Lectures on semisimple rings and representation theory — preliminary draft

Pedro Resende

November 25, 2024

Abstract

Support notes for the MMAC course "Modules and Representations" of IST in the academic year 2024/2025. Each of the following "lectures" corresponds to a 50 minute session.

Contents

0 Introduction

These notes are meant to provide an introduction to representation theory, in particular of finite groups, via the notion of semisimple ring and the theorem of Artin–Wedderburn. For further reading see [?DF, ?Beachy, ?Lang].

All the rings and ring homomorphisms in these notes are assumed to be unital.

1 Lecture 1 — More on injective modules

When we studied projective modules we saw that one of the equivalent conditions for a module P to be projective is that every epimorphism $\varphi : M \to P$ is a retraction. There is an analogous condition for injective modules which we did not address, so let us do it now.

First we need a simple condition regarding pushouts of modules (for an arbitrary ring R), where by a *pushout square* in any category C is meant the same as a pullback square in C^{op}. Let A, B and C be R-modules, with homomorphisms as follows:

$$\begin{array}{ccc} C & \xrightarrow{f} & A \\ {\scriptstyle g}\big\downarrow & & \\ B & & \end{array}$$

Let $K \subset A \oplus B$ consist of all the pairs $(f(c), -g(c))$ with $c \in C$. By an easy application of the submodule criterium we see that K is a submodule of $A \oplus B$. Let $P = (A \oplus B)/K$ (this means that all the pairs $(f(c), 0)$ and $(0, g(c))$ are identified in the quotient), and let $q : A \oplus B \to P$ the quotient homomorphism. Letting $\iota_1 : A \to A \oplus B$ and $\iota_2 : B \to A \oplus B$ be the canonical injections, we obtain a commutative square which is easily seen to be a pushout square (exercise!):

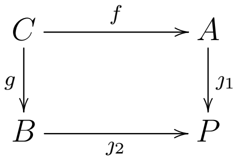
$$\begin{array}{ccc} C & \xrightarrow{f} & A \\ {\scriptstyle g}\big\downarrow & & \big\downarrow{\scriptstyle \jmath_1 := q\iota_1} \\ B & \xrightarrow[\jmath_2 := q\iota_2]{} & P \end{array}$$

(As always for universal properties, any other pushout of f and g is isomorphic to P.)

You may recall that, in any category, pullbacks are well behaved with respect to monomorphisms in the sense that the pullback of a monomorphism is itself a monomorphism. Dually, any pushout (also called a pushforward) of an epimorphism is itself an epimorphism. This holds for arbitrary categories. But for the category of R-modules we have an additional fact:

§1. LEMMA. *Any pushout of a monomorphism of R-modules is itself a monomorphism of R-modules.*

Proof. Let the following be a pushout square of R-modules:

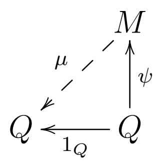


Let us assume concretely, as above, that $P = (A \oplus B)/K$ and $\jmath_i = q\iota_i$. The statement of the lemma means that if f is a monomorphism then so is $\jmath_2$ (and that if g is a monomorphism so is $\jmath_1$). So let us assume that f is a monomorphism, and let $b \in \ker \jmath_2$. This means that $(0, b) = \iota_2(b) \in K$, so there must be $c \in C$ such that $(0, b) = (f(c), -g(c))$. Since f is mono, this means that $c = 0$, so $b = g(c) = 0$, and we conclude that $\ker \jmath_2 = 0$. ∎

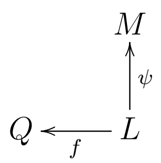
§2. THEOREM. *The following conditions are equivalent, for any R-module Q:*

1. *Q is injective.*
2. *Every monomomorphism $\psi : Q \to M$ is a section.*

Proof. The condition $1 \Rightarrow 2$ is an easy exercise, for if Q is injective and $\psi : Q \to M$ is mono then there exists a lifting μ of 1_Q as in the following diagram — the lifting is the required retraction of ψ:



Now let us prove $2 \Rightarrow 1$. Assume that every monomorphism $\jmath : Q \to P$ is a section, and consider the following diagram of R-modules, where $\psi : L \to M$ is a monomorphism:



In order to show that Q is injective we will obtain a lifting F of f. Consider the pushout of f and ψ:

$$\begin{array}{ccc} P & \xleftarrow{\jmath_1} & M \\ {\scriptstyle \jmath_2}\uparrow & & \uparrow{\scriptstyle \psi} \\ Q & \xleftarrow[f]{} & L \end{array}$$

