MA5Q6L Graduate Algebra

Daan Krammer

November 29, 2013

Contents

1 Introduction **3**
1.1 Groups . . . 3
1.2 Rings . . . 4
1.3 Exercises . . . 5

2 Categories **6**
2.1 Categories . . . 6
2.2 Relations and categories . . . 8
2.3 Free monoids and free categories . . . 9
2.4 $*$ Mono and epi . . . 9
2.5 Functors . . . 10
2.6 Products and coproducts . . . 12
2.7 Exercises . . . 15
2.8 Natural transformations . . . 16

3 The diamond lemma **18**
3.1 The diamond lemma . . . 18
3.2 Free groups . . . 19
3.3 Congruences and presentations . . . 21
3.4 The word problem . . . 22
3.5 Example: a monoid . . . 23
3.6 $*$ A diamond lemma for rings . . . 24

4 Tensor products **26**
4.1 Tensor products . . . 26
4.2 Extended tensor products . . . 28
4.3 Products of categories . . . 29
4.4 Functoriality . . . 29
4.5 Homsets of modules . . . 30
4.6 Tensor products and adjoint functors . . . 31
4.7 Tensor products of algebras . . . 32
4.8 Tensor algebras . . . 34
4.9 Symmetric and exterior algebras . . . 34

5 Homological algebra **35**
5.1 Short exact sequences . . . 35
5.2 Exact functors . . . 37
5.3 Projective modules . . . 38
5.4 Right exactness of $(D \otimes -)$ . . . 40
5.5 Derived functors . . . 41

5.6 The long exact sequence 42

6 Representation theory **44**
6.1 Some ring theory 44
6.2 Group algebras 45
6.3 Artin-Wedderburn 47
6.4 Character tables 49

1 Introduction

1.1 Groups

Definition 1.

(a) A **semigroup** is a set G along with a binary operation $G \times G \to G$: $(a,b) \mapsto ab$ satisfying

$$\textbf{associativity:} \quad a(bc) = (ab)c \quad \text{for all } a,b,c \in G.$$

(b) An **identity element, neutral element, unit, one** in a semigroup G is an element $1 \in G$ such that $1a = a1 = a$ for all $a \in G$. Sometimes it is written 1_G.

(c) A **monoid** is a semigroup along with an identity element.

(d) Let $(G,1)$ be a monoid and $a,b \in G$. We say that a,b are mutual **inverses** if $ab = ba = 1$. If $ab = 1$ then we say that a is a **left-inverse** to b and b a **right inverse** to a.

(e) A **group** is a monoid in which every element a has an inverse, usually written a^{-1}.

Every group is a monoid. Every monoid gives rise to a semigroup by forgetting the identity.

Exercise (1.1) Prove that every semigroup has at most one identity.

Because of the above exercise we may say *every monoid is a semigroup.* Moreover, it allows us to say *the semigroup G is a monoid* when we mean *the semigroup G has an identity.*

Example 2. Examples of semigroups that aren't monoids: $(\mathbb{Z}_{>0},+)$, $(2\mathbb{Z},\times)$, $(\mathbb{R},\min)$, $(P(\mathbb{Z}),\cup)$ where P denotes power set.

Examples of monoids that aren't groups: $(\mathbb{Z}_{\geq 0},+)$, $(\mathbb{Z},\times)$, $(\mathbb{Q},\times)$, $(M(n,\mathbb{Q}),\times)$, $(\mathbb{R}\cup\{\infty\},\min)$, $(\mathbb{Q}[x],\circ)$ where $\circ$ is composition: $(f\circ g)a := f(ga)$.

Exercise (1.2) Let $(G,1)$ be a monoid. Let $a,b,c \in G$ be such that $ab = bc = 1$. Prove $a = c$. In particular, an element in a monoid has at most one inverse.

Definition 3. Let G,H be semigroups. A **(semigroup) homomorphism** $f\colon G \to H$ is a map such that $f(ab) = f(a)f(b)$ for all $a,b, \in G$. Likewise for monoids and groups except that one should then add that $f(1_G) = 1_H$.

Exercise (1.3)

(a) Let G,H be groups and $f\colon G \to H$ a homomorphism. Prove $f(a^{-1}) = f(a)^{-1}$ for all $a \in G$.

(b) Find monoids G,H and a semigroup homomorphism $f\colon G \to H$ that's not a monoid homomorphism.

(c) Let G,H be groups and $f\colon G \to H$ a semigroup homomorphism. Prove that f is a group homomorphism.

Example 4.

(a) Let X be a set. Let $G = \mathrm{Map}(X)$ be the set of maps from X to itself. Then $(G,\circ)$ is a monoid. It satisfies associativity because for all $f,g,h \in G$ and all $a \in X$, omitting $\circ$ to save space

$$(f(gh))a = f((gh)a) = f(g(ha)) = (fg)(ha) = ((fg)h)a.$$

Its identity element is $\mathrm{id} = \mathrm{id}_X\colon X \to X\colon \mathrm{id}_X(a) = a$ for all $a \in X$.

A map $f\colon X \to X$ has an inverse in G if and only if it is bijective. If that is the case then the inverse of f in the sense of group theory is the inverse of f in the usual sense.

(b) Let $H = \mathrm{Sym}(X)$ denote the set of bijective maps $X \to X$. Then $(H, \circ)$ is a group called the **symmetric group** on X. We write $S_n = \mathrm{Sym}(\{1, \ldots, n\})$.

Definition 5.

(a) A **subsemigroup** of a semigroup G is a subset $H \subset G$ such that $ab \in H$ for all $a, b \in H$.

(b) A **submonoid** of a monoid G is a subsemigroup $H \subset G$ such that $1_G \in H$.

(c) A **subgroup** of a group G is a submonoid $H \subset G$ such that $a^{-1} \in H$ for all $a \in H$.

Exercise (1.4)

(a) Prove that every subsemigroup H of a semigroup G equipped with the operation $H \times H \to H\colon (a, b) \mapsto ab$ (same as in G) is a semigroup itself. Prove that the inclusion map $H \to G$ is a homomorphism. Same for monoids and groups.

(b) Let G be a group. Prove that a subgroup of G is the same thing as the image of a group homomorphism from some group to G. Likewise for monoids and semigroups.

(c) Find a monoid G and a subsemigroup H of G that's not a submonoid.

A semigroup G is **abelian** if $ab = ba$ for all $a, b \in G$.

1.2 Rings

Definition 6. A **ring** is a set R together with two binary operations $R \times R \to R$ written $(a, b) \mapsto a + b$ and $(a, b) \mapsto ab = a \times b$ such that:

- $(R, +)$ is an abelian group. Its identity element is written 0.
- $(R, \times)$ is a semigroup.
- We have $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for all $a, b, c \in R$.

If $(R, \times)$ is a monoid then we say that R is a **ring with identity** or **unital ring**. We say that R is **commutative** if $ab = ba$.

Definition 7. Let R, S be rings. A **(ring) homomorphism** $f\colon R \to S$ is a map satisfying $f(ab) = f(a)\,f(b)$ and $f(a + b) = f(a) + f(b)$ for all $a, b \in R$. If R, S have an identity then we usually require $f(1_R) = 1_S$.

Definition 8. A **division ring** is a ring R with $1_R \neq 0_R$ and in which all nonzero elements are invertible. A commutative division ring is called a **field**.

An example of a noncommutative division ring is provided by the quaternions, exercise 1.11. Examples of fields are $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{C}(X)$.

Definition 9. Let R be a ring. An ***R*-module** is an abelian group V (written additively) along with a map $R \times V \to V\colon (a, x) \mapsto ax$ such that

- We have $(ab)x = a(bx)$ for all $a, b \in R$ and $x \in V$.
- If R has 1 then $1x = x$ for all $x \in V$.

- We have $a(x+y) = ax + ay$ for all $a \in R$, $x, y \in V$.
- We have $(a+b)x = ax + bx$ for all $a, b \in R$, $x \in V$.

If R is a field then an R-module is nothing but a vector space.

Definition 10. Let V be an R-module. A **basis** for V is a set $X \subset V$ such that every element of V can uniquely be written as a finite sum $\sum_{x \in X} a_x\, x$ where $a_x \in R$. Here by **finite sum** we mean that only finitely many of the a_x are nonzero. An R-module is said to be **free** if it admits a basis.

Every vector space has a basis, exercise 1.12. However, an R-module may not. For example, $(R, V) = (\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$ or $(\mathbb{Q}[t], \mathbb{Q}[t]/(t^2-1))$.

Example 11. Let G be a group and R a commutative ring. The **group ring** $R[G] = RG$ is constructed as follows. Firstly, choose a free R-module RG with basis G. That is, every element of RG can uniquely be written as a finite sum $\sum_{x \in G} a_x\, x$ where $a_x \in R$. Addition and multiplication in RG are defined by

$$\Big(\sum_{x \in G} a_x\, x\Big) + \Big(\sum_{x \in G} b_x\, x\Big) = \sum_{x \in G} (a_x + b_x)\, x$$
$$\Big(\sum_{x \in G} a_x\, x\Big)\Big(\sum_{x \in G} b_x\, x\Big) = \sum_{x,y \in G} a_x\, b_y\, xy.$$

For example $R[\mathbb{Z}] \cong R[t, t^{-1}]$.

