Algebras over a field

October 14, 2014

Roughly speaking, an algebra over a field F is just a ring R with F contained in the center of R. In particular R is an F-vector space, and this extra structure often simplifies life. For example, in the next installment we'll introduce modules over a ring R, and if R is an F-algebra then every R-module is also an F-vector space, a most pleasant state of affairs. This is the reason that I'm introducing F-algebras now rather than later. There is also a direct link to group theory, via the *group algebra* FG.

1 Definitions and examples

Let F be a field. An *F-algebra*, or *algebra over F*, is a ring R together with ring homomorphism $\eta : F \longrightarrow R$ such that $\eta(F)$ is contained in the center of R. As long as R is not the zero ring, η is automatically injective. Often η is just an inclusion, but the specific η is still part of the data. Examples:

- the polynomial ring $F[x]$, with $F \subset F[x]$ as the constant polynomials.
- the matrix ring M_nF with $F \subset M_nF$ as the scalar matrices $a \cdot Id$, $a \in F$. Or in coordinate-free terms, End_FV for a vector space V.
- The quaternions $\mathbb{H}$ form an $\mathbb{R}$-algebra, with $\mathbb{R} \subset \mathbb{H}$ as usual. Note that also $\mathbb{C} \subset \mathbb{H}$, but $\mathbb{C}$ is not contained in the center ($=\mathbb{R}$) and hence $\mathbb{H}$ is not a $\mathbb{C}$-algebra.
- If D is a division ring containing F in its center, then M_nD is an F-algebra, with $\eta : F \subset M_nD$ the scalar matrices with entries in F.

One reason to consider F-algebras is simply the utility of the extra structure. An F-algebra R is in particular an F-vector space, which means we can often use dimension-counting arguments. We can also generate R more efficiently. Consider, for example $\mathbb{C}[x]$. To generate it as a ring, we would need an uncountable number of generators (for by a straightforward argument, any countably generated commutative ring is countable). But as an F-algebra it is generated by one element, namely x.[1]

[1] We leave it to the reader to supply the definition of (a) F-subalgebra, and (b) F-subalgebra generated by a subset X.

A *homomorphism of F-algebras* $\phi : (R_1, \eta_1) \longrightarrow (R_2, \eta_2)$ is a ring homomorphism such that $\phi \circ \eta_1 = \eta_2$. With this definition we have a category $F - alg$ of F-algebras. There are simple examples of ring homomorphisms of F-algebras that are not F-algebra homomorphisms. Indeed F itself is an F-algebra with $\eta = Id$, and hence the only F-algebra automorphism of F is the identity. So for example complex conjugation $\mathbb{C} \longrightarrow \mathbb{C}$ is a ring homomorphism but not a $\mathbb{C}$-algebra homomorphism (although it *is* an $\mathbb{R}$-algebra homomorphism).

An *ideal* (left, right, or two-sided) in an F-algebra R is just an ideal I of the ring R; note that I is automatically a vector subspace. The quotient ring R/I then has a unique F-algebra structure such that the quotient homomorphism $R \longrightarrow R/I$ is an F-algebra homomorphism.

Example. Take $R = F[x]$ and I the ideal generated by x^n. Then $F[x]/(x^n)$ is a finite-dimensional F-algebra called a *truncated polynomial algebra*.

Example. Let $\mathfrak{b}_n F$ denote the ring of all upper triangular $n \times n$-matrices, and let $\mathfrak{u}_n F \subset \mathfrak{b}_n F$ consist of the matrices with all diagonal entries equal to 0. Then $\mathfrak{b}_n F$ is an F-subalgebra of $M_n F$, and $\mathfrak{u}_n F$ is a 2-sided ideal in $\mathfrak{b}_n F$. The quotient algebra $\mathfrak{b}_n F / \mathfrak{u}_n F$ is isomorphic to the product algebra F^n.

Example: product algebras. Suppose $R_1 R_2$ are F-algebras, with associated homomorphisms $\eta_i : F \longrightarrow R_i$. In particular they are rings, and we may form the product ring $R_1 \times R_2$ in the usual way, with coordinate-wise addition and multiplication. In fact $R_1 \times R_2$ is an F-algebra, where $\eta = (\eta_1, \eta_2) : F \longrightarrow R_1 \times R_2$. This is the categorical product; in other words, it has and is characterized by the universal property: Given an F-algebra R and F-algebra homomorphisms $\phi_i : R \longrightarrow R_i$ for $i = 1, 2$, there is a unique F-algebra homomorphism $\phi : R \longrightarrow R_1 \times R_2$ such that $\pi_i \phi = \phi_i$.

