V.B. Finite-dimensional division algebras

What about a vector space where you can multiply and divide vectors?

V.B.1. Definition. A division algebra over a field $\mathbb{F}$ is an $\mathbb{F}$-algebra $A$ whose underlying ring is a division ring.

This rules out most of the examples in V.A.4; for example, products like $\mathbb{F} \times \mathbb{F}$ contain zero-divisors, as do matrix algebras.

V.B.2. Examples. (i) Field extensions are division algebras: e.g., $\mathbb{C}$ is an $\mathbb{R}$-division algebra; and $\mathbb{Q}[\zeta]$ is a $\mathbb{Q}$-division algebra.
(ii) Quaternion algebras give some non-commutative examples: $\mathbb{H}$ (Hamilton’s quaternions) is an $\mathbb{R}$-division algebra; while the non-split (i.e., division ring) cases in HW 6 #6 give $\mathbb{Q}$-division algebras.

We are particularly interested in division algebras which are finite-dimensional (as $\mathbb{F}$-vector spaces). While number fields (viewed as field extensions) easily yield an endless list of such examples over $\mathbb{Q}$, you may find it difficult to recall seeing any finite-dimensional field extensions of $\mathbb{C}$. That is because they don’t exist!

V.B.3. Definition. (i) An algebraic field extension\footnote{Warning: these need not be finite-dimensional (though they certainly are if they are finitely generated).} of $\mathbb{F}$ is one whose every element is algebraic (cf. III.G.6(ii)) over $\mathbb{F}$.
(ii) Call a field $\mathbb{F}$ algebraically closed if it has no algebraic field extensions (other than itself).

V.B.4. Example. The Fundamental Theorem of Algebra states that every polynomial over $\mathbb{C}$ has a root (hence all roots) in $\mathbb{C}$. (This theorem is proved in complex analysis.) Since any element $\alpha$ of a field extension which is algebraic over $\mathbb{C}$ satisfies a polynomial equation $P(\alpha) = 0$, $\alpha$ actually belongs to $\mathbb{C}$. So $\mathbb{C}$ is algebraically closed.

Clearly division algebras are the simplest kind of $\mathbb{F}$-algebra after field extensions; so we shall do a rough classification for $\mathbb{F} = \mathbb{R}, \mathbb{C}$, and finite fields. To begin with, we finish off $\mathbb{C}$ with the
V.B.5. **Theorem.** Let $\mathbb{F}$ be an algebraically closed field, and $A$ a finite-dimensional division algebra over $\mathbb{F}$. Then $A = \mathbb{F}$.

**Proof.** Let $a \in A$, and consider the ring homomorphism

$$\text{ev}_a : \mathbb{F}[\lambda] \rightarrow \mathbb{F}[a] \subset A,$$

$$f(\lambda) \mapsto f(a).$$

This cannot be injective, since $A$ (hence $\mathbb{F}[a]$) is finite-dimensional and $\mathbb{F}[\lambda]$ is not. So we have $\mathbb{F}[a] \cong \mathbb{F}[\lambda]/(m_a)$, where $m_a$ is the minimal polynomial of $a$ over $\mathbb{F}$. Were this reducible, $\mathbb{F}[a]$ wouldn’t be a domain, which is impossible since $A$ is a division algebra.

Hence $m_a$ is irreducible, and $\mathbb{F}[a]$ is a field, all of whose elements are algebraic over $\mathbb{F}$ (cf. III.G.8). Since $\mathbb{F}$ is algebraically closed, $\mathbb{F}[a] = \mathbb{F}$. So, in particular, $a \in \mathbb{F}$; and since $a \in A$ was arbitrary, $A = \mathbb{F}$. \[\square\]