Since, by §1, $\jmath_2$ is a monomorphism, by hypothesis it has a retraction $\mu : P \to Q$, so making $F = \mu\jmath_1$ we obtain the envisaged lifting of f:

$$F\psi = \mu\jmath_1\psi = \mu\jmath_2 f = f. \quad \blacksquare$$

t This characterization of injective modules leads to a surprising fact that relates injective to projective modules. Although injective modules are certainly not the same as projective modules (for instance, $\mathbb{Z}$ is a projective $\mathbb{Z}$-module but it is not injective, whereas $\mathbb{Q}$ is injective but not projective — check this as an exercise), the following property holds for any ring R:

§3. Corollary. *The following properties are equivalent:*

1. *All R-modules are injective.*
2. *All R-modules are projective.*
3. *Every short exact sequence of R-modules splits.*

Proof. Exercise. $\blacksquare$

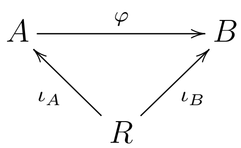
2 Lecture 2

2.1 Associative algebras

Here we recall the notion of *algebra* over a commutative ring, often termed *associative algebra* in order to distinguish it from other types of algebras, such as Lie algebras. Whenever we say only "algebra" we will be referring to associative algebras.

§4. Definition. Let R be a commutative ring. By an *R-algebra* is meant a ring A together with a ring homomorphism $\iota : R \to A$, called the *injection of scalars*, whose image is in the center of A.

§5. Definition. Given two R-algebras $A \equiv (A, \iota_A)$ and $B \equiv (B, \iota_B)$, a *homomorphism* of R-algebras $\varphi : A \to B$ is a (necessarily unital) homomorphism of rings for which the following diagram commutes (i.e., φ preserves the scalars):



(1)

This defines the category of R-algebras, which we denote by *R-Alg*.

§6. Examples. Let R be a commutative ring.

1. $M_n(R)$ is an R-algebra with injection of scalars $\iota : R \to M_n(R)$ given by $r \mapsto rI$ where I is the identity matrix.
2. $R[x]$ is an R-algebra with injection of scalars $\iota : R \to R[x]$ yielding the polynomial r of degree zero for each $r \in R$.

Note that in these two cases the injection of scalars is injective. In fact in the second example we always regard R concretely as a subring of $R[x]$. See appendix **??** for a brief account of the universal property of $R[x]$ and a consequence of it which has already been exploited in our study of Jordan canonical forms.

§7. Notation. Any R-algebra A with injection of scalars ι has a structure of R-module whose action $\cdot : R \times A \to A$ is given, for each $r \in R$ and $a \in A$, by $r \cdot a = \iota(r)a$. Usually we shall just write ra if no confusion may arise. In particular, if R is a field then A is a vector space over R, whose multiplication by scalars is given by the action.

§8. Exercise. Prove that a homomorphism φ of R-algebras is the same as a ring homomorphism which is equivariant with respect to the action; that is, such that for all $r \in R$ and $a \in A$,

$$\varphi(ra) = r\varphi(a).$$

§9. Exercise. Show that for all $r \in R$ and $a, b \in A$ the action satisfies the following additional conditions:

$$\begin{aligned} r(ab) &= (ra)b \\ r(ab) &= a(rb). \end{aligned}$$

§10. Exercise. Show that an R-algebra is the same thing as a ring A which is also an R-module such that the two conditions in the previous exercise hold. (Hint: define $\iota(r) = r1_A$.)

§11. Exercise. Let R be a commutative ring, and M an R-module. Show that $\mathrm{End}_R(M)$ is an R-algebra. (Hint: define the action of $r \in R$ on $f \in \mathrm{End}_R(M)$ by $(rf)(m) = rf(m)$.)

§12. Nonunital algebras. The definition of an R-algebra and of R-algebra homomorphisms in terms of the action of R makes sense even if A does not have a unit. In that case the injection of scalars is not well defined, but we still have a working definition of R-algebra in terms of the action. This is the case when we define the R-algebra of an arbitrary small category, or of a general quiver (see below) because, as we shall see, the algebra we obtain is unital only when the object set of the category is finite (resp., the vertex set of the quiver is finite).