Similarly we may form the product of any indexed collection of F-algebras, although we are mainly interested in finite products $R_1 \times ... \times R_n$. This is a good place to point out that for rings in general the projection maps $\pi_j : \prod_{i=1}^n R_i \longrightarrow R_j$ are ring homomorphisms, but the inclusion of a factor $\iota_j : R_j \longrightarrow \prod_{i=1}^n R_i$ is *not* a ring homomorphism, since it doesn't preserve identities ($\iota_j(1) = (0, ..., 1, ...0)$, where the 1 is in the j-th position). The same remark applies to F-algebras.

2 Group algebras

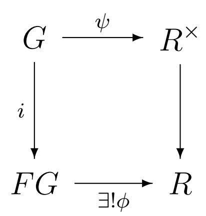
We next turn to one of the most important examples, namely group algebras. Let G be any group. Then for any field F we define the *group algebra* FG as follows: Form the vector space FG with basis G. Temporarily let $[g]$ denote the element $g \in G$ regarded as a basis vector in FG. Thus the elements of FG are formal sums $\sum_{g \in G} a_g [g]$, with $a_g \in F$ and $a_g = 0$ for all but finitely many g. We define a multiplication in FG by setting $[g] \cdot [h] = [gh]$ and extending to all of FG by linearity and the distributive law. Finally, define $\eta : F \longrightarrow FG$ by $\eta(a) = a[e]$, where $e \in G$ is the identity. When no confusion can result, we drop the brackets and simply write g in place of $[g]$, and 1 in place of $[e]$.

Note that $G \mapsto FG$ defines a functor $Grp \longrightarrow F - alg$: If $\phi : G \longrightarrow H$ is a group homomorphism, we extend ϕ linearly to get $F\phi : FG \longrightarrow FH$; it is readily verified that $F\phi$ is an

F-algebra homomorphism (and trivial that the conditions for a functor are satisfied). For example, any group admits a unique homomorphism to the trivial group; applying our functor yields a natural F-algebra homomorphism $\epsilon : FG \longrightarrow F$, which we call the *augmentation*. Explicitly, $\epsilon(\sum a_g g) = \sum a_g$.

Group algebras have a handy universal property. Note that the inclusion $i : G \subset FG$ satisfies $i(G) \subset (FG)^\times$, and hence if $\phi : FG \longrightarrow R$ is an F-algebra homomorphism, ϕ restricts to a group homomorphism $G \longrightarrow R^\times$.

Proposition 2.1 *Let R be an F-algebra. If $\psi : G \longrightarrow R^\times$ is a group homomorphism, there is a unique F-algebra homomorphism $\phi : FG \longrightarrow R$ whose restriction to G is ψ. Diagramatically:*



(The right vertical arrow is just inclusion.)

Proof: It is clear that there is a unique F-linear map ϕ that commutes in the diagram, since G is a basis for FG: $\phi(\sum a_g g) = \sum a_g \psi(g)$. Since ψ is a group homomorphism, it follows immediately that ϕ is an F-algebra homomorphism.

As is our custom, we will reformulate this proposition in two ways:

Plain English version: If you want to define an F-algebra homomorphism $FG \longrightarrow R$, it is enough (indeed equivalent) to define a group homomorphism $G \longrightarrow R^\times$.

Adjoint functor version: For a given field F, the group algebra functor $G \mapsto FG$ is left adjoint to the group of units functor $R \longrightarrow R^\times$. That is, there is a natural bijection

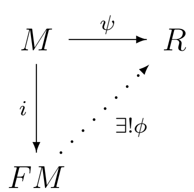
$$Hom_{F-alg}(FG, R) \cong Hom_{grp}(G, R^\times).$$

The universal property yields a third way to think about representations. Recall that we defined a representation of G over F as a linear action of G on an F-vector space V, and then observed that this is the same thing as a group homomorphism $G \longrightarrow GL(V)$. Since $GL(V)$ is the group of units of the F-algebra $End_F V$, we can think of a representation as an F-algebra homomorphism $FG \longrightarrow End_F V$. If $dim_F V = n$, we can choose a basis to get a homomorphism $FG \longrightarrow M_n F$.

In particular, one-dimensional representations correspond to (i) group homomorphisms $\chi : G \longrightarrow F^\times$ and (ii) F-algebra homomorphisms $\xi : FG \longrightarrow F$. The group homomorphisms χ are often called "characters" in the literature. Note that since $F^\times$ is abelian, χ factors uniquely through G_{ab} and ξ factors uniquely through $F(G_{ab})$.