Definition 12. Let U, V be R-modules. A **homomorphism of R-modules** $f\colon U \to V$ is a group homomorphism such that $af(x) = f(ax)$ for all $a \in R$, $x \in U$.

1.3 Exercises

(1.5) Let M be a monoid and G the set of invertible elements of M. Prove that G, equipped with the same multiplication as M, is a group.

(1.6) Let G be a monoid. Assume that for all $a \in G$ there exists b such that $ab = 1$. (We say that b is a right inverse to a). Prove that G is a group.

(1.7) How many semigroups of two elements are there, up to isomorphism? How many monoids? How many groups?

(1.8) Let $G = \mathrm{Sym}(\mathbb{Z}/7)$, so $G \cong S_7$. Define $f, g \in G$ by $f(x) = x+1$ and $g(x) = 2x$. Let H be the subgroup of G generated by f, g. How many elements does H have?

(1.9) Let G be a group. Let $\mathrm{Aut}(G)$ be the set of automorphisms of G, that is, isomorphisms $G \to G$.

(a) Prove that $\mathrm{Aut}(G)$ equipped with composition is a group.

(b) Let C_n denote a cyclic group of order n. Let p be a prime number. Prove $\mathrm{Aut}(C_p) \cong C_{p-1}$.

(1.10) Recall that the **characteristic** of a field K is the smallest $n \geq 1$ for which 1 added to itself n times is zero, or zero if there is no such n. Show that the characteristic of a field is either zero or a prime number p.

(1.11) Prove that the set of **quaternions**

$$\mathbb{H} := \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \;\middle|\; a, b \in \mathbb{C} \right\}$$

is a subring of $M(2, \mathbb{C})$. Prove that it is a division ring.

(1.12) Let $(P, \leq)$ be an ordered set (some people say partially ordered set). A **chain** in P is a subset inheriting a total order from $(P, \leq)$. An element $a \in P$ is said to be **maximal** if $a < b$ for no $b \in P$.

Zorn's lemma states the following. Let $(P, \leq)$ be an ordered set. Suppose that for every chain $C \subset P$ there exists $a \in P$ such that $c \leq a$ for all $c \in C$. Then P has a maximal element.

Use Zorn's lemma to prove that every vector space V (not necessarily spanned by finitely many elements) over a field K has a basis.

2 Categories

2.1 Categories

Bertrand Russell proposed the following paradox. Let A be the set of all sets that don't contain themselves:

$$A = \{B \mid B \notin B\}. \tag{13}$$

Then $A \in A \Leftrightarrow A \notin A$. This is a contradiction and cannot be tolerated.

Logicians have shown the way out. If you look at the axioms of mathematics you will find that in a definition like (13) A is not a set. Instead A is a **class**. A class is like a set but possibly bigger. Every set is a class but not conversely. A **proper class** is a class that's not a set.

Likewise you cannot say *set of all groups.* Say *class of all groups* instead.

Definition 14. A **category on the right** C consists of the data:

- A class $\mathrm{Ob}(C)$ of **objects** is given.
- A class of disjoint sets $C(U, V) = \mathrm{Hom}(U, V)$ is given, one for each pair of objects U, V of C. The elements of $C(U, V)$ are called the **morphisms** or **maps from U to V**. Instead of $f \in C(U, V)$ we may write $f\colon U \to V$. We write $\mathrm{Mor}(C)$ for the class of all morphisms of C.
- For all $U \in \mathrm{Ob}(C)$ a **trivial** or **identity morphism** $1_U \in C(U, U)$ is given.
- For any three objects U, V, W of C a map

$$C(U, V) \times C(V, W) \to C(U, W)\colon (f, g) \mapsto fg \tag{15}$$

  is given called **multiplication** or **composition**.

If $f \in C(U, V)$ then we write $\mathrm{source}(f) = U$, $\mathrm{target}(f) = V$. If f, g are morphisms of C and $\mathrm{target}(f) = \mathrm{source}(g)$ then we say (unsurprisingly) that **fg is defined**.

For this to be a category the following conditions should be satisfied:

- Associativity: $f(gh) = (fg)h$ whenever $f, g, h \in \mathrm{Mor}(C)$ and fg, gh are defined.
- Identity: $1_U f = f = f 1_V$ whenever $f \in \mathrm{Mor}(C)$ and $1_U f$ and $f 1_V$ are defined.

A category is said to be **small** if its object class is a set.

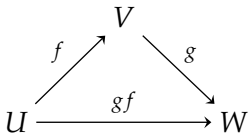
There is a category on the right $\mathbf{Sets}_R$ (R for right). Its object class is the class of all sets. The morphisms are the maps of sets. In this situation, if $f\colon U \to V$ is a map of sets (a morphism in $\mathbf{Sets}_R$) and $x \in U$ then we write xf rather than fx. That's why we call it a category on the right. Composition is as usual: $x(fg) = (xf)g$ whenever $f, g \in \mathrm{Mor}(C)$ and fg is defined and $x \in \mathrm{source}(f)$.

Definition 16. A category **on the left** is like a category on the right except that (15) is replaced by the slightly unpleasant

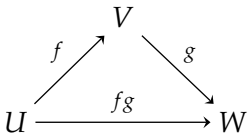
$$C(U,V) \times C(V,W) \to C(U,W)\colon (f,g) \mapsto gf$$

and this time, for morphisms f, g of C, gf is defined if and only if $\mathrm{target}(f) = \mathrm{source}(g)$.

The difference between categories on the left with those on the right is made clear by the diagrams:



A diagram in a category on the left



A diagram in a category on the right.

Note that for categories both on the right and on the left, an element in $C(U,V)$ is a morphism from U to V, not from V to U. Don't confuse this with the opposite of a category which we learn later.

There is also a category of sets on the left $\mathbf{Sets}_L$. It is like $\mathbf{Sets}_R$ except that we write fx instead of xf and composition is defined by $(fg)x = f(gx)$ whenever $f, g \in \mathrm{Mor}(C)$ and fg is defined and $x \in \mathrm{source}(g)$.

Horrible formulas such as $(fg)x = g(fx)$ should be avoided at all times. The order of f and g should be the same on both sides.

From now on we don't distinguish categories on the left from those on the right. To toggle between the two, replace fg by gf and (if necessary) fx by xf or vice versa. We simply write **Sets** for the category of sets.

Example 17. Here are some common categories.

- **Groups**. Objects: groups. Morphisms: group homomorphisms.
- **Semigroups**. Objects: semigroups. Morphisms: semigroup homomorphisms.
- **Monoids**. Objects: monoids. Morphisms: monoid homomorphisms.
- **Rings**. Objects: rings. Morphisms: ring homomorphisms.
- **Ab**. Objects: Abelian groups. Morphisms: group homomorphisms.
- ***R*-mod**. Objects: R-modules (with R fixed). Morphisms: homomorphisms of R-modules.
- $\mathbf{Vec}_K$. Objects: vector spaces over K. Morphisms: linear maps. This is the same as ***K*-mod**.
- **Top**. Objects: topological spaces. Morphisms: continuous maps.
- **Diff**. Objects: smooth (=differentiable) manifolds. Morphisms: smooth maps.

Example 18. In the examples of categories so far, every object is a set, possibly with more data and properties, and a morphism is a map of sets of some kind. This is no longer true in the following example.

(a). For a monoid G we have a category $\mathbf{Point}_G$ as follows. It has a single object pt. Moreover $\mathrm{Hom}(\mathrm{pt},\mathrm{pt}) = G$. Multiplication of morphisms is multiplication in the monoid. Prove yourself that this makes $\mathbf{Point}_G$ a category.

(b). Conversely, let U be an object of a category C. Then $C(U,U)$ becomes a monoid by equipping it with multiplication in C restricted to $C(U,U) \times C(U,U)$.

If moreover U is the only object then C is determined by M and U. Roughly speaking, monoids are essentially the same as categories of precisely one object.

Definition 19. Let f, g be morphisms in a category. If fg is defined and an identity morphism then we say that f is a **left-inverse** to g and g a **right-inverse** to f. If f is a left-inverse and right-inverse to g we say that f is an **inverse** to g. A morphism is said to be **invertible** or an **isomorphism** if it admits an inverse. If $C(U,V)$ contains an isomorphism then we say that U, V are isomorphic and write $U \cong V$.

In **Sets** two objects are isomorphic if there exists a bijection between them. If $\mathbf{Top}(U,V)$ contains an isomorphism then U and V are commonly called homeomorphic.

Exercise (2.1) Prove that a morphism in a category has at most one inverse.

Exercise (2.2) Do the same as in example 18 for groups instead of monoids.

Definition 20. The **opposite** category C^{op} to a category C is defined as follows. It has the same objects as C. Moreover $C^{\mathrm{op}}(U,V) = C(V,U)$ for all U, V. Let $*$ denote multiplication in C and $\triangledown$ in C^{op}. Assume that both categories are on the right. For morphisms f, g of C^{op} we define

$$f \triangledown g := \begin{cases} g * f & \text{if } g * f \text{ is defined} \\ \text{undefined} & \text{if } g * f \text{ is undefined.} \end{cases}$$

Prove yourself that this makes C^{op} into a category.