2.2 Group algebras and representations

Now let us take advantage of the fact that the students of this course already know the example of a group ring, at least for finite groups, in order to give the first example of how representations of finite groups relate to representations of an algebra. In what follows, given a ring R and a finite set X, we denote the free R-module on X by RX, and will think of it concretely as consisting of the set of all the formal linear combinations

$$RX = \left\{ \sum_{x \in X} r_x \, x \mid r_x \in R \right\}.$$

§13. Proposition. *Let R be a commutative ring and G a finite group with unit 1_G. The free R-module RG is an R-algebra whose unit coincides with 1_G and whose multiplication is defined by bilinear extension of the multiplication of G:*

$$\left(\sum_{g \in G}^{n} r_g \, g \right) \left(\sum_{h \in G}^{n} s_h \, h \right) = \sum_{g,h \in G} r_g s_h \, gh.$$

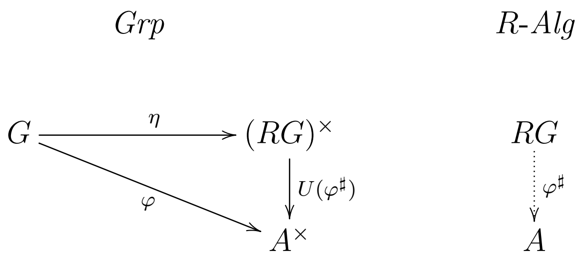
Proof. Straightforward. ∎

§14. Exercise. Let R be a commutative ring. Show that the mapping $A \mapsto A^\times$ yields a functor $U : R\text{-}Alg \mapsto Grp$.

§15. PROPOSITION. *Let R be a commutative ring with unit 1_R, G a finite group, and $\eta : G \to RG$ the mapping given by $g \mapsto 1_R\, g$. The pair (RG, η) is a universal arrow from G to the functor U.*

Proof. We need to show the following:

1. η defines a group homomorphism $G \to (RG)^\times$;
2. For any R-algebra A and any group homomorphism $\varphi : G \to A^\times$ there is a unique homomorphism of R-algebras $\varphi^\sharp : RG \to A$ whose restriction to $(RG)^\times$ makes the diagram on the left commute:



The fact that η is a homomorphism of groups is immediate. For the second condition let $G = \{g_1, \dots, g_n\}$. We define $\varphi^\sharp$ by

$$\varphi^\sharp(r_1 g_1 + \cdots + r_n g_n) = r_1\varphi(g_1) + \cdots + r_n\varphi(g_n).$$

The rest of the proof is left as an exercise: show that $\varphi^\sharp$ is a homomorphism of R-algebras, and that any other homomorphism of R-algebras $\psi : RG \to A$ such that $U(\psi) \circ \eta = \varphi$ must coincide with $\varphi^\sharp$. ∎

§16. DEFINITION. Let F be a field, and $n \in \mathbb{N}$. A *matrix representation of degree n over F* of a group G is a homomorphism of groups

$$\rho : G \to GL_n(F).$$

Similarly, a *matrix representation of degree n* of an F-algebra A is a homomorphism of F-algebras

$$\pi : A \to M_n(F).$$

Since $M_n(F)^\times = GL_n(F)$, the restriction $U(\pi)$ is a matrix representation over F of degree n of the group $A^\times$. Moreover, the universal property of §2.15 shows that there is a bijective correspondence between matrix representations

ρ over F of degree n of a finite group G and the matrix representations $\rho^\sharp$ of degree n of the group algebra FG:

$$\begin{array}{ccc} \mathit{Grp} & \qquad & F\text{-}\mathit{Alg} \\ & & \\ G & & FG \\ {\scriptstyle\rho}\downarrow & & \downarrow{\scriptstyle\rho^\sharp} \\ GL_n(F) & & M_n(F) \end{array}$$

§17. Exercise. Show that an entirely analogous construction of an R-algebra can be obtained from a finite monoid M, again by taking the multiplication of RM to be defined by bilinear extension of the multiplication of M. Show also that $\eta : M \to RM$, given by $m \mapsto 1_R\, m$, defines a universal arrow from M to the forgetful functor R-*Alg* $\to$ *Mon* where *Mon* is the category of monoids (for each R-algebra A the forgetful functor forgets the additive group structure and the injection of scalars of A, thus keeping only its multiplicative monoid structure).

3 Lecture 3 — Constructions of algebras

Throughout this lecture R is a commutative ring (with unit).

