Definition. Let F be a field. An F-*algebra* is a vector space A over F equipped with an operation $A \times A \to A$ which is bilinear. In other words, for a vector space A to be an F-algebra there must be a vector multiplication operation $(v, w) \to vw$ (defined for all $v, w \in A$) such that

$$(\lambda v + \mu w)u = \lambda(vu) + \mu(wu)$$

and

$$u(\lambda v + \mu w) = \lambda(uv) + \mu(uw)$$

for all $u, v, w \in A$ and $\lambda, \mu \in F$.

For example, $\mathbb{R}^3$ with the usual vector product (cross product) is an $\mathbb{R}$-algebra. Note that this algebra is not associative: it is not true that $(u \times v) \times w = u \times (v \times w)$ for all u, v and w in $\mathbb{R}^3$. In fact this algebra is an example of what are known as *Lie algebras*, which are the second most important kind of algebras. The most important kind, and the only kind that we will be concerned with in this course, are *associative algebras*: those algebras A satisfying $(uv)w = u(vw)$ for all $u, v, w \in A$. The best example of an associative F-algebra is $\mathrm{Mat}_n(F)$, the set of all $n \times n$ matrices over F. It is well known that this is an n^2 dimensional vector space over F, and that matrix multiplication (defined in the usual way) is bilinear and associative. Another example is $\mathcal{P}(F)$, the set of all polynomials over F. This is an infinite dimensional vector space, and multiplication of polynomials, defined in the usual manner, is a bilinear associative operation. Unlike the algebra of $n \times n$ matrices over F, the algebra of polynomials over F is *commutative*: it satisfies $pq = qp$ for all $p, q \in \mathcal{P}(F)$.

Suppose that A is an F-algebra which is finite-dimensional as a vector space over F. Let $v_1, v_2, \ldots, v_n$ be a vector space basis for A. Then there exist scalars $\alpha_{ijk} \in F$ such that

$$v_i v_j = \sum_{k=1}^{n} \alpha_{ijk} v_k \qquad \text{for all } i, j \in \{1, 2, \ldots, n\}.$$

These scalars α_{ijk} are called the *structure constants* of A for the given basis. Note that the structure constants determine the multiplication completely, since if $u, v \in A$ are arbitrary then there exist scalars λ_i, μ_j with $u = \sum_i \lambda_i v_i$ and $v = \sum_j \mu_j v_j$, and this gives

$$uv = \Big(\sum_i \lambda_i v_i\Big)\Big(\sum_j \mu_j v_j\Big) = \sum_{i,j} \lambda_i \mu_j \Big(\sum_k \alpha_{ijk} v_k\Big) = \sum_k \Big(\sum_{i,j} \lambda_i \mu_j \alpha_{ijk}\Big) v_k. \tag{1}$$

Conversely, given a vector space A with basis $v_1, v_2, \ldots, v_n$, if we choose scalars α_{ijk} arbitrarily and use Eq. (1) to define a multiplication operation on A, then the resulting operation is associative, and hence gives A the structure of an F-algebra.

Examples

(i) A 2-dimensional vector space over $\mathbb{R}$ with basis $v_1\, v_2$ can be given an $\mathbb{R}$-algebra structure by defining $v_1 v_j = v_j v_1 = v_j$ (for both values of j) and $v_2^2 = -v_1$. The resulting algebra is easily seen to be isomorphic to $\mathbb{C}$ via $\lambda v_1 + \mu v_2 \mapsto \lambda + i\mu$.

(ii) The is a 4-dimensional associative $\mathbb{R}$-algebra with basis $1, i, j, k$ and multiplication defined by

$$ij = k, \quad jk = i, \quad ki = j, \quad ji = -k, \quad ik = -j, \quad kj = -i,$$
$$1i = i1 = i, \quad 1j = j1 = j, \quad 1k = k1 = k, \quad i^2 = j^2 = k^2 = -1.$$

This algebra is known as the *algebra of quaternions* over $\mathbb{R}$. The elements ± 1, $\pm i$, $\pm j$, $\pm k$ of the quaternion algebra form a group called *the quaternion group* of order 8 (obtained in a different guise in Lectures 2 and 3).

(iii) If we let X_{ij} be the $n \times n$ matrix whose (r, s)-entry is $\delta_{ir}\delta_{js}$ then the n^2 matrices X_{ij} for $i, j \in \{1, 2, \ldots, n\}$ form a basis for the algebra of all $n \times n$ matrices. The structure constants for this basis are all either 0 or 1. Specifically, $X_{ij}X_{kl} = \delta_{jk}X_{il}$.

If A, B are F-algebras then their *direct sum* is

$$A \oplus B = \{\, (a, b) \mid a \in A,\ b \in B \,\}$$

made into a vector space in the usual way, with multiplication given by

$$(a, b)(a', b') = (aa', bb') \qquad \text{for all } a,\ a' \in A \text{ and } b,\ b' \in B.$$

Note that if $a_1, a_2, \ldots, a_n$ form a basis for A and $b_1, b_2, \ldots, b_m$ a basis for B then $A \oplus B$ has a basis

$$(a_1, 0),\ (a_2, 0),\ \ldots,\ (a_n, 0),\ (0, b_1),\ (0, b_2),\ \ldots,\ (0, b_m);$$

furthermore, the first n of these span a subalgebra A' of $A \oplus B$ which is isomorphic to A, the remaining m basis vectors span a subalgebra B' of $A \oplus B$ isomorphic to B, and A' and B' annihilate each other (meaning $ab = 0$ whenever $a \in A'$ and $b \in B'$.)

