ lies in $1^\perp$ and has $N(i) = -1$. If $x_1 = 0$, then the form $N^0(x_2, \ldots, x_n) = a_2 x_2^2 + \ldots + a_n x_n^2$ is isotropic and thus universal.) Thus $K = F1 \oplus Fi$ is a composition subalgebra. Moreover it is isotropic: $N(1 + i) = 0$. If C itself is a binion algebra, we are done. Otherwise we may find $j \in K^\perp$ with $N(j) = \beta \neq 0$ and the Cayley-Dickson-Albert doubling process shows that the quadratic form N on $B = K \oplus Kj$ is $\langle 1, -\beta\rangle \otimes N|_K \cong N_K \oplus (-\beta N_K)$. Since $N_K \cong \mathbb{H}$ (the hyperbolic plane), so is $-\beta N_K$, and thus $N|_B$ is a direct sum of two hyperbolic planes. If $C = B$, we're done; otherwise, applying the doubling process again shows that N is the direct sum of three hyperbolic planes. □

It follows from Theorem 2.18 and Corollary 2.17 that up to isomorphism the unique split binion algebra over F is $F \otimes F$ and the unique split quaternion algebra over F is $M_2(F)$. These are rather elementary and familiar mathematical objects. On the other hand, let $\mathbb{O}$ denote the unique (up to isomorphism) split octonion algebra over F. This is a much more interesting mathematical object. For instance, consider its automorphism group as a unital F-algebra. For any finite dimensional unital F-algebra A, $\mathrm{Aut}(A)$ naturally embeds into $\mathrm{GL}_F(A)$. If $e_1 = 1, e_2, \ldots, e_n$ is an F-basis of A, then a matrix $\Phi \in \mathrm{GL}_F(A)$ gives rise to an F-algebra automorphism of A iff for all $1 \leq i, j \leq n$, $\Phi(e_i e_j) = (\Phi e_i)(\Phi e_j)$. It follows that the subgroup $\mathrm{Aut}(A)$ of $\mathrm{GL}_F(A)$ is cut out by polynomial equations, i.e., is a linear algebraic group.

Theorem 2.19. *Let $\mathbb{O}$ be the split octonion algebra over the field F. Then $\mathrm{Aut}(\mathbb{O})$ is the split form of the exceptional simple algebraic group G_2.*

The proof of this result is (well) beyond the scope of these notes. See for instance [SV00, Ch. 2].

Corollary 2.20. *The isomorphism classes of octonion algebras over a field F are parameterized by the Galois cohomology set $H^1(F, G_2)$.*

This has many important consequences. For instance, if F is any field with u-invariant less than 8 – e.g. a finite field, a p-adic field, a Laurent series field over a finite field, a global field with no real places – then every G_2-torsor is trivial.

Exercise 2.4. *Let F be a global field with exactly a real places. Show that there are exactly 2^a isomorphism classes of G_2-torsors over F. (Suggestion: use the Hasse Principle to count the number of isomorphism classes of 3-fold Pfister forms.)*

References

[Al42] A.A. Albert, *Quadratic forms permitting composition.* Ann. of Math. (2) 43 (1942), 161-177.

[Sch54] R.D. Schafer, *On the algebras formed by the Cayley-Dickson process.* Amer. J. Math. 76 (1954), 435-446.

[Sch66] R.D. Schafer, *An introduction to nonassociative algebras.* Pure and Applied Mathematics, Vol. 22 Academic Press, New York-London 1966.

[SV00] T.A. Springer and F.D. Veldkamp, *Octonions, Jordan algebras and exceptional groups.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000.