3.1 Endomorphisms and matrices

§18. Definition. Let V be an R-module. Then $\mathrm{End}_R(V)$ is an R-algebra with product given by composition and R-action defined by $(rf)(v) = r(f(v))$.

§19. Exercise. Prove that if V is a free R-module of rank $n > 1$ then $\mathrm{End}_R(V) \cong M_n(R)$.

3.2 Algebra of a small category

§20. Definition. Let C be a small category. Define the R-algebra RC to be $F_R(C_1)$ with multiplication defined by, for all $f, g \in RC$:

$$(f * g)(x) = \sum_{x=yz} f(y)g(z).$$

(This operation is called *convolution*.) Note that all the sums have only finitely many nonzero elements because the supports of f and g are finite.

§21. Exercise. Verify that RC is indeed an R-algebra, i.e., show that the multiplication is associative and R-bilinear as required, but that it may fail to be unital. Show that if C_0 is a finite set the algebra RC is unital with unit the function $1 : C_1 \to R$ defined by

$$1(x) = \begin{cases} 1 & \text{if } x \text{ is an identity arrow,} \\ 0 & \text{otherwise.} \end{cases}$$

Note: for associativity it may help to think of each $f \in RC$ as a formal linear combination $\sum_{x \in C_1} f(x)x$.

§22. Example. The algebra RG of a finite group is the algebra of G regarded as a category with only one object. More generally, the construction of the algebra of a category applies to infinite groups, and also to monoids, always yielding a unital algebra.

§23. Exercise. Prove that for a group G the ring RG has an *involution*, by which is meant an additive map $i : RG \to RG$ such that $i(i(f)) = f$ and $i(fg) = i(g)i(f)$ for all $f, g \in G$. Hint: define it by $i(f)(x) = f(x^{-1})$.

§24. Remark. For $R = \mathbb{C}$ the involution is usually defined by $i(f)(x) = \overline{f(x^{-1})}$, so it is an anti-linear map.

§25. Free algebras. Let X be a set, and X^* its free monoid. The *free R-algebra* generated by X is RX^*, usually denoted by $R\langle X\rangle$. If $|X| = n < \infty$ we write $R\langle x_1, \ldots, x_n\rangle$.

§26. Warning: Do not confuse $R\langle x_1, \ldots, x_n\rangle$ with the polynomial ring $R[x_1, \ldots, x_n]$ in n indeterminates. In particular, the latter is always commutative, whereas the former is not (unless $n = 1$, in which case $R[x] = R\langle x\rangle$).

§27. Exercise. Consider the forgetful functor $U : R\text{-}Alg \to Set$. Show that for every set X there is a universal arrow from X to U. Hint: for each set X consider the algebra $R\langle X\rangle$ and the function $\eta : X \to R\langle X\rangle$ given by $x \mapsto \delta_x$.

§28. Note: Often we shall identify elements generators x of a free module with the corresponding basis elements δ_x, for instance regarding the free monoid X^* as a subset of the algebra $R\langle X\rangle$. In particular, we think of elements $x_1, \ldots, x_n$ as belonging to the free algebra $R\langle x_1, \ldots, x_n\rangle$, just as we do for the polynomial algebra $R[x_1, \ldots, x_n]$.

3.3 Quivers

§29. Definition. A *quiver* is a directed graph $Q = (I, E)$ whose set of vertices is I and whose set of edges is E. A *homomorphism of quivers* is a homomorphism of directed graphs. Often the domain and the codomain of an edge h are denoted by d' and d'', respectively.

§30. Free category on a quiver. The free category on a quiver Q, denoted by Q^*, has objects the vertices of Q and edges the paths formed by concatenating edges of Q, including the empty paths, which are the units of the category.

§31. Exercise. Formulate and prove the universal property of the free category of a quiver.

§32. Definition. Let Q be a quiver. The R-algebra of Q, denoted by RQ, is the algebra of the free category of Q; that is, RQ is defined to be RQ^*.

3.4 Tensor algebras

§33. Definition. Let R be a commutative ring and V an R-module. The tensor algebra $T_R(V)$ is defined to be

$$T_R(V) = \bigoplus_{n=0}^{\infty} V^{\otimes n}.$$

with the required R-bilinear multiplication corresponding to the following homomorphism of R-modules,

$$T_R(V) \otimes_R T_R(V) \cong \bigoplus_{i,j=0}^{\infty} V^{\otimes i} \otimes_R V^{\otimes j} \to T_R(V)$$

which for each pair i, j is given by $V^{\otimes i} \otimes_R V^{\otimes j} \xrightarrow{\cong} V^{\otimes(i+j)} \to T_R(V)$.