Given $p(\lambda) \in \mathbb{R}[\lambda]$ monic, we have

$$p(\lambda) = \prod_{j=1}^{n}(\lambda - a_j) = \prod_{j=1}^{n}(\lambda - \bar{\alpha}_j)$$

in $\mathbb{C}[\lambda]$, by the Fundamental Theorem of Algebra. We can rewrite this as

$$p(\lambda) = \prod_{i=1}^{n}(\lambda - a_i) \times \prod_{k=1}^{g}(\lambda - \beta_k)(\lambda - \bar{\beta}_k)$$

$$= \prod_{i=1}^{n}(\lambda - a_i) \times \prod_{k=1}^{g}(\lambda^2 - 2\Re(\beta_k) + |\beta_k|^2),$$

with $a_i \in \mathbb{R}$ and $\beta_k \notin \mathbb{R}$. Hence no polynomial of degree $> 2$ is irreducible in $\mathbb{R}[\lambda]$.

Let $A$ be a finite-dimensional division algebra over $\mathbb{R}$. Given $\alpha \in A \setminus \mathbb{R}$, we consider as usual

$$\text{ev}_\alpha : \mathbb{R}[\lambda] \rightarrow \mathbb{R}[\alpha] \subset A,$$

which as above has a nontrivial kernel $K$ since $\dim_{\mathbb{R}}(A) < \infty$. Since $\mathbb{R}[\lambda]$ is a PID, $K = (m_\alpha)$ with $m_\alpha$ irreducible (also as above); and as $\alpha \notin \mathbb{R}$, $\deg(m_\alpha) > 1$. So $\deg(m_\alpha) = 2$, and $m_\alpha(\lambda) = \lambda^2 - 2a\lambda + b$.

with $a^2 < b$. We may thus write $\alpha = \beta + a$, where $\beta \in A \setminus \mathbb{R}$ and $\beta^2 = a^2 - b < 0$.
Now consider the subset
\[ A' := \{ \alpha \in A \mid \alpha^2 \in \mathbb{R}_{\leq 0} \} \subset (A \setminus \mathbb{R}) \cup \{ 0 \}. \]
From the last paragraph it is clear that if \( A \setminus \mathbb{R} \neq \emptyset \), then \( A' \neq \{ 0 \} \)
(and the converse is obvious).

**V.B.6. Lemma.** \( A' \) is an \( \mathbb{R} \)-subspace of \( A \).

**Proof.** Given \( r \in \mathbb{R}, \alpha \in A' \), we have \((ar)^2 = \alpha^2 r^2 \leq 0 \implies ar \in A'\). So \( A' \) is closed under multiplication and we only need to check sums of elements. So let \( u, v \in A' \setminus \{ 0 \} \) be linearly independent over \( \mathbb{R} \) in \( A \). (If they are dependent, \( u + v \) is a multiple of \( u \) and we are done.) By assumption, we have \( u^2, v^2 \in \mathbb{R}_{<0} \).

Suppose first that \( u = av + b \), with \( a, b \in \mathbb{R} \). Then in
\[ u^2 = (av + b)^2 = a^2 v^2 + 2abv + b^2, \]
the RHS terms are real except for \( 2abv \), which forces \( ab = 0 \). But we can’t have \( a = 0 \), for then \( u = b \in \mathbb{R} \); and if \( b = 0 \), then \( u = av \) contradicts the independence.

So \( u \) is not of the form \( av + b \), which means that \( u, v \), and \( 1 \) are independent over \( \mathbb{R} \). Hence \( u + v, u - v \in A \setminus \mathbb{R} \); and so as above (for \( \alpha \), they satisfy irreducible quadratic equations
\[ 0 = (u + v)^2 - p(u + v) - q \quad \text{and} \quad 0 = (u - v)^2 - r(u - v) - s. \]
Writing \( c = u^2, d = v^2 \), these become
\[ 0 = c + d + (uv + vu) - p(u + v) - q \]
and \[ 0 = c + d - (uv + vu) - r(u - v) - s, \]
and adding gives
\[ 0 = (p + r)u + (p - r)v + (q + s - 2c - 2d)1. \]
By independence of \( \{ u, v, 1 \} \) it now follows that \( p = r = 0 \). So for the original equations to have been irreducible, we must have \( q, s < 0 \); in particular, \( (u + v)^2 = q \in \mathbb{R}_{<0} \). Hence \( u + v \in A' \) as desired. \( \square \)
For \( u \in A' \), set
\[ Q(u) := -u^2 \in \mathbb{R}. \]

V.B.7. LEMMA. \( Q \) is a positive-definite quadratic form on \( A' \).

