2.11 Algebras

Let A be a ring.

Suppose that B is both a ring and an A-module where the ring and module additions coincide.

Denote ring multiplication (whether in B or in A) by juxtaposition, and **scalar multiplication** by elements of A by $\cdot$

(in practice both denoted by juxtaposition).

Call B an A-**algebra** or **algebra** (**over** A) if

$$(\forall a \in A)\ (\forall b, c \in B)$$

$$a \cdot (b\,c) \;=\; (a \cdot b)\,c \qquad \left[=\; b\,(a \cdot c) \right]$$

↑ needed in the noncommutative case

Suppose B is an A-algebra.

Define $f : A \longrightarrow B$ by

$$f(a) = a \cdot 1 \qquad (a \in A)$$

↑ ring identity element of B

Then, for all $a_1, a_2 \in A$,

$$\begin{aligned} f(a_1 + a_2) &= (a_1 + a_2) \cdot 1 \\ &= a_1 \cdot 1 + a_2 \cdot 1 = f(a_1) + f(a_2) \end{aligned}$$

and

$$
\begin{aligned}
f(a_1 a_2) &= (a_1 a_2) \cdot 1 = a_1 \cdot (a_2 \cdot 1) \\
&= a_1 \cdot \big(a_2 \cdot (1\,1)\big) = a_1 \cdot (1(a_2 \cdot 1)) \\
&= (a_1 \cdot 1)(a_2 \cdot 1) = f(a_1)\, f(a_2) \; ,
\end{aligned}
$$

which proves f is a **ring** homomorphism.

Conversely, let $f : A \to B$ be a ring homomorphism.

Then (by restriction of scalars) B becomes an A-module by defining

$$a \cdot b \;=\; f(a)\, b \qquad\qquad (a \in A,\ b \in B)\ .$$

Further this turns B into an A-algebra, because

$$(\forall a \in A)\ (\forall b, c \in B)$$

$$a \cdot (bc) \;=\; f(a)(bc) \;=\; (f(a)b)c \;=\; (a \cdot b)c\ .$$

Moreover, these processes, turning an A-algebra into a ring homomorphism, and vice-versa, undo each other, so

> A-algebras B correspond to pairs consisting of a ring B and a ring homomorphism
>
> $$f : A \to B .$$

Remarks:

(1) In particular if $A = F$ is a field and $f : A \to B$ is not the zero homomorphism, then f is injective (an early Proposition), so F can be identified with its image under f :

$$(\forall a \in F) \qquad a \equiv a \cdot 1 \, .$$

Thus

a nonzero F-algebra may be thought of as a ring containing F as a subring.

(2) If A is any nonzero ring then

$$f : \mathbb{Z} \longrightarrow A \qquad \text{where} \qquad f(n) \;=\; n\,1$$

is easily seen to be a ring homomorphism, so A becomes a $\mathbb{Z}$-algebra.

Observe that

$$\ker f \;=\; k\mathbb{Z} \qquad \exists\, k \geq 0 \; .$$

But A is nonzero, so $k \neq 1$. We call k the **characteristic** of A .

We can identify

$$\mathbb{Z}_k \quad (= \mathbb{Z} \text{ if } k = 0\,)$$

with the subring of A generated by 1, called the **prime subring** of A (though it may have nothing to do with primes!).

$\Big[$ If A is a field then all nonzero elements are invertible, so the prime subring must be a copy of $\mathbb{Z}$ or a copy of $\mathbb{Z}_p$ for some prime p. $\Big]$

Algebra homomorphisms:

Let $f : A \to B$ and $g : A \to C$ be ring homomorphisms, so that

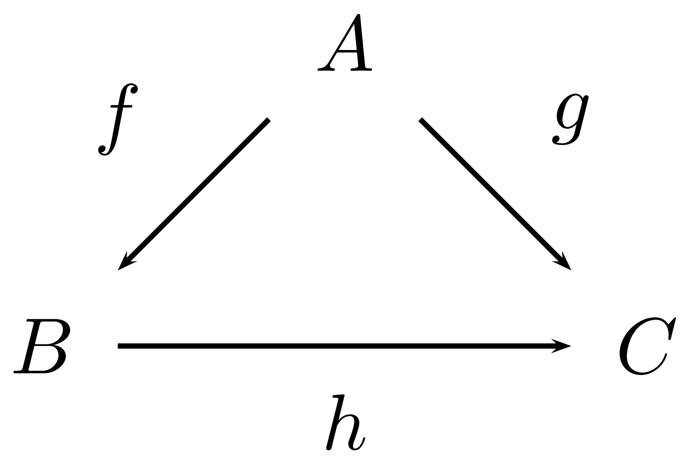
B , C become A-algebras.

Consider a ring homomorphism $h : B \to C$.

Call h an A-**algebra homomorphism** if h respects scalar multiplication, that is,

$$(\forall a \in A)(\forall b \in B) \qquad h(a \cdot b) \;=\; a \cdot h(b) \; .$$

Observation: h is an A-algebra homomorphism iff the following diagram commutes:



Proof: $(\Longrightarrow)$ If h is an A-algebra homomorphism then

$$(\forall a \in A)(\forall b \in B) \qquad h\,(f(a)\,b) \;=\; g(a)\,h(b)\;,$$

so, in particular, taking $b = 1$,

$$(\forall a \in A) \qquad h\,(f(a)) = g(a)\ ,$$

that is, $h \circ f = g$.

$(\Longleftarrow)$ If $h \circ f = g$ then, for all $a \in A$, $b \in B$

$$h(a \cdot b) = h\big(f(a)\,b\big) = h\big(f(a)\big)\,h(b)$$

$$= g(a)\,h(b) = a \cdot h(b)\ ,$$

so h is an A-algebra homomorphism.