Warning: This has nothing to do with the distinction between categories on the left or right. We happily identify a category on the right with the same category on the left but don't identify a category with its opposite.

Exercise (2.3) Let G be a monoid. Show that there exists a unique monoid H such that $(\mathbf{Point}_G)^{\mathrm{op}} = \mathbf{Point}_H$ (not just isomorphic). It is known as the **opposite** to G: $H = G^{\mathrm{op}}$.

Exercise (2.4) Assuming that you know (or guess) what isomorphic categories means (it's coming soon anyway): Prove that **Sets** is not isomorphic to its opposite.

2.2 Relations and categories

Reminder on relations. Let A be a set. A (binary relation) on A is a subset $R \subset A \times A$. Instead of $(x,y) \in R$ we may write xRy. Instead of xRy and yRz we write $xRyRz$, and so on. Here are some properties which a relation may or may not have.

- Reflexive: xRx for all $x \in A$.
- Symmetric: $xRy \Rightarrow yRx$ for all $x, y \in A$.
- Anti-symmetric: $xRyRx \Rightarrow x = y$ for all $x, y \in A$.

- Transitive: $xRyRz \Rightarrow xRz$ for all $x, y, z \in A$.

A **preordering** is a reflexive, transitive relation. An **equivalence relation** is a symmetric preordering. An **ordering** is an anti-symmetric preordering (usually written $\leq$). An **ordered set** is a pair $(A, \leq)$ of a set A and an ordering on A. An ordering $\leq$ on A is **total** if ($x \leq y$ or $y \leq x$) for all $x, y \in A$.

Example 21. Let $(A, \leq)$ be an ordered set. This gives rise to a category C as follows. The class of objects is A. For $a, b \in A$ we put $C(a,b) = \varnothing$ unless $a \leq b$ in which case $C(a,b)$ has precisely one element (for example, $C(a,b) = \{(a,b)\}$). This already determines the multiplication and thereby the category C.

Conversely a category C with $\#C(U,V) \leq 1$ for all U, V and no two isomorphic objects gives rise to an ordered set. Roughly speaking, a small category C with $\#C(U,V) \leq 1$ for all U, V and no two isomorphic objects is essentially the same as an ordered set.

If something about categories seems hard, it often helps to do it for ordered sets first.

Exercise (2.5) Do the same as in example 21 for preordered sets instead of ordered sets. Also for equivalence relations.

2.3 Free monoids and free categories

Let A be a set. The **free monoid** on A is $\bigsqcup_{n \geq 0} A^n$ where $\sqcup$ denotes the disjoint union and A^n the Cartesian nth power. We make this into a monoid by concatenation:

$$(a_1, \ldots, a_m)(a_{m+1}, \ldots, a_n) = (a_1, \ldots, a_n).$$

Free categories are a straightforward generalisation of free monoids.

Let P be a class. Let disjoint sets $Q(U,V)$ be given, one for each pair $(U,V) \in P^2$. The elements of the $Q(U,V)$ are called **generators**. For $f \in Q(U,V)$ write $\text{source}(f) = U$ and $\text{target}(f) = V$.

With P and the $Q(U,V)$ as above is associated a **free category** or **path category** C (on the right) which is defined as follows. Its object class is P. Its nontrivial morphisms are those finite nonempty sequences $(f_1, \ldots, f_n)$ of generators such that $\text{target}(f_i) = \text{source}(f_{i+1})$ for all i. This morphism is said to be from $\text{source}(f_1)$ to $\text{target}(f_n)$. Composition in C of nontrivial morphisms is defined by concatenation:

$$(f_1, \ldots, f_m)(f_{m+1}, \ldots, f_n) = (f_1, \ldots, f_n).$$

Prove yourself that this determines C and that C is a category.

Any category isomorphic to the foregoing free category is also said to be free.

In particular, if $\#P = 1$, the above again defines the free monoid.

Exercise (2.6) Prove that **Sets** is not a free category.

2.4 $*$ Mono and epi

For the academic year 2013-2014 we skip this section.

Definition 22. Let f be a morphism in a category C on the right.

(a) We call f a **monomorphism** in C if for all $g, h \in \text{Mor}(C)$ such that gf and hf are defined and equal, we have $g = h$.

(b) We call f an **epimorphism** in C if for all $g, h \in \mathrm{Mor}(C)$ such that fg and fh are defined and equal, we have $g = h$.

Note that epimorphisms in C are monomorphisms in C^{op} and vice versa.

Example 23. In **Sets** a map is a monomorphism if and only if it is injective. In **Sets** a map is an epimorphism if and only if it is surjective.

Proposition 24. *In* **Groups** *a homomorphism is a monomorphism if and only if it is injective.*

Proof. Let $f\colon G \to H$ be a monomorphism of groups. Let $x, y \in G$ be such that $f(x) = f(y)$. Note that we have changed to notation on the left. Define $g, h\colon \mathbb{Z} \to G$ by $g(n) = x^n$, $h(n) = y^n$. Then g, h are homomorphisms of groups. Also $fg(n) = f(x)^n = f(y)^n = fh(n)$ for all $n \in \mathbb{Z}$. So $fg = fh$. But f is mono so $g = h$. So $x = g(1) = h(1) = y$. So f is injective. The converse is trivial. □

In **Groups** every epimorphism is surjective but this is a bit harder.

Exercise (2.7) It's not hard to contrive epimorphisms that are not surjective and monomorphisms that are not injective. Here are somewhat "natural" ones.

(a) Prove that the inclusion $\mathbb{Z} \to \mathbb{Q}$ is an epimorphism in **Rings**.

(b) Consider the category C with one object $\mathbb{C}$ and whose morphisms are the maps $\mathbb{C} \to \mathbb{C}$ given by a polynomial. Composition in C is composition of maps. Define $f \in C(\mathbb{C}, \mathbb{C})$ by $f(x) = x^3 + x$. Prove that f is a monomorphism.

So epimorphism doesn't imply surjective. Don't say epimorphism when you mean surjective or vice versa. Likewise for monomorphism and injective.

Exercise (2.8)

(a) Prove that a morphism in **Rings** is a monomorphism if and only if it is injective.

(b) Prove that a morphism in ***R*-mod** is a monomorphism if and only if it is injective.

(c) Prove that a morphism in ***R*-mod** is an epimorphism if and only if it is surjective.

Exercise (2.9) Let f, g be morphisms in a category on the right such that fg is defined. Prove that if f and g are monomorphisms then so is fg. Prove that if fg is a monomorphism then so is f.

2.5 Functors

Not only does a category contain maps, there are also maps from one category to another. They are called functors and are defined as follows.

Definition 25. Let C, D be categories on the right. A **functor** $T\colon C \to D$ consists of the following:

- A map of classes $\mathrm{Ob}(C) \to \mathrm{Ob}(D)$ is given which is also simply written T.
- For all objects $U, V \in \mathrm{Ob}(C)$ a map of sets $C(U, V) \to D(T(U), T(V))$ is given again simply written T.

These should satisfy:

- Let $f, g \in \mathrm{Mor}(C)$ be such that fg is defined (whence so is $T(f)\,T(g)$). Then $T(fg) = T(f)\,T(g)$.
- For all $U \in \mathrm{Ob}(C)$ we have $T(1_U) = 1_{T(U)}$.

Example 26. Here are a few examples of functors.

(a). Let $T\colon C \to D$ be a functor. Let U be an object of C and write $V = F(U)$. Recall that $C(U,U)$ and $D(V,V)$ are monoids. Then the map $C(U,U) \to D(V,V)$ induced by T is a homomorphism of monoids.

We have the following converse. Let G, H be monoids and $\phi\colon G \to H$ a monoid homomorphism. Let $C = \mathbf{Point}_G$, $D = \mathbf{Point}_H$ be the associated categories so in particular $\mathrm{Ob}(C) = \mathrm{Ob}(D) = \{\mathrm{pt}\}$ and $C(\mathrm{pt},\mathrm{pt}) = G$ and $D(\mathrm{pt},\mathrm{pt}) = H$. Then there is a (unique) functor $T\colon C \to D$ defined by $T(\mathrm{pt}) = \mathrm{pt}$ and $T(f) = \phi(f)$ for all $f \in \mathrm{Mor}(C)$.

Summarising one can say, somewhat vaguely, that a homomorphism between two monoids G, H is the same as a functor between $\mathbf{Point}_G$, $\mathbf{Point}_H$.

(b). There is a 'forgetful functor' T: **Rings** $\to$ **Ab** taking a ring R to the additive group $(R,+)$: it forgets multiplication in R. For $f \in \mathrm{Mor}(\mathbf{Rings})$ we put $T(f) = f$. Prove yourself that T is a functor.

The term *forgetful functor* has no precise definition. Usually it means that the functor is very easy to define.

Some other forgetful functors are **Rings** $\to$ **monoids**, **Rings** $\to$ **Sets**, $\boldsymbol{R}$**-mod** $\to$ $\boldsymbol{S}$**-mod** if $S \subset R$ are rings.

(c). We define a functor P: **Sets** $\to$ **Sets** called **power set**. For objects U of **Sets** $P(U)$ is the set of subsets of U. Let now $f \in \mathbf{Sets}(U,V)$. We define $P(f) := g$ where, for all subsets $X \subset U$, we put

$$g(X) = \{f(y) \mid y \in X\}$$

which is a subset of V as it should. You're probably used to writing $f(X)$ instead of $g(X)$ which we continue to do. Prove yourself that P is a functor.