**Proof.** Since \( A \) is a domain, \( Q(u) = 0 \iff u = 0 \). Moreover, for \( a \in \mathbb{R}, Q(au) = a^2Q(u) \), so \( Q \) is quadratic. Finally, \( Q(u) \geq 0 \) for all \( u \in A' \) (by definition of \( A' \)). \( \square \)

Write \( B(u, v) := Q(u + v) - Q(u) - Q(v) = -(uv + vu) \) for the associated positive-definite symmetric bilinear form. Now suppose \( A' \neq \{0\} \), i.e. \( A \supset \mathbb{R} \), and pick \( i \in A' \) such that \( Q(i) = 1 \); we can do this by rescaling any element in \( A' \setminus \{0\} \) by a real number. Then \( i^2 = -1 \), and we fix the copy of \( \mathbb{C} = \mathbb{R} + i\mathbb{R} = \mathbb{R}[i] \subset A \).

Next, suppose that \( A \supset \mathbb{C} \); then \( A' \supset i\mathbb{R} \), and we pick \( j \in A' \setminus i\mathbb{R} \) and take \( j := j - iB(i,j) \). This gives \( B(j, i) = B(j, i) - B(i, j)B(i, i) = 0 \), and rescaling \( j \) gives \( j \) with \( j^2 = -1 \) and \( j \perp i \) (i.e. \( 0 = B(i, j) = ij + ji \)). Setting \( k = ij \), we compute
\[ \begin{aligned}
    k^2 &= ijjj = -iijj = \frac{1}{(-1)(-1)} = -1 \\
    ik &= i^2j = -j = jii = -iji = -ki \\
    jk &= \cdots = -kj
\end{aligned} \]

\[ \implies \begin{cases} 
    k \in A' , \; k \perp i,j \\
    1,i,j,k \text{ R-linearly independent} \\
    \mathbb{R} + i\mathbb{R} + j\mathbb{R} + k\mathbb{R} = \mathbb{H} \subset A.
\end{cases} \]

Finally, suppose \( A \supset \mathbb{H} \). Then there exists \( \ell \in A' \) with \( Q(\ell) = 1 \) and \( \ell \perp i,j,k \). As above, this gives \( \ell i = -i\ell, \ell j = -j\ell, \) and \( \ell k = -k\ell \); substituting \( k = ij \) in the last of these gives
\[ -(ij)\ell = \ell(ij) = (\ell i)j = -(i\ell)j = -i(\ell j) = i(j\ell) = (ij)\ell, \]
a contradiction. This proves the famous

V.B.8. THEOREM (Frobenius, 1877). Let \( A \) be a finite-dimensional division algebra over \( \mathbb{R} \). Then \( A = \mathbb{R}, \mathbb{C}, \) or \( \mathbb{H} \).
V.B.9. Remark. If one allows $A$ to be nonassociative, then there is one more (8-dimensional) option, Cayley’s octonions $O = H \times H$ with the multiplication law

$$(q,r) \cdot (s,t) = (qs - r^*t, q^*t + rs)$$

where “$*$” denotes “quaternionic conjugation” ($i \mapsto -i$, $j \mapsto -j$, $k \mapsto -k$). More or less, this mimics the way you get $H$ from $C \times C$ and $C$ from $R \times R$. The octonions play a starring role in the explicit construction of the exceptional Lie groups $G_2, F_4, E_6, E_7, E_8$ in Cartan’s classification of simple Lie groups over $C$.

V.B.10. Remark. There are lots of non-isomorphic 4-dimensional “quaternion algebras” over $Q$, and there are lots of algebraic field extensions. But one might have held out hope that, say, there is an upper bound on the dimension of non-commutative $Q$-division algebras. Alas, this is not the case: for instance, if $\gamma$ is an even integer not divisible by 8, the $Q$-algebra generated by $x, y$ subject to the relations

$$x^3 + x^2 - 2x - 1 = 0, \ xy = y(x^2 - 2), \ y^3 = \gamma$$

is a division algebra of dimension 9. A classification of such examples was carried out by Dickson.

