

## §46 Algebras

In this last paragraph of Chapter 4, we consider multiplication of vectors. If, on a vector space, there is an associative multiplication which is distributive over addition and compatible with multiplication by scalars, the vector space is said to be an algebra. The formal definition is as follows.

**46.1 Definition:** Let  $K$  be a field and  $(V,+)$  an abelian group. A quintuple  $(V,+,\circ,K,\cdot)$  is called an *algebra over  $K$* , or a  *$K$ -algebra* provided

- (i)  $(V,+,\circ)$  is a ring,
- (ii)  $(V,+,\cdot)$  is a vector space,
- (iii)  $(\alpha \cdot a) \circ b = \alpha \cdot (a \circ b) = a \circ (\alpha \cdot b)$  for all  $\alpha \in K, a, b \in V$ .

It is implicit in this definition that  $\circ$  is a binary operation on  $V$ , called multiplication, and  $\cdot$  is a mapping from  $K \times V$  into  $V$ , called multiplication by scalars. As usual, we drop these symbols and write  $\alpha a$  for  $\alpha \cdot a$ , and  $ab$  for  $a \circ b$ . Then (iii) becomes a kind of associativity law:  $(\alpha a)b = \alpha(ab) = a(\alpha b)$ . As usual, we shall call  $V$ , rather than the quintuple  $(V,+,\circ,K,\cdot)$ , a  $K$ -algebra.

**Examples: (a)** Let  $K$  be a field and  $L$  a field containing  $K$ . Then  $L$  is a algebra over  $K$ .

**(b)** Let  $K$  be a field. Then  $Mat_n(K)$  is a  $K$ -vector space (Theorem 43.4) and also a ring (Theorem 43.11). Since  $(\alpha A)B = \alpha(AB) = A(\alpha B)$  for all  $\alpha$  in  $K$  and  $A, B$  in  $Mat_n(K)$  (see (e) in §43, p. 523), we conclude that  $Mat_n(K)$  is a  $K$ -algebra. ?

**(c)** Let  $K$  be a field and  $V$  a vector space over  $K$ . Then  $L_K(V, V)$  is a  $K$ -vector space (Theorem 43.1) and also a ring (Theorem 43.12). Moreover, whenever  $\alpha \in K$  and  $T, S \in L_K(V, V)$ , there hold

$$\varkappa((\alpha T)S) = (\varkappa(\alpha T))S = ((\alpha \varkappa)T)S = (\alpha \varkappa)(TS) = \varkappa(\alpha(TS))$$

and

$$\varkappa(T(\alpha S)) = (\varkappa T)(\alpha S) = (\alpha(\varkappa T))S = \alpha((\varkappa T)S) = \alpha(\varkappa(TS)) = (\alpha \varkappa)(TS) = \varkappa(\alpha(TS))$$

for all  $\varkappa \in V$ , thus  $(\alpha T)S = \alpha(TS) = T(\alpha S)$ . Thus  $L_K(V, V)$  is a  $K$ -algebra.

**(d)** Let  $K$  be a field and  $x$  an indeterminate over  $K$ . Then  $K[x]$  is a vector space over  $K$  (Example 39.2(d)) and also a ring. We have  $(af(x))g(x) = a(f(x)g(x)) = f(x)(ag(x))$  for all  $a \in K$  and  $f(x), g(x) \in K[x]$ . Thus  $K[x]$  is an algebra over  $K$ . Likewise the ring  $K[x_1, x_2, \dots, x_n]$  of polynomials in  $n$  indeterminates is an algebra over  $K$ .

**46.3 Lemma:** *Let  $K$  be a field and  $V$  a finite dimensional vector space over  $K$ . Suppose there is a multiplication on  $V$  which is distributive over addition, and suppose that*

$$(\alpha a)c = \alpha(ac) = a(\alpha c) \quad \text{for all } \alpha \in K \text{ and } a, c \in V$$

(thus all conditions for  $V$  to be an algebra over  $K$  are satisfied except that associativity of multiplication is open).

Let  $B$  be a  $K$ -basis of  $V$ . Then multiplication on  $V$  is associative and  $V$  is a  $K$ -algebra if and only if

$$(bb')b'' = b(b'b'') \quad \text{for all } b', b'', b''' \in B.$$

**Proof:** If multiplication on  $V$  is associative, then  $(bb')b'' = b(b'b'')$  holds for all elements  $b', b'', b'''$  of  $V$ , in particular, for all  $b', b'', b'''$  in  $B$ .

