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 $\mathbb{Q}[\zeta_5]$ 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**[3] 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 α of a field extension which is algebraic over $\mathbb{C}$ satisfies a polynomial equation $P(\alpha) = 0$, α 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

[3]Warning: these need not be finite-dimensional (though they certainly are if they are finitely generated).

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

$$\begin{aligned} \mathrm{ev}_a \colon \mathbb{F}[\lambda] &\twoheadrightarrow \mathbb{F}[a] \subset A \\ f(\lambda) &\mapsto f(a). \end{aligned}$$

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, $A = \mathbb{F}$. □

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

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

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

$$\begin{aligned} p(\lambda) &= \textstyle\prod_{i=1}^{r}(\lambda - a_i) \times \prod_{k=1}^{s}(\lambda - \beta_k)(\lambda - \bar{\beta}_k) \\ &= \textstyle\prod_{i=1}^{r}(\lambda - a_i) \times \prod_{k=1}^{s}(\lambda^2 - 2\Re(\beta_k) + |\beta_k|^2), \end{aligned}$$

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 $\alpha \in A \backslash \mathbb{R}$, we consider as usual

$$\mathrm{ev}_\alpha \colon \mathbb{R}[\lambda] \twoheadrightarrow \mathbb{R}[\alpha] \subset A,$$

which as above has a nontrivial kernel K since $\dim_{\mathbb{F}}(A) < \infty$. Since $\mathbb{R}[\lambda]$ is a PID, $K = (m_\alpha)$ with m_α 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 $\beta \in A\backslash\mathbb{R}$ and $\beta^2 = a^2 - b < 0$.

Now consider the subset

$$A' := \{\alpha \in A \mid \alpha^2 \in \mathbb{R}_{\leq 0}\} \subset (A \backslash \mathbb{R}) \cup \{0\}.$$

From the last paragraph it is clear that if $A \backslash \mathbb{R} \neq \emptyset$, 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 $(\alpha r)^2 = \alpha^2 r^2 \leq 0 \implies \alpha r \in A'$. So A' is closed under multiplication and we only need to check sums of elements. So let $u, v \in A' \backslash \{0\}$ 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 $u + v$, $u - v \in A \backslash \mathbb{R}$; and so as above (for α), 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

$$0 = c + d + (uv + vu) - p(u + v) - q$$
$$\text{and} \quad 0 = c + d - (uv + vu) - r(u - v) - s,$$

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. □

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 $a \in \mathbb{R}$, $Q(au) = a^2 Q(u)$, so Q is quadratic. Finally, $Q(u) \geq 0$ for all $u \in A'$ (by definition of A'). □

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. $A \supsetneq \mathbb{R}$, and pick $\mathbf{i} \in A'$ such that $Q(\mathbf{i}) = 1$; we can do this by rescaling any element in $A' \backslash \{0\}$ by a real number. Then $\mathbf{i}^2 = -1$, and we fix the copy of $\mathbb{C} = \mathbb{R} + \mathbf{i}\mathbb{R} = \mathbb{R}[\mathbf{i}] \subset A$.

Next, suppose that $A \supsetneq \mathbb{C}$; then $A' \supsetneq \mathbf{i}\mathbb{R}$, and we pick $\hat{\jmath} \in A' \backslash \mathbf{i}\mathbb{R}$ and take $\tilde{\mathbf{j}} := \hat{\mathbf{j}} - \mathbf{i}B(\mathbf{i}, \hat{\mathbf{j}})$. This gives $B(\tilde{\mathbf{j}}, \mathbf{i}) = B(\hat{\mathbf{j}}, \mathbf{i}) - B(\mathbf{i}, \hat{\mathbf{j}})B(\mathbf{i}, \mathbf{i}) = 0$, and rescaling $\tilde{\mathbf{j}}$ gives $\mathbf{j}$ with $\mathbf{j}^2 = -1$ and $\mathbf{j} \perp \mathbf{i}$ (i.e. $0 = B(\mathbf{i}, \mathbf{j}) = \mathbf{ij} + \mathbf{ji}$). Setting $\mathbf{k} = \mathbf{ij}$, we compute

$$\begin{cases} \mathbf{k}^2 = \mathbf{ijij} = -\mathbf{iijj} = -(-1)(-1) = -1 \\ \mathbf{ik} = \mathbf{i}^2\mathbf{j} = -\mathbf{j} = \mathbf{jii} = -\mathbf{iji} = -\mathbf{ki} \\ \mathbf{jk} = \cdots = -\mathbf{kj} \end{cases}$$

$$\Longrightarrow \quad \begin{cases} \mathbf{k} \in A', \quad \mathbf{k} \perp \mathbf{i}, \mathbf{j} \\ 1, \mathbf{i}, \mathbf{j}, \mathbf{k} \;\; \mathbb{R}\text{-linearly independent} \\ \mathbb{R} + \mathbf{i}\mathbb{R} + \mathbf{j}\mathbb{R} + \mathbf{k}\mathbb{R} = \mathbb{H} \subset A. \end{cases}$$