§34. Exercise. Formulate and prove the universal property of the tensor algebra (adjunction between *R-Mod* and *R-Alg*). Note that the canonical map $V \to T_R(V)$ that sends V to the "degree 1 component" $V^{\otimes 1}$ is injective.

§35. Grading. The tensor algebra $T_F(L)$ is *graded* over the additive monoid $\mathbb{Z}_{\geq 0}$ in the sense that will be defined next:

§36. Definition. Let A be an R-algebra, and S a semigroup. A *grading* of A over S is a direct decomposition $A = \bigoplus_{s\in S} A_s$ into R-submodules A_s such that for all $a \in A_s$ and $b \in A_t$ we have $ab \in A_{st}$.

3.5 Quotients of algebras

§37. Definition. Let A be an R-algebra (possibly non-unital). By a *left ideal* of A is meant an R-submodule $J \subset A$ which is closed under multiplication by elements of A on the left. By a *right ideal* of A is meant an R-submodule $J \subset A$ which is closed under multiplication by elements of A on the right. By an *ideal* of A is meant an R-submodule $J \subset A$ which is both a left ideal and a right ideal.

§38. Remark. If A has a unit then its three notions of ideal coincide with the same notions when we view A simply as a unital ring, because being an A-module automatically implies being an R-module due to the inclusion of scalars $\iota : R \to A$.

§39. Exercise. Prove that if A is an R-algebra and $I \subset A$ is an ideal of A the quotient ring A/I is itself an R-algebra.

§40. Generators and relations. If $f_1, \dots, f_m$ are elements of

$$R\langle x_1, \dots, x_n\rangle,$$

the R-algebra presented by generators $x_1, \dots, x_n$ and relations

$$f_1 = 0, \dots, f_m = 0$$

is

$$R\langle x_1, \dots, x_n\rangle/I,$$

where I is the ideal of A generated by $f_1, \dots, f_m$. This definition can be extended to any set X of generators and any subset $Y \subset R\langle X\rangle$. We shall write $\langle Y\rangle$ for the ideal generated by the set Y, or $\langle f_1, \dots, f_m\rangle$ in the case of a finite set.

§41. Example. Let M be a monoid (or a group). The algebra RM equals $R\langle M\rangle/I$ where the ideal I is generated by the relations $\delta_{xy} = \delta_x\delta_y$ and $1 = \delta_{1_M}$.

§42. Exercise. Show how the algebra of a quiver can be presented by generators and relations taking the edges as generators.

§43. Example. The Weyl algebra (over R) is

$$R\langle x, y\rangle / \langle yx - xy - 1\rangle.$$

(This is "almost free" on x and y but subject to the commutation relation $yx - xy = 1$.)

4 Lecture 4

Again R is a commutative ring with unit.

4.1 Complements on previous lecture

§44. Exercise. Show that $T_R(V)$ is an R-algebra.

§45. Exercise. Show that the R-algebra of a group G is graded over G.

§46. Exercise. Formulate a "natural" definition of R-algebra graded over a small category C and prove that RC is graded in this sense.

§47. Exercise. Give a presentation of RC, for a small category C, by generators and relations that uses C_1 as set of generators. Prove that this presentation indeed presents RC. Particularize for group algebras.

§48. Exercise. The *exterior algebra* $\bigwedge(V)$, or *Grassmann algebra*, of a vector space V over a field F, is defined to be the quotient of $T_F(V)$ by the ideal I generated by all the simple tensors of the form $x \otimes x$. The class $x \otimes y + I$ is denoted by $x \wedge y$, so in $\bigwedge(V)$ we have $x \wedge x = 0$.

1. Prove that $x \wedge y = -y \wedge x$.

2. Prove that if $\operatorname{char} F \neq 2$ then $\bigwedge(V)$ is also the quotient of $T_F(V)$ by the ideal generated by the elements $x \otimes y + y \otimes x$.

§49. Exercise. The *symmetric algebra* $S(V)$ of a vector space V over a field F is defined to be the quotient of $T_F(V)$ by the ideal generated by all the diferences $x \otimes y - y \otimes x$ with $x, y \in V$.