Assume conversely that  $(bb')b'' = b(b'b'')$  for all  $b', b'', b'''$  in  $B$ . We put  $B = \{b_1, b_2, \dots, b_n\}$ . If  $x, y, z$  are arbitrary elements of  $V$ , we write them as

$$x = \sum_{i=1}^n \alpha_i b_i, \quad y = \sum_{j=1}^n \beta_j b_j, \quad z = \sum_{k=1}^n \gamma_k b_k$$

with suitable scalars  $\alpha_i, \beta_j, \gamma_k$ . Using distributivity and (iii), we find

$$\begin{aligned} (xy)z &= \left( \sum_{i=1}^n \alpha_i b_i \sum_{j=1}^n \beta_j b_j \right) \cdot \sum_{k=1}^n \gamma_k b_k = \sum_{i,j=1}^n (\alpha_i b_i)(\beta_j b_j) \cdot \sum_{k=1}^n \gamma_k b_k \\ &= \sum_{i,j=1}^n \alpha_i (\beta_j (b_i b_j)) \cdot \sum_{k=1}^n \gamma_k b_k = \sum_{i,j=1}^n \alpha_i (\beta_j (b_i b_j)) \cdot \sum_{k=1}^n \gamma_k b_k \\ &= \sum_{i,j=1}^n (\alpha_i \beta_j) (b_i b_j) \cdot \sum_{k=1}^n \gamma_k b_k = \sum_{i,j,k=1}^n ((\alpha_i \beta_j) (b_i b_j)) (\gamma_k b_k) \end{aligned}$$

$$\begin{aligned}
&= \sum_{i,j,k=1}^n (\alpha_i \beta_j) ((b_i b_j) (\gamma_k b_k)) &= \sum_{i,j,k=1}^n (\alpha_i \beta_j) [\gamma_k ((b_i b_j) b_k)] \\
&= \sum_{i,j,k=1}^n ((\alpha_i \beta_j) \gamma_k) ((b_i b_j) b_k)
\end{aligned}$$

and likewise  $x(yz) = \sum_{i=1}^n \alpha_i b_i \cdot \left( \sum_{j=1}^n \beta_j b_j \sum_{k=1}^n \gamma_k b_k \right) = \sum_{i=1}^n \alpha_i b_i \cdot \sum_{j,k=1}^n (\beta_j \gamma_k) (b_j b_k)$

$$= \sum_{i,j,k=1}^n (\alpha_i (\beta_j \gamma_k)) (b_i (b_j b_k)).$$

Now  $(\alpha_i \beta_j) \gamma_k = \alpha_i (\beta_j \gamma_k)$  since the multiplication on  $K$  is associative and  $(b_i b_j) b_k = b_i (b_j b_k)$  by hypothesis, so  $(xy)z = x(yz)$ . Hence the multiplication on  $V$  is also associative.  $\square$

**46.4 Examples: (a)** Let  $K$  be a field and  $G$  a finite multiplicative group. Let  $KG$  denote the  $K$ -vector space that has  $G$  as a  $K$ -basis. Thus the elements of  $KG$  are sums  $\sum_{i=1}^{|G|} \alpha_i g_i$  where  $G = \{g_1, g_2, \dots, g_{|G|}\}$ . It will be

convenient to modify this notation as  $\sum_{g \in G} \alpha_g g$ . Two elements  $\sum_{g \in G} \alpha_g g$  and

$\sum_{g \in G} \beta_g g$  of  $KG$  are equal if and only if  $\alpha_g = \beta_g$  for each  $g \in G$ . The sum of