Finally, suppose $A \supsetneq \mathbb{H}$. Then there exists $\ell \in A'$ with $Q(\ell) = 1$ and $\ell \perp \mathbf{i}, \mathbf{j}, \mathbf{k}$. As above, this gives $\ell\mathbf{i} = -\mathbf{i}\ell$, $\ell\mathbf{j} = -\mathbf{j}\ell$, and $\ell\mathbf{k} = -\mathbf{k}\ell$; substituting $\mathbf{k} = \mathbf{ij}$ in the last of these gives

$$-(\mathbf{ij})\ell = \ell(\mathbf{ij}) = (\ell\mathbf{i})\mathbf{j} = -(\mathbf{i}\ell)\mathbf{j} = -\mathbf{i}(\ell\mathbf{j}) = \mathbf{i}(\mathbf{j}\ell) = (\mathbf{ij})\ell,$$

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** $\mathbb{O} = \mathbb{H} \times \mathbb{H}$ with the multiplication law

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

where "$*$" denotes "quaternionic conjugation" ($\mathbf{i} \mapsto -\mathbf{i}$, $\mathbf{j} \mapsto -\mathbf{j}$, $\mathbf{k} \mapsto -\mathbf{k}$). More or less, this mimics the way you get $\mathbb{H}$ from $\mathbb{C} \times \mathbb{C}$ and $\mathbb{C}$ from $\mathbb{R} \times \mathbb{R}$. 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 classsification of simple Lie groups over $\mathbb{C}$.

V.B.10. REMARK. There are lots of non-isomorphic 4-dimensional "quaternion algebras" over $\mathbb{Q}$, 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 $\mathbb{Q}$-division algebras. Alas, this is not the case: for instance, if γ is an even integer not divisible by 8, the $\mathbb{Q}$-algebra generated by x, y subject to the relations

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

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 $\mathbb{F}$ (i.e. $|\mathbb{F}| < \infty$), with $n := \dim_{\mathbb{F}} A < \infty$. Clearly $|A| = |\mathbb{F}|^n$, and so (forgetting the $\mathbb{F}$-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 $\mathbb{F}$-division algebras when $|\mathbb{F}| < \infty$.

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 $A = F$.[4]

Applying the class equation to the group $A^* = A\backslash\{0\}$ gives

$$|A^*| = \textstyle\sum_i |\mathrm{ccl}(x_i)| = \sum_i [A^* \colon \mathrm{stab}(x_i)] \tag{V.B.13}$$

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 $x_i \in A^*\backslash F^*$, 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 $|\mathrm{stab}(x_i)| = q^{m_i} - 1$. Thus (V.B.13) becomes

$$q^n - 1 = |A| - 1 = |A^*| = (q-1) + \textstyle\sum_{i \geq q} \frac{q^n - 1}{q^{m_i} - 1}. \tag{V.B.14}$$

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,

$$F^n = A = \underbrace{A_i \oplus \cdots \oplus A_i}_{d_i} = \underbrace{F^{m_i} \oplus \cdots \oplus F^{m_i}}_{d_i}$$

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

Finally, define the d^{th} cyclotomic polynomial

$$f_d(\lambda) := \prod_{\substack{1 \leq j \leq d-1 \\ (d,j) = 1}} (\lambda - \zeta_d^j),$$

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

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

[4]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

$$\begin{aligned} m_i \mid n \ (\forall i \geq q) &\implies \frac{\lambda^n - 1}{\lambda^{m_i}-1} \in (f_n(\lambda)) \subset \mathbb{Z}[\lambda] \ \ (\forall i \geq q) \\ &\implies q^n - 1, \ \frac{q^n-1}{q^{m_i}-1} \in (f_n(q)) \subset \mathbb{Z} \ \ (\forall i \geq q) \\ &\underset{\text{(V.B.15)}}{\implies} f_n(q) \mid q-1 \\ &\implies |f_n(q)| | q-1. \end{aligned}$$

But

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

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

V.B.15. COROLLARY. *Any finite domain R is a field.*

PROOF. For any $r \in R$, left-multiplication ℓ_r gives a map $R \to R$. This map is injective since there R has no zero-divisors. By the pigeonhole principle, it is therefore surjective, and there exists $r' \in R$ with $rr' = 1_R$. So $R \setminus \{0\} = R^*$ and R is a division ring, and we are done by V.B.11. □