(d). Let U be an object in a category C. We define a functor $T = C(U,-)\colon C \to$ **Sets**. To keep the notation convenient we write A^T instead of $T(A)$ if A is either an object or morphism of C. For $V \in \mathrm{Ob}(C)$ we put $V^T = C(U,V)$. For $f \in C(V,W)$ and $x \in V^T = C(U,V)$ we put $x f^T := xf$ (note that xf is the product of two morphisms in C). Prove yourself that T is a functor.

Suppose we have two functors

$$C \xrightarrow{S} D \xrightarrow{T} E.$$

The **composition** $TS\colon C \to E$ is defined on objects by $(TS)U = T(SU)$ and on morphisms by $(TS)f = T(Sf)$. Every category C admits an **identity functor** $1_C\colon C \to C$ which takes every object or morphism to itself.

It may seem that we have defined the category of categories. Unfortunately there is no such thing for the same reason that we cannot say *the class of all classes.* At least we have obtained the **category of small categories**.

Definition 27. A functor $S\colon C \to D$ is said to be **invertible** or an **isomorphism of categories** if there exists a functor $T\colon D \to C$ such that $ST = 1_D$ and $TS = 1_C$. Don't confuse this with equivalence of categories to be defined later.

Definition 28. Let C, D be categories. By a **contravariant functor** $C \to D$ we mean a functor $C \to D^{\mathrm{op}}$.

Exercise (2.10) Give a definition of *contravariant functor* that avoids the use of opposites, by modifying the definition of *functor*.

Exercise (2.11) Prove that a functor $C \to D^{\mathrm{op}}$ is the same as a functor $C^{\mathrm{op}} \to D$.

Sometimes we say **covariant functor** instead of functor.

Exercise (2.12) For $s \in \{-1, 1\}$ an ***s*-functor** (or functor with **sign** s) is meant to be a covariant functor if $s = 1$ or a contravariant functor if $s = -1$.

Suppose S is an s-functor and T a t-functor in a diagram

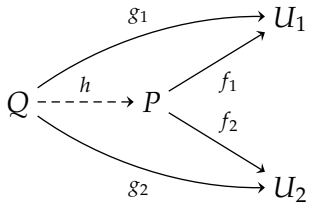
$$C \xrightarrow{S} D \xrightarrow{T} E.$$

Explain how the composition TS should be defined. Prove that TS is an st-functor $C \to E$.

2.6 Products and coproducts

Definition 29. Let C be a category on the right. Let $\{U_i \mid i \in I\}$ be an indexed family of objects in C. A **product** in C (in the categorical sense) of these objects consists of an object P of C and morphisms $f_i \colon P \to U_i$ for all $i \in I$ with the following property.

Let $Q \in \mathrm{Ob}(C)$. For all $i \in I$ let a morphism $g_i \colon Q \to U_i$ be given. Then there exists a unique $h \colon Q \to P$ such that $g_i = hf_i$ for all $i \in I$. The following diagram shows the situation for $I = \{1, 2\}$.



If $(P, \{f_i \mid i \in I\})$ is a product we also say (oversimplifying) that P is a/the product.

Exercise (2.13) Let C be a category all of whose morphisms are identity morphisms. Prove that two distinct objects in C don't have a product.

So products don't always exist. If they exist then they are unique in the following sense.

Proposition 30. *Let $\{U_i \mid i \in I\}$ be objects in a category C on the right admitting two products $(P, \{f_i \mid i \in I\})$ and $(Q, \{g_i \mid i \in I\})$. Then there exists a unique isomorphism $h \colon Q \to P$ such that $g_i = hf_i$ for all i. In particular, $P \cong Q$.*

Proof. Since P is a product, there exists a morphism $h \colon Q \to P$ such that $g_i = hf_i$ for all i. Likewise, interchanging the roles of P, Q, there exists $\ell \colon P \to Q$ such that $f_i = \ell g_i$ for all i.

In the definition that P is a product, choose $Q = P$ and $g_i = f_i$. We find that there exists at most one $m \colon P \to P$ such that $f_i = mf_i$ for all i. But we know two such m, namely, identity and ℓh. This proves $\ell h = 1$. Likewise $h\ell = 1$. Therefore h is an isomorphism. This proves the existence part of the proposition. Finally h is unique because P is a product. □

The definition of products in categories is an example of a **universal property**. Universal properties are very common and one of the great uses of categories. They

all have in common that uniqueness is true and easy to prove, just as in proposition 30. But existence may be hard to prove or simply false.

Example 31. Consider the category of groups. Let $\{G_i \mid i \in I\}$ be a family of groups.

Let's first define the direct product of these groups even though you've probably seen this. Let P be the set of maps p from I to the disjoint union of the G_i such that $p(i) \in G_i$ for all i. Multiplication in P is defined pointwise: $(pq)i = (pi)(qi)$ for all $p, q \in P$, $i \in I$. Prove yourself that this makes P into a group. It is known as the **direct product** of $\{G_i \mid i \in I\}$.

We define group homomorphisms $f_i\colon P \to G_i$ by $f_i(p) = p(i)$.

We claim that

$$P \text{ and the } f_i \text{ are a product of } \{G_i \mid i \in I\} \text{ in the categorical sense.}$$

To prove this, let Q be a group and $g_i\colon Q \to G_i$ a homomorphism. Define $h\colon Q \to P$ by $(hx)i = g_i(x)$ for all $x \in G_i$. Then $g_i = f_i h$ for all i as required.

Conversely, let $h\colon Q \to P$ be a homomorphism such that $g_i = f_i h$ for all i. For all $x \in G_i$ then, $g_i(x) = (f_i h)(x) = (hx)i$, which shows that there is just one such h.

A branch of mathematics called *universal algebra* studies a wide-ranging family of categories called algebraic categories. The definition of **algebraic categories** is outside our scope but to give an impression we shall define a typical algebraic category **Smurfs**. More about algebraic categories you don't need to know! Moreover smurfs are just that bit harder to keep you from getting bad ideas like solving the word problem in a free smurf. Otherwise smurfs are completely uninteresting.

A **smurf** is a set G along with a binary operation $G^2 \to G\colon (a, b) \mapsto ab$ such that $(ab)(ba) = b(a(ab))$ for all $a, b \in G$. For smurfs G, H a **smurf homomorphism** $f\colon G \to H$ is a map such that $f(ab) = (fa)(fb)$ for all $a, b \in G$. This gives us a category **Smurfs** whose objects are the smurfs and their homomorphisms.

The results in example 31 are easily generalised to all algebraic categories including **Sets**, **Groups**, **Rings**, and **Smurfs**. (Note that all operations in the direct product are pointwise.) So an algebraic category has all products. But the opposites to algebraic categories behave very differently.

Definition 32. Let $\{U_i \mid i \in I\}$ be objects in a category C. A **coproduct** of these consists of an object P and morphisms $f_i \in C(U_i, P)$ provided they form a product in C^{op} of the same objects.

Exercise (2.14) Define *coproduct* in a way that avoids opposite categories, by modifying the definition of *product*.

Proposition 33. *Let $\{U_i \mid i \in I\}$ be objects in a category C on the right admitting two coproducts $(P, \{f_i \mid i \in I\})$ and $(Q, \{g_i \mid i \in I\})$. Then there exists a unique isomorphism $h\colon Q \to P$ such that $g_i = f_i h$ for all i. In particular, $P \cong Q$.*

Proof. This is immediate from proposition 30 applied to C^{op} instead of C. □

Propositions 30 and 33 are examples of two **dual** results. There are many more pairs of dual results about categories. They arise by reversing all arrows (slang for replacing a category by its opposite). We often state just one of a dual pair and tacitly expect the reader to understand that the dual version exists, and that it doesn't need any further proof.

We have seen that products don't always exist. Therefore neither do coproducts.

Example 34. In **Sets** every coproduct exists. It is the disjoint union.

Exercise (2.15) Let $\{G_i \mid i \in I\}$ be smurfs admitting a coproduct $(P, \{f_i \mid i\})$. Prove that P is generated by the $f_i(G_i)$.

Definition 35. Let $\{G_i \mid i \in I\}$ be disjoint semigroups. Let U be their (disjoint) union. The **free product** of $\{G_i \mid i \in I\}$ is the following semigroup P. As a set we put

$$P = \left\{(x_1, \ldots, x_n) \in U^n \;\middle|\; n \geq 1,\ \{x_i, x_{i+1}\} \not\subset G_j \text{ for all } i, j\right\}.$$

Multiplication in P is defined by

$$(x_1, \ldots, x_m)(y_1, \ldots, y_n) = \begin{cases} (x_1, \ldots, x_{m-1}, x_m\, y_1, y_2, \ldots, y_n) & \text{if } \{x_m, y_1\} \subset G_i \\ & \text{for some } i, \\ (x_1, \ldots, x_m, y_1, \ldots, y_n) & \text{otherwise.} \end{cases}$$

Prove yourself that P is a semigroup. We define $f_i \colon G_i \to P$ by $f_i(x) = (x)$ (a sequence of just one element). Clearly f_i is a semigroup homomorphism for all i.