$\sum_{g \in G} \alpha_g g$  and  $\sum_{g \in G} \beta_g g$  is  $\sum_{g \in G} (\alpha_g + \beta_g) g$ , and the product of  $\gamma \in K$  by  $\sum_{g \in G} \alpha_g g$

is  $\sum_{g \in G} \gamma \alpha_g g$ . We now define a multiplication on  $KG$  by extending the

multiplication on  $G$  using distributivity. More precisely, we define the

product of  $\sum_{g \in G} \alpha_g g$  by  $\sum_{g \in G} \beta_g g = \sum_{h \in G} \beta_h h$  to be  $\sum_{g \in G} \alpha_g g \sum_{h \in G} \beta_h h =$

$$\sum_{g,h \in G} \alpha_g \beta_h gh = \sum_{k \in G} \left( \sum_{\substack{g,h \in G \\ gh=k}} \alpha_g \beta_h \right) k.$$



$$\begin{aligned}
& + (\alpha\beta' + \beta\alpha' + \gamma\delta' - \delta\gamma')i \\
& + (\alpha\gamma' - \beta\delta' + \gamma\alpha' + \delta\beta')j \\
& + (\alpha\delta' + \beta\gamma' - \gamma\beta' + \delta\alpha')k
\end{aligned}$$

which may be taken as the definition of multiplication on  $\mathbb{H}$ . One checks that this multiplication is distributive over addition, and that  $e$  is an identity element. To prove the associativity of multiplication, we must only verify the  $4^3 = 64$  equations  $(ab)c = a(bc)$ , where  $a, b, c \in \{e, i, j, k\}$  (Lemma 46.3). This verification is left to the reader. The multiplication is thus seen to be associative. One also finds immediately  $(\alpha a)b = \alpha(ab) = a(\alpha b)$  for any  $\alpha \in \mathbb{R}$  and  $a, b \in \mathbb{H}$ . Thus  $\mathbb{H}$  is an algebra over  $\mathbb{R}$ . This algebra was discovered by the Irish mathematician W. R. Hamilton (1805–1865). The elements of  $\mathbb{H}$  are called *quaternions*, and  $\mathbb{H}$  is known as the *Hamiltonian algebra of quaternions*. It is not commutative, since  $ij = e \neq e = ji$ , for example.

Since  $e$  is the identity of  $\mathbb{H}$ , we will write 1 instead of  $e$  and  $\alpha$  instead of  $\alpha e$  (here  $\alpha \in \mathbb{R}$ ). Then any real number  $\alpha$  can be thought of as a quaternion  $\alpha 1 = \alpha + 0i + 0j + 0k$ . In like manner, any complex number  $\alpha + \beta i$  (where  $\alpha, \beta \in \mathbb{R}$ ) can be considered as a quaternion  $\alpha + \beta i + 0j + 0k$ . In this way, we may suppose that  $\mathbb{R}$  and  $\mathbb{C}$  are subrings of  $\mathbb{H}$ .

For any  $a \in \mathbb{H}$ , say  $\alpha + \beta i + \gamma j + \delta k$  with  $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ , we say  $\alpha$  is the *real part of  $a$*  and  $\beta i + \gamma j + \delta k$  is the *imaginary part of  $a$* . We also put  $\bar{a} = \alpha - \beta i - \gamma j - \delta k$  and call  $\bar{a}$  the *conjugate of  $a$* . It is easily seen that  $\overline{ab} = \bar{b}\bar{a}$  for any  $a, b \in \mathbb{H}$  (note the reversal of the conjugates). We define the *norm of  $a$* , denoted as  $N(a)$ , to be  $a\bar{a}$ . Thus  $N(\alpha + \beta i + \gamma j + \delta k)$  is equal to  $\alpha^2 + \beta^2 + \gamma^2 + \delta^2$ . Note that  $N(a) \in \mathbb{R}$ . Clearly  $N(a) = 0$  if and only if  $a = 0$ .

There holds  $N(ab) = ab\overline{ab} = ab\bar{b}\bar{a} = aN(b)\bar{a} = N(b)a\bar{a} = N(b)N(a) = N(ab)$  for any quaternions  $a, b \in \mathbb{H}$ . This is equivalent to the identity

$$\begin{aligned}
(\alpha^2 + \beta^2 + \gamma^2 + \delta^2)(\alpha'^2 + \beta'^2 + \gamma'^2 + \delta'^2) &= (\alpha\alpha' - \beta\beta' - \gamma\gamma' - \delta\delta')^2 \\
&+ (\alpha\beta' + \beta\alpha' + \gamma\delta' - \delta\gamma')^2 \\
&+ (\alpha\gamma' - \beta\delta' + \gamma\alpha' + \delta\beta')^2 \\
&+ (\alpha\delta' + \beta\gamma' - \gamma\beta' + \delta\alpha')^2
\end{aligned}$$

which holds in fact in any commutative ring. Thus the product of two numbers, each of which is a sum of four squares, is also a sum of four squares.