The polynomial ring $A[t_1, \ldots, t_n]$ in n commuting indeterminates is called the **free** A-**algebra** on n generators because of the following:

Property: $A[t_1, \ldots, t_n]$ is an A-algebra such that if B is any A-algebra and $b_1, \ldots, b_n \in B$ then the map

$$t_i \mapsto b_i \qquad \forall i$$

extends uniquely to an A-algebra homomorphism: $A[t_1, \ldots, t_n] \to B$.

If $p(t_1, \ldots, t_n) \in A[t_1, \ldots, t_n]$ then this homomorphism is just the **evaluation** mapping

$$p(t_1, \ldots, t_n) \mapsto p(b_1, \ldots, b_n) \ .$$

Evaluation is **onto** precisely when $b_1, \ldots, b_n$ generate B as an A-algebra, in which case we say that B is **finitely generated**.

Note: a ring is finitely generated as a ring iff it is finitely generated as a $\mathbb{Z}$-algebra.

Tensor product of algebras:

Let B , C be A-algebras via ring homomorphisms

$$f : A \to B \quad , \quad g : A \to C .$$

In particular, ignoring their ring multiplication, B and C become A-modules, so we may form the A-module

$$D = B \otimes_A C .$$

We shall define multiplication on D making D into a ring and an A-algebra.

The mapping

$$\phi \;:\; B \times C \times B \times C \;\longrightarrow\; B \otimes C$$

where

$$(b, c, b', c') \;\mapsto\; bb' \otimes cc' \qquad\qquad (b, b' \in B \;,\; c, c \in C)$$

is easily checked to be multilinear.

Thus there is a unique A-module homomorphism ψ which makes the following diagram commute:

$$\begin{array}{ccc} B \times C \times B \times C & \longrightarrow & B \otimes C \otimes B \otimes C \\ & \phi \searrow \quad \swarrow \psi & \\ & B \otimes C & \end{array}$$

Also (**exercise**), there is a "canonical isomorphism"

$$\theta : (B \otimes C) \otimes (B \otimes C) \ \rightarrow \ B \otimes C \otimes B \otimes C$$

extending the following map on generators:

$$(b \otimes c) \otimes (b' \otimes c') \ \mapsto \ b \otimes c \otimes b' \otimes c' \ .$$

Let

$$g : (B \otimes C) \times (B \otimes C) \;\longrightarrow\; (B \otimes C) \otimes (B \otimes C)$$

where

$$(\alpha, \beta) \;\mapsto\; \alpha \otimes \beta \qquad\qquad (\alpha, \beta \in B \otimes C) \;,$$

which is clearly bilinear.

Put

$$\mu \;\;=\;\; \psi \circ \theta \circ g$$

so that the following diagram commutes:

$$
\begin{array}{ccc}
D \times D \ = & & \\
(B \otimes C) \times (B \otimes C) & \xrightarrow{\quad g \quad} & (B \otimes C) \otimes (B \otimes C) \\
 & & \downarrow \theta \\
 & \mu \searrow & B \otimes C \otimes B \otimes C \\
 & & \downarrow \psi \\
 & & B \otimes C \ = \ D
\end{array}
$$

Further μ is bilinear (being the composite of a bilinear map with linear maps).

For $b, b' \in B$, $c, c' \in C$,

$$\mu(b \otimes c\ ,\ b' \otimes c') \;\; = \;\; \psi\Big(\theta\big(g(b \otimes c, b \otimes c')\big)\Big)$$

$$= \;\; \psi\Big(\theta\big((b \otimes c) \otimes (b' \otimes c')\big)\Big)$$

$$= \;\; \psi\big(b \otimes c \otimes b' \otimes c'\big) \;\; = \;\; \phi(b, c, b', c') \;\; = \;\; (bb') \otimes (cc') \ .$$

The bilinearity of μ gives

$$\mu\left(\sum_i (b_i \otimes c_i)\ ,\ \sum_j (b'_j \otimes c'_j)\right)$$

$$= \sum_{i,j} b_i b'_j \otimes c_i c'_j \ .$$

It is easy now to check that μ defines a multiplication on $D = B \otimes C$ making D into a ring with identity element $1 \otimes 1$. Using juxtaposition, the rule for multiplication is simply

$$\left(\sum_i (b_i \otimes c_i) \right) \left(\sum_i (b'_j \otimes c'_j) \right)$$

$$= \sum_{i,j} b_i b'_j \otimes c_i c'_j \, .$$

Define $h : A \longrightarrow D$ by, for $a \in A$

$$\begin{aligned} h(a) &= a \cdot (1 \otimes 1) \\ &= (a \cdot 1) \otimes 1 \;=\; 1 \otimes (a \cdot 1) \\ &= f(a) \otimes 1 \;=\; 1 \otimes g(a) \; . \end{aligned}$$

Clearly h preserves addition and maps 1 to $1 \otimes 1$.

Further, h preserves multiplication, because, for $a_1, a_2 \in A$,

$$h(a_1 a_2) \;=\; f(a_1 a_2) \otimes 1 \;=\; \Big(f(a_1) f(a_2) \otimes (1\ 1) \Big)$$

$$=\; \Big(f(a_1) \otimes 1 \Big) \Big(f(a_2) \otimes 1 \Big) \;=\; h(a_1) h(a_2) \ .$$

Thus h is a ring homomorphism, with respect to which D becomes an A-algebra.

In summary, given A-algebras B and C :

> The A-module $B \otimes_A C$ becomes an A-algebra with multiplication which extends the following multiplication on generators:
>
> $$(b \otimes c)(b' \otimes c) \quad = \quad bb' \otimes cc'$$
>
> for $b, b' \in B$ and $c, c' \in C$.