3 Monoid algebras, polynomial algebras and Laurent polynomial algebras

Note that the definition of the group algebra makes no use of inverses. Thus if M is a monoid, we can define the *monoid algebra* FM in exactly the same way. The monoid ring has a universal property analogous to that of a group ring. The difference is that now we only need a monoid homomorphism $M \longrightarrow R$, where R is a monoid under multiplication. Thus the commutative diagram in Proposition 2.1 can be written as a triangle (in fact we could have done this for group algebras too)



Here ψ is a monoid homomorphism and ϕ is an F-algebra homomorphism. Although we won't make much use of this more general construction, there is at least one case worth knowing. Let N_1 denote the monoid $\mathbb{Z}_{\geq 0}$ of non-negative integers, written multiplicatively: the identity is 1, the (unique) generator is x and $N_1 = \{x^n : n \geq 0\}$. Then FN_1 is none other than the polynomial ring $F[x]$, and indeed this is really the *definition* of $F[x]$. The polynomial ring has the following universal property:

Proposition 3.1 *Let R be an F-algebra. Then for every $y \in R$ there is a unique F-algebra homomorphism $\phi : F[x] \longrightarrow R$ such that $\phi[x] = y$.*

Proof: Version 1: $F[x]$ has F-basis x^i, $i \geq 0$. So there is a unique F-linear map $\phi : F[x] \longrightarrow R$ such that $\phi(x^i) = y^i$ for all i. This map is the desired F-algebra homomorphism, as one can readily check.

Version 2 (which shows what you're really doing): Note that N_1 has a universal property among all monoids: Given any monoid M and any $y \in M$, there is a unique monoid homomorphism $\lambda : N_1 \longrightarrow M$ such that $\lambda(x) = y$. Applying the universal property of monoid rings to λ yields the desired ϕ.

More generally we could take $N_n = (\mathbb{Z}_{\geq 0})^n$. Writing $x_1, ..., x_n$ for the evident generators of N_n, we see that FN_n is none other than the multi-variable polynomial ring $F[x_1, ..., x_n]$, and once again this is really the *definition* of $F[x_1, ..., x_n]$ (even in undergraduate texts, although the word "monoid" might not be explicitly mentioned). More generally still, one can define a polynomial ring in any infinite set of variables as a suitable monoid ring, but we will stick to the finite case for now.

Polynomial rings in more than one variable also have a universal property, but only in the category of *commutative* F-algebras:

Proposition 3.2 *Let R be a commutative F-algebra, and let $y_1, ..., y_n \in R$. Then there is a unique F-algebra homomorphism $\phi : F[x_1, ..., x_n] \longrightarrow R$ such that $\phi(x_i) = y_i$.*

Proof: It is clear that N_n itself has a universal property among *abelian* monoids: Given an abelian monoid M for any $y_1, ..., y_n \in M$, there is a unique monoid homomorphism $\lambda : N_n \longrightarrow M$ such that $\lambda(x_i) = y_i$ (namely, $\lambda(x_1^{i_1}...x_n^{i_n}) = y_1^{i_1}...y_n^{i_n}$). Take $M = R$ under multiplication and apply the universal property of monoid algebras. (Or if you prefer, rewrite this argument without ever mentioning monoids.)

Remark: We've deliberately omitted the diagrammatic and adjoint functor versions of these universal properties, as the set-up is so simple as it stands. A more systematic adjoint functor treatment should and will await the more "coordinate-free" version of polynomial algebras we'll encounter later.

Finally, the *Laurent polynomial algebra* $F[x_1, x_1^{-1}, ..., x_n, x_n^{-1}]$ is obtained from the ordinary polynomial algebra by "formally adjoining inverses" of the x_i's. In our present context it is no work at all to make this precise: The Laurent polynomial algebra is just the group algebra $F\mathbb{Z}^n$, where of course $\mathbb{Z}$ has to be written multiplicatively. The monoid inclusion $N_n \subset \mathbb{Z}^n$ then induces a map of monoid algebras that is just the inclusion $F[x_1, ..., x_n] \subset F[x_1, x_1^{-1}, ..., x_n, x_n^{-1}]$. The Laurent polynomials in one (resp. more than one) variable have a universal property identical to that of ordinary polynomials in one (resp. more than one) variable, except that the elements y (resp. y_i) must be taken to be units in R.