Exercise (2.16) In the notation of definition 35, prove that $(P, \{f_i \mid i\})$ is a coproduct of $\{G_i \mid i \in I\}$ in **Semigroups**.

Exercise (2.17) Using that **Semigroups** has coproducts, prove that **Monoids** has.

An algebraic category has all coproducts. The proof of this for monoids is similar to the one for semigroups but slightly harder. For rings it is again a bit harder. As you go further it soon gets so hard that a completely different proof is needed, which applies to all algebraic categories but is less informative. See exercise 2.18.

It is less informative because it doesn't solve the *word problem* in a coproduct. Roughly speaking this means that it doesn't give a list of the elements of the coproduct unless you allow it to list the same element more than once. A theorem exists that the word problem in a coproduct is in general unsolvable.

Exercise (2.18) (Outside our scope.) Prove that **Smurfs** has all coproducts. Hint: don't use anything special about smurfs like solving the word problem.

Exercise (2.19) We consider the category **Ab** of abelian groups. Let $\{G_i \mid i \in I\}$ be abelian groups.

(a) Prove that $\{G_i \mid i \in I\}$ admit a product $(P, \{f_i \mid i\})$ and a coproduct $(Q, \{g_i \mid i\})$.

(b) Prove that if I is finite then $P \cong Q$.

(c) Give an example where $P \ncong Q$.

Exercise (2.20) Give an example of a functor $T \colon C \to D$ and objects U, V of C such that the (categorical) products $U \times V$ and $T(U) \times T(V)$ exist but $T(U \times V) \ncong T(U \times V)$.

Exercise (2.21) (Outside our scope.) For $g \in S_n$ put

$$N(g) = \left\{(i, j) \in \mathbb{Z}^2 \;\middle|\; 1 \leq i < j \leq n,\ g^{-1}(i) > g^{-1}(j)\right\}.$$

Let $\leq$ be the ordering on S_n defined by $g \leq h$ if and only if $N(g) \subset N(h)$. Prove that the category associated with $(S_n, \leq)$ has all products and coproducts. (We say $(S_n, \leq)$ has all meets and joins.)

2.7 Exercises

(2.22) Prove that a morphism in a category has at most one inverse.

(2.23) Prove that **Sets** is not isomorphic to its opposite.

(2.24) Prove that every group is isomorphic to its opposite. Give an example of a monoid that's not isomorphic to its opposite.

(2.25) In an example we saw that an ordered set is essentially the same as a category C with $\#C(U,V) \leq 1$ for all U, V and not containing isomorphisms other than identity maps. Without proof give similar statements for preordered sets and for equivalence relations.

(2.26) Let $(P, \leq)$ be an ordered set and $Q \subset P$. A greatest common lower bound or **meet** of Q written $\wedge Q$ is an element $r \in P$ such that for all $s \in P$

$$(s \leq q \quad \text{for all } q \in Q) \iff s \leq r.$$

Likewise, a least common upper bound or **join** of Q written $\vee Q$ is an element $r \in P$ such that for all $s \in P$

$$(q \leq s \quad \text{for all } q \in Q) \iff r \leq s.$$

(a) Prove without using categories that $\wedge Q$ may not exist.

(b) Prove without using categories that if $\wedge Q$ exists then it is unique.

(c) Let C be the category associated with $(P, \leq)$ as in example 21. Then a meet in P is the same as a product in C. Restate this more precisely and prove it.

(d) Let G be a group. Let P be the set of subgroups of G, ordered by inclusion. Prove that $(P, \leq)$ has all joins and meets.

(2.27) Let C, D be categories and $T\colon C \to D$ a functor. Let U, V be isomorphic objects of C. Prove that $T(U)$ and $T(V)$ are isomorphic in D.

(2.28) For a group G let G' be the subgroup of G generated by $\{[a,b] \mid a, b \in G\}$ where $[a,b] = aba^{-1}b^{-1}$. We know that G' is a normal subgroup of G and that G/G' is abelian.

(a) For a homomorphism of groups $h\colon G \to H$ prove that there exists a unique homomorphism $h'\colon G/G' \to H/H'$ defined by $h'(xG') = h(x)H'$.

(b) Prove that there exists a functor F: **Groups** $\to$ **Ab** which on objects is given by $F(G) = G/G'$ and on morphisms by $F(h) = h'$. It is called the **abelianisation**.

(2.29) The **centre** $Z(G)$ of a group G is the subgroup $\{a \in G \mid ab = ba \text{ for all } b \in G\}$. Prove that there is no functor F: **Groups** $\to$ **Ab** which on objects is $F(G) = Z(G)$. Hint: $S_2 \hookrightarrow S_3 \twoheadrightarrow S_2$.

(2.30) Construct a functor T: **Groups** $\to$ **Rings** that takes a group G to the group algebra $\mathbb{Z}[G]$. Prove your claims.

(2.31) Prove that **Sets** can be embedded into its opposite. That is, prove that there exists a functor **Sets** $\to$ **Sets**$^{\text{op}}$ which is injective on objects and morphisms. Hint: modify the power set functor.

2.8 Natural transformations

Definition 36. Let C, D be categories and $S, T\colon C \to D$ be functors. A **natural transformation** $\alpha\colon S \to T$ consists of morphisms $\alpha_U\colon S(U) \to T(U)$ in D, one for each object $U \in \mathrm{Ob}(C)$, such that the diagram

$$\begin{array}{ccc} S(U) & \xrightarrow[\alpha_U]{} & T(U) \\ {\scriptstyle S(f)}\downarrow & & \downarrow{\scriptstyle T(f)} \\ S(V) & \xrightarrow{\alpha_V} & T(V) \end{array}$$

commutes whenever $f \in C(U, V)$.

Example 37. The determinant is a natural transformation.

Let **CRings** denote the category of commutative rings with one and ring homomorphisms. Fix $n \geq 1$. We have a functor S: **CRings** $\to$ **Monoids** where on objects $S(U) = M(n, U)$ (having only multiplication, no addition) and on morphisms $S(f)$ applies the morphism f to n^2 entries separately. Let T: **CRings** $\to$ **Monoids** denote the forgetful functor which forgets addition in a ring. This is just S with 1 instead of n.

Recall that the determinant is a monoid morphism $M(n, U) \to U$ for every commutative ring U. Denote it by α_U. Then α is a natural transformation $S \to T$.

$$\begin{array}{ccc} M(n,U) & \xrightarrow[\det]{} & U \\ {\scriptstyle S(f)}\downarrow & & \downarrow{\scriptstyle T(f)} \\ M(n,V) & \xrightarrow{\det} & V \end{array}$$

Example 38. Let C be a category on the right and $f \in C(V, U)$. Recall from example 26(d) the functors $S = C(U, -)$, $T = C(V, -)\colon C \to$ **Sets** given by $S(W) = C(U, W)$, $x(Sg) = xg$ and likewise for T.

We define a natural transformation $\alpha\colon S \to T$ as follows. Let $W \in \mathrm{Ob}(C)$. Then $\alpha_W\colon C(U, W) \to C(V, W)$ is defined by $x\,\alpha_W = fx$ (composition in C).

To prove that α is a natural transformation let $g \in C(W, X)$. Then the following diagram commutes, so α is a natural transformation $S \to T$.

$$\begin{array}{ccc} C(U,W) & \xrightarrow[\alpha_W\colon x\mapsto fx]{} & C(V,W) \\ {\scriptstyle S(g)\colon x\mapsto xg}\downarrow & & \downarrow{\scriptstyle T(g)\colon x\mapsto xg} \\ C(U,X) & \xrightarrow{\alpha_X\colon x\mapsto fx} & C(V,X) \end{array}$$

Definition 39. A **natural isomorphism** is a natural transformation α such that α_U is an isomorphism for all U.

Example 40. Fix a field K. For a vector space U over K we define the **dual** U^* to be $\mathrm{Hom}(U, K)$, the set of linear maps $U \to K$. Then U^* is again a vector space over K.

If U has finite dimension then U and U^* are isomorphic, that is, have the same dimension. But there is no 'best' isomorphism between them.

Let C be the category of finite-dimensional vector spaces over K and their linear maps.

We define a contravariant functor $T\colon C \to C$ by $T(U) = U^*$ for all $U \in \mathrm{Ob}(C)$ and $x(Tf) = fx$ whenever $f \in C(U, V)$ and $x \in T(V) = C(V, K)$.

Clearly T is not an isomorphism of categories $C \to C^{\mathrm{op}}$, because a finite-dimensional vector spaces may not be of the form $\mathrm{Hom}(U, K)$, though it is certainly isomorphic to one of these.