If A is an F-algebra then an *identity element* for A is an element $1 \in A$ such that $1a = a1 = a$ for all $a \in A$. Henceforth in this course we shall use the term "F-algebra" as an abbreviation for "associative F-algebra with an identity element".

Definition. Let G be a finite group an F a field. The *group algebra* FG is an F-algebra having the elements of G as a basis, the multiplication of basis elements coinciding with multiplication in the group G.

The elements of FG are *formal linear combinations* of elements of G: expressions of the form $\sum_{g \in G} \lambda_g g$. What this really means is that we choose some vector space over F whose dimension is $|G|$—the space of all $|G|$-component column vectors would do—and fix a basis of this space. Then choose (arbitrarily) a one to one correspondence between these basis elements and elements of G, and use this to identify the elements of G with the basis vectors. Multiplication in G then determines a natural way to define multiplication of the basis elements, and, as we have seen, bilinearity then determines multiplication uniquely for arbitrary elements of the space.

Examples

(i) Let $G = \{1, x\}$ be the group of order 2. The real group algebra $\mathbb{R}G$ is $\{\, \lambda 1 + \mu x \mid \lambda,\ \mu \in \mathbb{R} \,\}$, with multiplication given by

$$(\lambda 1 + \mu x)(\lambda' 1 + \mu' x) = (\lambda\lambda' + \mu\mu')1 + (\lambda\mu' + \mu\lambda')x.$$

Now choose new basis for $\mathbb{R}G$ consisting of the two elements $e = \frac{1}{2}(1 + x)$ and $f = \frac{1}{2}(1 - x)$. It is easily seen that e and f are *idempotent elements*: $e^2 = e$ and $f^2 = f$. Furthermore, $ef = fe = 0$. Thus it follows that for all λ, λ', μ, $\mu' \in \mathbb{R}$

$$(\lambda e + \mu f)(\lambda' e + \mu' f) = (\lambda\lambda')e + (\mu\mu')f,$$

and hence $\mathbb{R}G$ is isomorphic to $\mathbb{R}\oplus\mathbb{R}$ via the one to one correspondence $\lambda e+\mu f \leftrightarrow (\lambda,\mu)$.

(ii) Let G be the Klein 4-goup, with elements 1, a, b and c (where a, b and c all have order 2 and $ab=c$). The real group algebra $\mathbb{R}G$ consists of all linear combinations $\lambda 1+\mu a+\nu b+\xi c$, where λ, μ, ν, $\xi\in\mathbb{R}$. It can be checked that the four elements of the form $\frac{1}{4}(1\pm a\pm b\pm c)$ where the product of the signs is $+1$ are all idempotents and annihilate one another. Moreover, they form a basis for $\mathbb{R}G$. In this way it can be shown that $\mathbb{R}G$ is isomorphic to the direct sum of four copies of $\mathbb{R}$.

(iii) The complex group algebra of S_3 is the six dimensional complex vector space

$$\{\,\alpha\,\mathrm{id}+\beta(1\,2)+\gamma(1\,3)+\delta(2\,3)+\varepsilon(1\,2\,3)+\zeta(1\,3\,2)\mid \alpha,\ \beta,\ \gamma,\ \delta,\ \varepsilon,\ \zeta\in\mathbb{C}\,\}$$

with multiplication determined by the rule for multiplying permutations. It can be shown that this algebra is isomorphic to the sum of two copies of $\mathbb{C}$ and one copy of $\mathrm{Mat}_2(\mathbb{C})$.

Definition. Let A be an F-algebra. A matrix representation of A of degree d is a function $\phi\colon A\to\mathrm{Mat}_d(F)$ satisfying $\phi 1=I$ and

$$\begin{aligned}\phi(a+b)&=\phi a+\phi b\\ \phi(ab)&=(\phi a)(\phi b)\\ \phi(\lambda a)&=\lambda(\phi a)\end{aligned}$$

for all a, $b\in A$ and $\lambda\in F$.

The connection all this has with the representation theory of groups is provided by the following easy proposition.

Proposition. *If $\phi\colon FG\to Mat_d(F)$ is a representation of a group algebra FG then the restriction of ϕ to the basis G of FG gives a matrix representation of the group G. Conversely, if $\psi\colon G\to\mathrm{GL}(d,F)$ is a matrix representation of G then we can obtain a matrix representation of FG by extending the domain of definition of ψ to the whole of FG by the formula*

$$\psi\Big(\sum_{g\in G}\lambda_g g\Big)=\sum_{g\in G}\lambda_g(\psi g).$$

Thus, representations of G are essentially the same as representations of FG.