Just like we divide a complex number  $a = \alpha + \beta i$  by a nonzero complex number  $b = \gamma + \delta i$  by multiplying the numerator and denominator of  $a/b$  by the conjugate  $\bar{b} = \gamma - \delta i$  of  $b$ :

$$\frac{a}{b} = \frac{\alpha + \beta i}{\gamma + \delta i} = \frac{\alpha + \beta i}{\gamma + \delta i} \frac{\gamma - \delta i}{\gamma - \delta i} = \frac{\alpha\gamma + \beta\delta}{\gamma^2 + \delta^2} + \frac{-\alpha\delta + \beta\gamma}{\gamma^2 + \delta^2} i,$$

we can divide any quaternion  $a$  by any nonzero quaternion  $b$  by multiplying the "numerator" and "denominator" of  $a/b$  by the conjugate  $\bar{b}$ :

$$\frac{a}{b} = \frac{a\bar{b}}{b\bar{b}} = \frac{a\bar{b}}{N(b)}.$$

More exactly, any nonzero quaternion  $b$  has a multiplicative inverse  $(1/N(b))\bar{b}$ . Thus  $\mathbb{H}$  is a division ring. An algebra which is a division ring is called a division algebra. So  $\mathbb{H}$  is a division algebra.

An interesting theorem of F. G. Frobenius (1849-1917) states that  $\mathbb{R}, \mathbb{C}$  and  $\mathbb{H}$  are the only division algebras over  $\mathbb{R}$ .

(c) The last example can be generalized. Let  $K$  be a field in which  $1 + 1$  is distinct from 0. Let  $Q = K^4$  be the four-dimensional  $K$ -vector space of ordered quadruples, and let  $e = (1,0,0,0)$ ,  $i = (0,1,0,0)$ ,  $j = (0,0,1,0)$ ,  $k = (0,0,0,1)$ . Thus  $\{e, i, j, k\}$  is a basis of  $Q$  over  $K$ . We define a multiplication on  $Q$  by

$$\begin{aligned} (\alpha e + \beta i + \gamma j + \delta k)(\alpha' e + \beta' i + \gamma' j + \delta' k) &= (\alpha\alpha' - \beta\beta' - \gamma\gamma' - \delta\delta')e \\ &+ (\alpha\beta' + \beta\alpha' + \gamma\delta' - \delta\gamma')i \\ &+ (\alpha\gamma' - \beta\delta' + \gamma\alpha' + \delta\beta')j \\ &+ (\alpha\delta' + \beta\gamma' - \gamma\beta' + \delta\alpha')k \end{aligned}$$

This multiplication is associative, distributive over addition and  $e$  is an identity element. One checks easily  $(\alpha a)b = \alpha(ab) = a(\alpha b)$  for any  $\alpha \in K$  and  $a, b \in Q$ . Thus  $Q$  is a  $K$ -algebra.  $Q$  is called the *algebra of quaternions over  $K$* . This time it will be convenient *not* to identify  $\alpha \in K$  with  $\alpha e \in Q$ .

The *conjugate*  $\bar{a}$  of  $a = \alpha e + \beta i + \gamma j + \delta k \in Q$  is defined to be  $\alpha e - \beta i - \gamma j - \delta k$  and the *norm*  $N(a)$  of  $a$  to be  $a\bar{a}$ . Thus  $N(\alpha e + \beta i + \gamma j + \delta k) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$ . If  $K$  is a field such that  $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 0$  implies  $\alpha = \beta = \gamma = \delta = 0$ , then any nonzero  $a \in Q$  has a multiplicative inverse  $(1/N(a))\bar{a}$  and  $Q$  is a division algebra. Otherwise,  $Q$  has zero divisors: there is a nonzero  $a \in Q$  such that  $a\bar{a} = 0$ .

## Exercises

1. Multiply  $2\iota + 3(12) + (13) - 2(23) + (123) - 3(132)$  by  $\iota + 2(12) + 4(13) - 3(23) + 2(123) + (132)$  in  $\mathbb{Q}S_3$ .