We claim however:

$$T^2 \text{ is naturally isomorphic to the identity functor } S\colon C \to C.$$

For $U \in \mathrm{Ob}(C)$ define $\alpha_U \in C(U, T^2(U))$ by $y(x\alpha_U) = xy$ for all $x \in U$, $y \in U^*$. We claim that α is a natural transformation $S \to T^2$.

$$\begin{array}{ccc} U & \xrightarrow[\alpha_U]{} & U^{**} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle T^2(f)} \\ V & \xrightarrow[\alpha_V]{} & V^{**} \end{array}$$

Proof of this. Write all maps on the right except S, T. Let $f \in C(U, V)$. For all $x \in U$, $y \in V^*$ then

$$\begin{aligned} &y(x(f \circ \alpha_V)) = y((xf)\alpha_V) = (xf)y = x(f \circ y) = (f \circ y)(x\alpha_U) \\ &= (y(Tf))(x\alpha_U) = y((Tf) \circ (x\alpha_U)) = y([x\alpha_U](T^2 f)) = y(x[\alpha_U \circ (T^2 f)]) \end{aligned}$$

whence $f \circ \alpha_V = \alpha_U \circ (T^2 f)$. Prove yourself that α_U is an isomorphism using that U is finite-dimensional. So α is a natural isomorphism $S \to T^2$.

Definition 41. Two categories C, D are said to be **equivalent**, notation $C \sim D$, if there exist functors $S\colon C \to D$, $T\colon D \to C$ such that ST and TS are naturally isomorphic to identity functors.

So in example 40 we have shown that the category of finite-dimensional vector spaces over a field is equivalent to its opposite.

Exercise (2.32) Prove that **Sets** is not equivalent to its opposite.

Exercise (2.33) Let G, H be groups considered as categories (with one object). Let $S, T\colon G \to H$ be functors (group homomorphisms). Prove that there exists a natural transformation $S \to T$ if and only if S, T are conjugate, that is, there exists $h \in H$ such that $Tg = h(Sg)h^{-1}$ for all $g \in G$.

Exercise (2.34) For a group G let $\alpha_G\colon G \to G/G'$ be the natural homomorphism, $\alpha_G(x) = xG'$.

Recall the functor T: **Groups** $\to$ **Groups** from sheet 2: On objects $T(G) = G/G'$ and if $h\colon G \to H$ is a group homomorphism and $x \in G$ then $(Th)(xG') = (hx)H'$. Let S: **Groups** $\to$ **Groups** be the identity functor.

Prove that α is a natural transformation $S \to T$.

Exercise (2.35) Let C be a category. For each isomorphism class $A \subset \mathrm{Ob}(C)$ choose an element $U_A \in A$. Let D denote the category whose objects are the U_A and such that $D(U, V) = C(U, V)$ whenever $U, V \in \mathrm{Ob}(D)$, and D has the same multiplication as C. We call D a **skeleton** of C.

(a) Prove that any two skeletons of C are isomorphic categories. This justifies saying *the* skeleton of C.

(b) Prove that a category is equivalent to any skeleton of itself.

(c) Prove that two categories are equivalent if and only if they have isomorphic skeletons.

Exercise (2.36) Let C, D, E be categories. Prove that if $C \sim D \sim E$ then $C \sim E$.

Exercise (2.37) Fix a field K. Let C be the category whose object set is $\mathbb{Z}_{\geq 0}$ and such that $C(m,n)$ is the set of $m \times n$ matrices over K. Note that $\#C(m,n) = 1$ if $mn = 0$. Composition in C is matrix multiplication.

Let D be the category of finite-dimensional vector spaces over K and linear maps.

(a) Prove that C is isomorphic to its opposite.

(b) Prove that C is equivalent to D.

(c) Deduce (again) that D is equivalent to its opposite.

Exercise (2.38) Find two distinct functors F: **Groups** $\to$ **Groups** with $F(G) = G$ for all groups G.

3 The diamond lemma

3.1 The diamond lemma

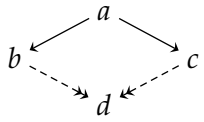
Let $(P, \geq)$ be an ordered set. An element $a \in P$ is said to be **minimal** if $(a \geq b \Rightarrow a = b)$ for all $b \in P$. An element $a \in P$ is **least** if $b \geq a$ for all $b \in P$. Note:

- Every least element is minimal but not conversely.
- If a least element exists then it is unique.
- If P has a least element then it has a unique minimal element.
- If P is finite then a least element exists if and only if there is just one minimal element. For infinite P this is false in general.

Let $R \subset A \times A$ be a relation on a set A. The intersection of the reflexive transitive relations on A containing R is called the **reflexive transitive closure of R**. Likewise, the intersection of the equivalence relations on A containing R is called the equivalence relation **generated by R**.

Lemma 42: Diamond lemma. *Let $\to$ be a relation on a set P. Let $\twoheadrightarrow$ denote the reflexive transitive closure of $\to$ and $\sim$ the equivalence relation generated by $\to$. Assume:*

- *Well-founded: there is no infinite sequence $a_0 \to a_1 \to \cdots$.*
- *Confluent: Let $a, b, c \in P$ be such that $a \to b$ and $a \to c$. Then there exists $d \in P$ such that $b \twoheadrightarrow d$ and $c \twoheadrightarrow d$.*



*An element $a \in P$ is said to be **reduced** if $a \to b$ for no $b \in P$. Then every $\sim$-class contains a unique reduced element.*

Proof. We shall only prove this with the following additional assumption:

$$\begin{aligned} &\text{There is a function } h\colon P \to \mathbb{Z} \text{ such that } a_0 \to \cdots \to a_n \\ &\text{with } a_i \in P \text{ for all } i \text{ implies } n \leq h(a_0). \end{aligned} \tag{43}$$

For a full proof see exercise 3.1.

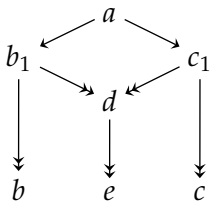
By well-foundedness, $\twoheadrightarrow$ is an ordering. If $a \twoheadrightarrow b$ we say that b is a lower bound to a.

For $a \in P$ let $\ell(a)$ be the least integer k such that $a = a_0 \to \cdots \to a_n$ implies $n \leq k$. Such a k exists by (43). By induction on $k = \ell(a)$ we shall prove that every $a \in P$ admits a unique reduced lower bound which we shall denote by $R(a)$. Existence is clear; it is the uniqueness that must be proved.

If $\ell(a) = 0$ then a is reduced and the claim is clear. Assuming that it's true for $k-1$ we prove it for k. Suppose that $b, c \in P$ are reduced lower bounds of a. We must prove $b = c$.

If $a \in \{b, c\}$ then a is reduced so $a = b = c$ as required.

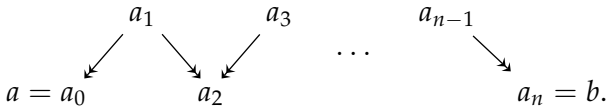
Suppose now $a \notin \{b, c\}$. Say $a \to b_1 \twoheadrightarrow b$ and $a \to c_1 \twoheadrightarrow c$. By confluence there exists d such that $b \twoheadrightarrow d$ and $c \twoheadrightarrow d$. Let e be a reduced lower bound of d.



Note $\ell(b_1) \leq \ell(a) - 1$. By the induction hypothesis b_1 has a unique reduced lower bound. But b and e are two reduced lower bounds. Therefore $b = e$. Likewise $e = c$. Therefore $b = c$ as required.

We know that every equivalence class contains a reduced element. It remains to prove that it is unique. Let a, b be equivalent reduced elements. We must prove $a = b$.

Since a, b are equivalent there exists a 'zig-zag path'



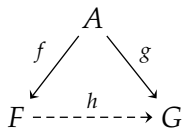
Clearly $R(a_i) = R(a_{i+1})$ for all i. Therefore $a = R(a) = R(b) = b$ as promised. □

Exercise (3.1) Give a full proof of the diamond lemma, that is, not assuming (43). (It is easy to find an example where (43) is false.)

Hint: For $a \in P$ put $Q(a) = \{b \in P \mid a \twoheadrightarrow b\}$. Let R be the set of elements $a \in P$ such that $Q(a)$ doesn't have a least element.

3.2 Free groups

Definition 44. Let A be a set. A **free group** on A consists of a group F and a map of sets $f\colon A \to F$ such that if G is a group and $g\colon A \to G$ is a map then there exists a unique homomorphism $h\colon F \to G$ such that $g = fh$ (category on the right).



Remark 45. This definition has an obvious analogue for semigroups, monoids and so on.

More generally, let C be a category equipped with a functor $T\colon C \to$ **Sets** (a **concrete category**). Let A be a set. Then a **free object** in C on A consists of an object $U \in \mathrm{Ob}(C)$ along with a map $u\colon A \to T(U)$ such that if $V \in \mathrm{Ob}(C)$ and $v\colon A \to T(V)$ then there exists a unique morphism $h\colon U \to V$ such that $v = uh$.

Exercise (3.2) Prove that free groups are unique in the following sense. Let two free groups $f\colon A \to F$, $g\colon A \to G$ on a set A be given. Then there exists a unique group isomorphism $h\colon F \to G$ such that $g = fh$.

Remark 46. Free objects in concrete categories (see remark 45) are always unique.

Exercise (3.3) Give an example of a concrete category where some free objects don't exist.

Exercise (3.4) Let A, B be sets. Prove that $F(A \sqcup B)$ is the coproduct of $F(A), F(B)$, assuming that these free groups exist.

Proposition 47. *Free groups exist.*

Proof. The **first proof** is a general one that applies to all algebraic categories. This is analogous to coproducts in algebraic categories. Do this as an exercise. □

Let's prepare for our **second proof** of the existence of free groups. It is more informative than the first but doesn't apply to all algebraic categories.