Finally, we consider the case of a division algebra $A$ over a finite field $F$ (i.e. $|F| < \infty$), with $n := \dim_F A < \infty$. Clearly $|A| = |F|^n$, and so (forgetting the $F$-action) $A$ is a finite division ring. Conversely, if $A$ a finite division ring, then $C(A)$ is a finite field and $A$ is an algebra over it (cf. V.A.3), necessarily finite-dimensional.

V.B.11. Theorem (Wedderburn, 1905). Any finite division ring is commutative, hence a field.

V.B.12. Remark. The theorem means that algebraic field extensions furnish the only examples of finite-dimensional $F$-division algebras when $|F| < \infty$. 
Proof of V.B.11. Set \( F = C(A), q = |F|, n = \dim_F A \). We need to show that \( n = 1 \), since this is equivalent to \( A = F \).

Applying the class equation to the group \( A^* = A \setminus \{0\} \) gives

\[ |A^*| = \sum_i |\text{ccl}(x_i)| = \sum_i [A^* : \text{stab}(x_i)] \]

where \( x_i \) is a set of representatives for the conjugacy classes in \( A^* \). In particular, there are \( q - 1 \) one-element conjugacy classes, given by the elements \( x_1, \ldots, x_{q-1} \) of \( F^* \); each has stabilizer equal to all of \( A^* \). Each \( x_i \in A^* \setminus F^* \), on the other hand, is stabilized by the nonzero elements of a proper subring \( A_i \subset A \) containing \( F \). (Why?) These \( A_i \) are \( F \)-algebras, and so \( |A_i| = q^{m_i} \) with \( 1 \leq m_i < n \), and \( |\text{stab}(x_i)| = q^{m_i} - 1 \). Thus (V.B.13) becomes

\[ q^n - 1 = |A| - 1 = |A^*| = (q - 1) + \sum_{i \geq q} q^{m_i} - 1. \]

Now regard, for each \( i \), \( A \) as a module over \( A_i \). Clearly, it is free (\( A \) has no zero-divisors), of some finite rank \( d_i \). Moreover, \( A_i \) is a \( m_i \)-dimensional vector space over \( F \). So as \( F \)-vector spaces,

\[ F^n = A = A_i \oplus \cdots \oplus A_i = F_{m_i} \oplus \cdots \oplus F_{m_i} \]

\( \implies n = m_i d_i \implies m_i \mid n \ (\forall i) \).

Finally, define the \( d \)th cyclotomic polynomial

\[ f_d(\lambda) := \prod_{1 \leq j \leq d - 1} \text{if } (d, j) = 1 (\lambda - \zeta_d^j), \]

with \( f_1(\lambda) = 1 \) by convention; then we have

\[ \lambda^n - 1 = \prod_{1 \leq d \leq n, d \mid n} f_d(\lambda), \]

\footnote{I have changed font for the field, because we want to think of \( A = F \) as a field extension of some original field \( \mathbb{F} \).}
and similarly for $\lambda^{m_i} - 1$. So

$$m_i \mid n \ (\forall i \geq q) \implies \frac{\lambda^n - 1}{\lambda^{m_i} - 1} \in (f_n(\lambda)) \subset \mathbb{Z}[\lambda] \ (\forall i \geq q)$$

$$\implies q^n - 1, \frac{q^n - 1}{q^{m_i} - 1} \in (f_n(q)) \subset \mathbb{Z} \ (\forall i \geq q)$$

$$\implies f_n(q) \mid q - 1 \quad \text{(V.B.14)}$$

$$\implies |f_n(q)||q - 1.$$ 

But

$$|f_n(q)| = \prod_{(j,n) = 1} |q - \zeta_n^j| > q - 1,$$ 

and we have a contradiction, unless $n = 1$. \qed