2. Let  $G$  be a finite group,  $K$  a field. Put  $e = \sum_{g \in G} g \in KG$ . Show that  $e^2 = |G|e$ .

3. Let  $K$  be a field and  $A$  an algebra over  $K$ . Prove that the center  $Z(A)$  of  $A$  (see §32, Ex. 1) is a subspace of  $A$ .

4. Let  $G$  be a finite group. Show that  $\dim_{\mathbb{Q}} Z(\mathbb{Q}G)$  is equal to the number of conjugacy classes in  $G$ .

5. For any  $a \in \mathbb{H}$ , show that there are real numbers  $t, n$  such that

$$a^2 - ta + n = 0.$$

6. Prove that  $a^2iai + ia^2ia - iaia^2 - aia^2i = 0$  for any  $a \in \mathbb{H}$ .

7. Let  $a, b \in \mathbb{H}$ . Show that  $ab = ba$  if and only if  $1, a, b$  are linearly dependent over  $\mathbb{R}$ .

8. Prove that  $\{\mp 1, \mp i, \mp j, \mp k\} \subseteq \mathbb{H}$  is a group isomorphic to  $Q_8$  (see §17, Ex.15) and that  $S = \{\mp 1, \mp i, \mp j, \mp k, \frac{\mp 1 \mp i \mp j \mp k}{2}\} \subseteq \mathbb{H}$  is a group isomorphic to  $SL(2, \mathbb{Z}_3)$ . Show that  $\{\mp 1\} \triangleleft S$  and  $S/\{\mp 1\} \cong A_4$ .

9. Prove that the quaternion algebra over  $\mathbb{C}$  is isomorphic (as ring and  $\mathbb{C}$ -vector space) to the  $\mathbb{C}$ -algebra  $Mat_2(\mathbb{C})$ .

10. Let  $K$  be a field in which  $1 + 1 \neq 0$  and  $\alpha, \beta$  nonzero elements in  $K$ . Let  $A$  be the four dimensional  $K$ -vector space with  $K$ -basis  $e, i, j, k$ . On  $A$ , we define a multiplication by the multiplication table on the basis elements:

$$\begin{array}{ccccc}
& e & i & j & k \\
e & e & i & j & k \\
i & i & \alpha e & k & j \\
j & j & -k & \beta e & -\beta i \\
k & k & -\alpha j & \beta i & -\alpha \beta e
\end{array}$$

(a) Prove that this multiplication makes  $A$  into a  $K$ -algebra ( $\mathbb{H}$  is a special case  $K = \mathbb{R}$ ,  $\alpha = \beta = -1$ ).

(b) Show that the center of  $A$  is  $\{ke \in A: k \in K\}$  and that  $A$  has no ideals aside from  $0$  and  $A$ .

(c) Define the *conjugate*  $\bar{a}$  of  $a = \alpha e + \beta i + \gamma j + \delta k \in A$  to be  $\alpha e - \beta i - \gamma j - \delta k$  and the *norm*  $N(a)$  of  $a$  to be  $a\bar{a}$ . Verify  $\overline{ab} = \bar{b}\bar{a}$  and  $N(ab) = N(a)N(b)$  for any  $a, b \in A$ .

(d) Prove that  $A$  is a division algebra if and only if  $N(a) \neq 0$  for any nonzero  $a \in A$  and this holds if and only if  $\gamma_0^2 = \alpha \gamma_1^2 + \beta \gamma_2^2$  implies  $\gamma_0 = \gamma_1 = \gamma_2 = 0$  for any  $\gamma_0, \gamma_1, \gamma_2 \in K$ .

(e) If  $K$  is finite, say  $|K| = q$ , show that there are  $q + 1$  elements in  $\{\alpha \gamma_1^2 \in K: \gamma_1 \in K\}$  and  $\{1 - \beta \gamma_2^2 \in K: \gamma_2 \in K\}$  and conclude that  $A$  is not a division algebra (This is a special case of an important theorem due to H. J. M. Wedderburn (1882-1948) which states that any finite division algebra is a field).

11. If  $1 + 1 = 0$  in a field  $K$  and  $A$  is as in Ex.10, show that the mapping  $x \rightarrow x^2$  is a ring homomorphism from  $A$  into  $A$ .