Let A be a set. Let A^* denote the free monoid on $A \times \{-1, 1\}$, see section 2.3. An element of A^* is often called a **word** and then the elements of A are called **letters** and A an **alphabet**.

Let us write an element of $A \times \{-1, 1\}$ as $\binom{a}{s}$ instead of (a, s). The **inverse of a word** is defined by

$$(\binom{a_1}{s_1}, \cdots, \binom{a_n}{s_n})^{-1} = (\binom{a_n}{-s_n}, \cdots, \binom{a_1}{-s_1}).$$

Warning: $uu^{-1} \neq 1$ for $u \in A^*$ in general.

We simplify notation for words and write

$$(\binom{a_1}{s_1}, \cdots, \binom{a_n}{s_n}) = a_1^{s_1} \cdots a_n^{s_n}.$$

This notation saves a lot of ink but it can be confusing. In case of ambiguity, mention that you mean a *word* rather than an element in a group.

Let $\to$ be the least relation on A^* such that $uaa^{-1}v \to uv$ and $ua^{-1}av \to uv$ whenever $u, v \in A^*$ and $a \in A$. Define $\twoheadrightarrow$ and $\sim$ and **reduced** as in the diamond lemma with $(A^*, \to)$ instead of $(P, \to)$. So $\twoheadrightarrow$ is the reflexive transitive closure of $\to$ and $\sim$ the equivalence relation generated by $\to$. In the following the term *equivalent* always refers to $\sim$. A word is reduced if and only if it is not of the form $uaa^{-1}v$ or $ua^{-1}av$ for any $u, v \in A^*$, $a \in A$.

Our next aim is to prove confluence as defined in the diamond lemma, lemma 42.

Lemma 48. *Let $u, v, w \in A^*$ be such that $u \to v$ and $u \to w$. Then there exists $x \in A^*$ such that $v \twoheadrightarrow x$ and $w \twoheadrightarrow x$.*

Proof. We say that there is **overlap** if some letter of u is absent in both v and w.

First assume that there is no overlap. Then there are $p, q, r, s, t \in A^*$ such that $u = pqrst$, $v = prst$, $w = pqrt$ and $p \to 1$, $q \to 1$. Then $x = prt$ does it.

Finally assume that there is overlap. If $v = w$ we can put $x = v$ so assume now $v \neq w$. Then there exists $a \in A \times \{-1, 1\}$ and $p, q \in A^*$ such that $u = paa^{-1}aq$ and v (respectively, w) is obtained by removing aa^{-1} (respectively, $a^{-1}a$). But then $v = paq = w$, a contradiction because we could exclude this case. The proof is finished. □

Proposition 49. *Every equivalence class in A^* contains a unique reduced element.*

Proof. Prove yourself that $(A, \to)$ is well-founded as defined in the diamond lemma, lemma 42. It is confluent by lemma 48. The result follows from the diamond lemma, applied to $(A^*, \to)$ instead of $(P, \to)$. □

Definition 50.

(a) For $u \in A^*$ let $R(u)$ denote the unique reduced element in its equivalence class, which we know to exist by proposition 49.

(b) For $u, v \in A^*$ put $u * v = R(uv)$.

(c) Let $F(A)$ denote the set of reduced words in A^*.

Exercise (3.5) Let $u, v \in A^*$. Prove: $R(R(u)\, v) = R(uv) = R(u\, R(v))$.

Proposition 51. *Let A be a set. Then $(F(A), *)$ is a group.*

Proof. Firstly, $F(A)$ contains the empty word (written 1) and is hence not empty, even if A is empty. Secondly, it is clear that $u * 1 = 1 * u = u$ for all $u \in F(A)$.

Prove yourself $u * u^{-1} = u^{-1} * u = 1$ for all $u \in F(A)$ (even though $uu^{-1} \neq 1$).

It remains to prove that the star product is associative. Let $u, v, w \in A^*$. Using the result of exercise (3.5) twice we find

$$\begin{aligned}(u * v) * w &= R((u * v)w) = R(R(uv)w) = R((uv)w) \\ &= R(u(vw)) = R(u\, R(vw)) = R(u(v * w)) = u * (v * w).\end{aligned}$$ □

Exercise (3.6) Consider the map $f\colon A \to F(A)$ defined by $f(a) = (a)$ (a word of one letter). Prove that $(F(A), f)$ satisfies the universal property of definition 44. Same for monoids.

Exercise (3.7) Let A, B be finite sets with $\#A = m$, $\#B = n$. Prove that the abelianisation of $F(A)$ is isomorphic to $\mathbb{Z}^m$. Deduce that $F(A) \ncong F(B)$ if $m \neq n$.

Exercise (3.8) Prove that the coproduct $G * H$ of two groups exists. Use an explicit method similar to the one for semigroups (exercise 2.16), not the general method that applies to all algebraic categories.

Hint: mimic our explicit construction of the free group (proposition 51).

3.3 Congruences and presentations

Definition 52. Let M be a monoid. A **congruence** on M is an equivalence relation $\equiv$ on M such that there exists a (necessarily unique) monoid structure on $M/\equiv$ such that the natural map $M \to (M/\equiv)$ is a monoid homomorphism. The resulting monoid $M/\equiv$ is called the **quotient monoid**.

Exercise (3.9) Let $\equiv$ be an equivalence relation on a monoid M. Prove that $\equiv$ is a congruence on M if and only if $(a \equiv a',\ b \equiv b') \Rightarrow ab \equiv a'b'$ for all $a, a', b, b' \in M$.

Exercise (3.10) Let M be a monoid. Show that the intersection of a family of congruences on M is again a congruence.

Definition 53. Let M be a monoid and $R \subset M \times M$ a relation. The congruence **generated by R** is the intersection of the congruences containing R. Equivalently, it is the least congruence containing R.

Definition 54.

(a) A **monoid presentation** is a pair (A, R) where A is a set and $R \subset A^+ \times A^+$ where A^+ is the free monoid on A. The elements of A are called **letters** or **generators** and those of R **relations** or **relators**.

(b) Associated with a monoid presentation (A, R) it is the **presented monoid** $\langle A \mid R \rangle := A^+/\equiv$ where $\equiv$ is the congruence on A^+ generated by R.

(c) More generally, (A, R) is said to be a **presentation** of any monoid isomorphic to $\langle A \mid R \rangle$.

Exercise (3.11) Prove that every monoid M admits a presentation (A, R). Hint: put $A = M$.

Remark 55. The above results have obvious analogues in all algebraic categories including groups, rings, R-modules, and smurfs.

Let $\equiv$ be a congruence on a group G. Then there exists a (unique) normal subgroup $N \subset G$ such that for all $a, b \in G$ we have $(a \equiv b) \Leftrightarrow (aN = bN)$. We shorten a relation (x, y) to xy^{-1}.

A similar happens for rings. Let $\equiv$ be a congruence on a ring R. Then there exists a (unique) (two-sided) ideal $I \subset R$ such that for all $a, b \in I$ we have $(a \equiv b) \Leftrightarrow (a - b \in I)$. We may shorten a relation (x, y) to $x - y$.

To summarise, for groups and rings, congruences boil down to normal subgroups and ideals.

Example 56. Let $n \in \mathbb{Z}_{\geq 1}$. Then $\langle x \mid x^n \rangle_{\text{group}}$ is a cyclic group of order n. Also $\langle x \mid x^n = 1 \rangle_{\text{monoid}}$ is a cyclic group of order n. But $\langle x \mid x^{n+1} = x \rangle_{\text{monoid}}$ is not a group; it is a monoid of $n + 1$ elements.

3.4 The word problem

There exists a precise definition of **algorithm** but we shall not worry about it. It should suffice to know the following. An algorithm is like a cooking recipy or a computer program. It tells you what to do step by step to obtain a desired result. Carrying it out requires no understanding (computers are dumb). An algorithm runs on an imaginary computer having an infinite amount of memory, but the algorithm should occupy only a finite amount of it.

Let M be a monoid generated by a *finite* set A. Recall that we then have a surjective monoid homomorphism $f\colon M(A) \to M$ where $M(A)$ is the free monoid on A. The **word problem** for (M, A) asks whether there exists an algorithm which on input two elements $u, v \in M(A)$ decides whether or not $f(u) = f(v)$.

A strange but common use of language is that if such an algorithm exists then the word problem for (M, A) is said to be **solvable**. Otherwise it is said to be **unsolvable**.

There exist (explicit) finitely presented monoids with unsolvable word problem.

Again, we have only used monoids as an example here. There is an obvious analogue for all algebraic categories (and far beyond).

In some algebraic categories even some of the free objects have unsolvable word problems, contrary to the free monoids. Still, the word problem for objects in such a category is meaningful and may indeed be solvable for some objects.

A simple, yet nontrivial, example of a word problem is in the free group. It is solvable: this follows immediately from our construction of the free group by reduced words, proposition 51.

3.5 Example: a monoid

Let G be the monoid $\langle a, b, c \mid abc = ac,\ cab = cb\rangle$. We aim to solve the word problem in G by the same method applied before to free groups, involving the diamond lemma.

Put $A = \{a, b, c\}$ and let A^+ be the free monoid on A. Let $f\colon A^+ \to G$ be the natural map.