4 Algebras over a commutative ring

Our definition of F-algebra only used the fact that F is commutative, not that F is a field. Hence for any commutative ring S we define an S-algebra to be a ring R equipped with a ring homomorphism $\eta : S \longrightarrow R$ whose image is contained in the center of R. For example, the polynomial ring $S[x]$ and the matrix ring $M_n S$ are S-algebras. The group algebra SG can be defined similarly to FG, but we will wait for the chapter on modules before elaborating on this case.

The one new phenomenon to note is that η need not be injective. For example, if R is commutative then any quotient ring R/I is an R-algebra, with $\eta : R \longrightarrow R/I$ the quotient homomorphism. Note also that every ring R has a unique $\mathbb{Z}$-algebra structure, given by the unique ring homomorphism $\eta : \mathbb{Z} \longrightarrow R$.

5 Exercises

The point of these exercises is to get used to computing in a group algebra, and at the same time prove some very useful formulas, as well as an interesting theorem 3b.

Let G be a finite group, F a field. For any subset $S \subset G$, we let $\overline{S} = \sum_{g \in S} g \in FG$.

1. Let C be a conjugacy class in G. Show that the elements $\overline{C}$, C ranging over all conjugacy classes, form a basis for the center of FG. (Recall that the center $C(R)$ of a ring R is exactly analogous to the center of a group: $C(R) = \{x \in R : rx = xr \, \forall \, r \in R\}$. It is a subring of R, and in the case of an F-algebra it is a subalgebra.)

2. *Idempotents.* First some definitions: An element of a ring satisfying $e^2 = e$ is called an *idempotent*. Any ring has the idempotents 0 and 1, and in a field or division ring these are the only idempotents (why?). On the other hand, a product ring $R_1 \times R_2$ has also the idempotents $e_1 = (1, 0)$ and $e_2 = (0, 1)$. A *central idempotent* is an idempotent $e \in C(R)$. Idempotents e_1, e_2 are *orthogonal* if $e_1 e_2 = 0 = e_2 e_1$. In the product ring example, e_1, e_2 are central orthogonal idempotents.

NOTICE: From here on we assume *char* F doesn't divide $|G|$, so that $|G|^{-1} \in F$. This is a fundamental dichotomy in the subject; the so-called "modular" case when *char* $F = p$ for a prime p dividing $|G|$ is much harder.

a) Set $e_0 = \frac{1}{|G|}\overline{G}$. Then e_0 is a central idempotent in FG (known as the "averaging operator").

Note: If you prefer, you could go straight to part (b), which is more general. But I do recommend (a) as a warm-up and as the most important case.

b) Let $\chi : G \longrightarrow F^\times$ be a group homomorphism, and set

$$e_\chi = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1}) g.$$

Show that $h e_\chi = \chi(h) e_\chi$ for all $h \in G$, and that e_χ is a central idempotent. (Note that e_0 in part (a) is the special case when χ is the trivial homomorphism.)

c) Suppose $\chi, \psi : G \longrightarrow F^\times$ are distinct homomorphisms. Show that e_χ, e_ψ are orthogonal.

Suggestion: Don't expand out the sums all over again. Make use of formulas you already have to keep it clean and simple.

d) In any F-algebra R, any set of pairwise orthogonal nonzero idempotents $e_1, ..., e_m$ is linearly independent over F. In particular this is true for the idempotents of part (c).

3. Let G be a finite *abelian* group. In this exercise you may assume the following fact (we, meaning you, will prove it later after we've done the classification of finite abelian groups): $Hom_{grp}(G, \mathbb{C}^\times) \cong G$ as groups. All you actually need below is that the orders are the same.

a) Conclude from the "fact" that the idempotents e_χ form a $\mathbb{C}$-basis for $\mathbb{C}G$, where χ ranges over $Hom\,(G, \mathbb{C}^\times)$.

b) Show that $\mathbb{C}G \cong \mathbb{C}^n$ as $\mathbb{C}$-algebras, where $n = |G|$ and $\mathbb{C}^n$ is the n-fold product of copies of $\mathbb{C}$.

This is an especially important exercise because part (b) is the prototype of a vastly more general result, to be considered later, that will be a cornerstone of the representation theory of finite groups.

4. This exercise gives a first illustration of how the "modular" case differs from the non-modular case.

Suppose *char* $F = p$, and let G be cyclic of order p^n. Show that FG is isomorphic as an F-algebra to the truncated polynomial algebra $F[x]/x^{p^n}$.

(This should be contrasted with the previous problem, where $\mathbb{C}G$ is a product of copies of $\mathbb{C}$. Note that a product of fields has no nilpotent elements.)