1. Prove that $S(V)$ is a commutative algebra.
2. Writing $\eta : V \to S(V)$ for the natural injection of generators, prove that any F-linear map $f : V \to A$ to a commutative F-algebra A factors uniquely through η.
3. If B is a basis of V, prove that $S(V) \cong F[B]$, where $F[B]$ is the polynomial F-algebra of polynomials written using the basis vectors as indeterminates.

4.2 The universal enveloping algebra of a Lie algebra

By a Lie algebra over a field F is meant a vector space L over F equipped with an operation

$$[-,-] : L \times L \to L,$$

called the *bracket*, which has the following properties:

1. It is bilinear,
2. $[x, x] = 0$ for all $x \in L$,
3. $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ for all $x, y, z \in L$ (Jacobi identity).

A homomorphism $f : L \to M$ of Lie algebras is a linear map that preserves the bracket:

$$f([x, y]) = [f(x), f(y)].$$

The category of Lie algebras over F is denoted by $LieAlg_F$.

§50. Exercise. Prove anticommutativity in any Lie algebra: $[x, y] = -[y, x]$. Prove that 2 above can be replaced by anticommutativity if char $F \neq 2$.

§51. Example. Any F-vector space is a Lie algebra with bracket defined by $[x, y] = 0$ for all $x, y \in V$. Such Lie algebras are called *abelian*.

§52. Example. Any F-algebra is a Lie algebra over F with the bracket defined by $[x, y] = xy - yx$. This assignment extends to a functor $L : F\text{-}Alg \to LieAlg_F$.

§53. Example. Given an F-vector space V, the *general linear Lie algebra* $\mathfrak{gl}(V)$ is the Lie algebra obtained as above from the F-algebra $\mathrm{End}_F(V)$. Hence, the bracket is the commutator

$$[f, g] = fg - gf,$$

where as usual the product fg is composition $f \circ g$.

§54. Universal enveloping algebras. Let L be a Lie algebra. The *universal enveloping Lie algebra* of L is the quotient $U(L) := T_F(L)/I$ where the ideal I is generated by the relations $[x, y] = xy - yx$. Or, being fussy with the definition of the tensor algebra, the relations are $[x, y] = x \otimes y - y \otimes x$, which means we are identifying the element $[x, y] \in L$ with $x \otimes y - y \otimes x \in L^{\otimes 2}$.

§55. Exercise. Given a Lie algebra L and an F-algebra A, prove that the homomorphisms of Lie algebras $f : L \to L(A)$ are in a bijective correspondence with the homomorphisms of F-algebras $f^\sharp : U(L) \to A$. More precisely, establish an adjunction between LieAlg_F and F-*Alg*.

§56. Remark. Contrary to tensor algebras, it is no longer obvious that the injection of generators $L \to U(L)$ is injective. Indeed it is, so L can be regarded as being a Lie subalgebra of its universal enveloping algebra, but this is a consequence of the PBW Theorem (for Poincaré–Birkhoff–Witt), whose proof is nontrivial and lies beyond the scope of these notes.

4.3 Derivations

§57. Definition. By a *not necessarily associative* R-algebra is meant an R-module A equipped with an R-bilinear operation $- \bullet - : A \times A \to A$; or, equivalently, with a homomorphism of R-modules $A \otimes_R A \to A$.

§58. Examples. Associative algebras, with $a \bullet b = ab$, and Lie algebras, with $a \bullet b = [a, b]$ (the later with R a field, although one can equally define Lie algebras over more general commutative rings).

§59. Definition. Let A be a not necessarily associative F-algebra for a field F. By a *derivation* on A is meant a homomorphism of R-modules $D : A \to A$ such that for all $a, b \in A$ the Leibniz rule is satisfied:

$$D(ab) = D(a)b + aD(b).$$

We write $\mathrm{Der}(A)$ for the set of derivations of A.

§60. EXAMPLE. The usual derivative of a smooth map $f : \mathbb{R} \to \mathbb{R}$ is a derivation $\frac{d}{dx} : C^\infty(\mathbb{R}) \to C^\infty(\mathbb{R})$, where the multiplication in $C^\infty(\mathbb{R})$ is pointwise multiplication of smooth functions.

§61. EXERCISE. Prove that $\mathrm{Der}(A)$ is a Lie subalgebra of $\mathfrak{gl}(A)$. But show that the product fg of two derivations might not be a derivation.

§62. REMARK. So we see that derivations of associative algebras, but also derivations of Lie algebras, form Lie algebras.