Note $(cb)c = (cab)c = c(abc) = cac$. Let $\to$ be the least relation on A^+ such that

$$abc \to ac, \qquad cab \to cb, \qquad cbc \to cac \tag{57}$$

and $pxq \to pyq$ whenever $x \to y$ and $p, q \in A^+$.

Exercise (3.12) Prove that $(A^+, \to)$ satisfies the assumptions of the diamond lemma. Why would this be false if $cbc \to cac$ wasn't there in (57)? If it wasn't given, how would you discover that an arrow between cbc, cac is needed in one direction?

Define $\twoheadrightarrow$, $\sim$, **reduced** as in the diamond lemma. For all $u, v \in A^+$, we have $f(u) = f(v)$ if and only if $u \sim v$. The diamond lemma tells us that every $\sim$-class has a unique reduced element. There is an obvious algorithm which on input a word $u \in A^+$ returns the reduced word $R(u)$ equivalent to u: follow the arrows $\to$ until you get stuck. In order to decide whether $u \sim v$ (that is, $f(u) = f(v)$) all you need to do is decide if $R(u) = R(v)$.

The foregoing is an example of a **complete rewriting system** which we shall not define in full generality. Roughly, the three parts of (57) are the **rewriting rules** while **complete** means that the assumptions of the diamond lemma are satisfied.

Exercise (3.13) Apply the methods of this section to the monoid

$$\langle a, b, c \mid abc = ac,\ cba = ba\rangle.$$

Exercise (3.14) In this exercise you find a presentation of the symmetric group. Let F_n be the free monoid on $\{x_1, \ldots, x_n\}$. We agree that $F_n \subset F_{n+1}$ for all n. For $a, b, c \in F_n$ we call b a **subword** of abc.

Write $(x_i, x_j] := x_{i+1}\, x_{i+2} \cdots x_j$ whenever $0 \le i \le j$.

An element of F_{n-1} is said to be **standard** if it belongs to

$$\{x_j(x_i, x_j] \mid 0 \le i < j\} \cup \{x_i\, x_j \mid j - i \ge 2\}.$$

An element of F_{n-1} is called **reduced** if it is of the form

$$(x_{i(n-1)}, x_{n-1}] \cdots (x_{i(1)}, x_1]$$

where $0 \le i(k) \le n-1$ whenever $n-1 \ge k \ge 1$. Clearly there are at most $n!$ reduced words in F_{n-1}.

(a) Let $u \in F_{n-1}$ and assume that u has no standard subword. Prove that u is reduced. Hint: induction on n.

(b) Let $\approx$ be the least relation on F_{n-1} such that

$$\begin{aligned} x_i\, x_j\, x_i &\approx x_j\, x_i\, x_j && \text{if } j - i = 1 \\ x_i\, x_j &\approx x_j\, x_i && \text{if } j - i \ge 2 \\ x_i^2 &\approx 1 && \text{for all } i. \end{aligned}$$

Let $\equiv$ be the congruence on F_{n-1} generated by $\approx$. For each *standard* word u find an explicit reduced word $R(u)$ such that $u \equiv R(u)$ and prove your claim. ($R(u)$ is unique but you don't need to prove that here).

(c) Let $\to$ be the least relation on F_{n-1} such that $u \to R(u)$ for all standard u, and $(x \to y) \Rightarrow (axb \to ayb)$ for all $a, b, x, y \in F_{n-1}$. Prove that $\to$ is well-founded.

(d) Prove that $F_{n-1}/\equiv$ has at most $n!$ elements.

(e) Let p: $F_{n-1} \to S_n$ be the monoid homomorphism defined by $p(x_i) = (i, i+1)$. Let $\sim$ be the congruence on F_{n-1} defined by $x \sim y$ if and only if $p(x) = p(y)$. Prove: $\equiv \subset \sim$.

(f) Without proof you may assume that p is surjective. Prove $\equiv = \sim$. Prove that $(F_{n-1}/\equiv) \cong S_n$. This is called the **Coxeter presentation** of S_n. Hint: no calculations are needed.

(g) Prove that $\to$ is confluent as defined in the diamond lemma. Hint: no calculations are needed (fortunately). Instead combine the foregoing parts.

3.6 $*$ A diamond lemma for rings

For the academic year 2013-2014 we skip this section.

Without proof we state a diamond lemma for rings. It is not obviously a consequence for the original diamond lemma (lemma 42) but comes close.

Let A^+ be the free monoid on a set A. Let K be a commutative ring and $K\langle A\rangle = KA^+$ the 'monoid ring': it is a free K-module on with basis A^+ and the product of two basis elements is the same in both A^+ and $K\langle A\rangle$. Elements of A^+ are called **monomials**.

Let $R \subset A^+ \times K\langle A\rangle$. Let $\to$ be the least relation on $K\langle A\rangle$ such that

$$y + \lambda abc \to y + \lambda axc$$

whenever $(b, x) \in R$, $\lambda \in K$, $a, b, c \in A^+$, and ***abc* does not appear in *y***, that is, y is a K-linear combination of monomials other than abc. An element $x \in K\langle A\rangle$ is said to be **reduced** if $x \to y$ for no $y \in K\langle A\rangle$.

Let $\leq$ be a relation on A^+ satisfying the following:

- Suppose $\leq$ is a **monoid ordering** on A^+, that is, an ordering such that if $a, b, x, y \in A^+$ and $x \leq y$ then $axb \leq ayb$.
- Assume further that there is no infinite **falling chain** $a_0 > a_1 > \cdots$ with $a_i \in A^+$ for all i.
- Suppose that the ordering $\leq$ on A^+ is **compatible with *R***, that is, if $(a, x) \in R$ then x is a linear combination of monomials less than a.

Exercise (3.15) Prove that there exists no infinite sequence $x_0 \to x_1 \to \cdots$ with $x_i \in K\langle A\rangle$ for all i.

Let $\twoheadrightarrow$ be the reflexive transitive closure of $\to$. Clearly, $\twoheadrightarrow$ is an ordering.

Let I be the ideal of $K\langle A\rangle$ generated by $\{a - x \mid (a, x) \in R\}$. We write $x \sim y$ if $x, y \in K\langle A\rangle$ and $x - y \in I$.

Assume finally the following variation of **confluence**:

- Let $a \in A^+$ and $v, w \in K\langle A\rangle$ be such that $a \to v$ and $a \to w$. Then there exists $x \in K\langle A\rangle$ such that $v \twoheadrightarrow x$ and $w \twoheadrightarrow x$. (58)

Theorem 59: Diamond lemma for rings. *We use the above notation and assumptions. Then for all $x \in K\langle A\rangle$ there is a unique reduced element $R(x) \in K\langle A\rangle$ equivalent to x.* □

It follows that the quotient ring $K\langle A\rangle/I$ is isomorphic to the set T of reduced elements of $K\langle A\rangle$ on which multiplication $*$ is defined by $x * y := R(xy)$. Moreover $\sim$ is the equivalence relation generated by $\to$. Also note that T is a free K-module with the reduced monomials for basis. It is common to call $\{a - x \mid (a,x) \in R\}$ a **Gröbner basis** of I.

Example: Poincaré-Birkhoff-Witt

We turn to an example illustrating the use of the diamond lemma for rings.

Let K be a commutative ring. A **Lie algebra** over K is a K-module L along with a K-bilinear map $L \times L \to L$: $(a,b) \mapsto [a,b]$ such that $[a,a] = 0$ for all $a \in L$ and satisfying the **Jacobi identity**

$$[a,[b,c]] + [b,[c,a]] + [c,[a,b]] = 0 \quad \text{for all } a,b,c \in L.$$

Recall that a ***K*-algebra** S is a ring equipped with a ring homomorphism $K \to S$.

Exercise (3.16) Let S be a K-algebra and put $[x,y] := xy - yx$ for all $x,y \in S$. Prove that $(S,[\cdot,\cdot])$ is a Lie algebra.

Fix a Lie algebra L over K. Assume that L is a free K-module with basis A. Choose a total ordering $<$ on A.

The **enveloping algebra** $U = U(L)$ of L is by definition presented as K-algebra by generators A and relations $xy - yx = [x,y]$ for all $x,y \in A$ (we agree that $[x,y]$ is expressed as a linear combination in the A so that the relations make sense).

Theorem 60: Poincaré-Birkhoff-Witt. *Use the above notation. The enveloping algebra $U(L)$ admits a K-basis*

$$\Big\{ a_1 \cdots a_n \;\Big|\; n \geq 0,\ \ a_i \in A \ \textit{ for all } i,\ \ a_i \leq a_{i+1} \ \textit{ for all } i \Big\}.$$

Proof. The proof is an application of the diamond lemma for rings (theorem 59).

Put

$$R = \Big\{ (yx, xy - [x,y]) \;\Big|\; x,y \in A,\ x < y \Big\}.$$

Let $a_i, \ldots, a_n \in A$ and $x = a_1 \cdots a_n$. So $x \in A^+$. In this case we write $\ell(x) = n$. This is called the length of x. Define the misordering index $m(x)$ of x to be the number of pairs (i,j) such that $1 \leq i < j \leq n$ but $a_i > a_j$.

Let $\leq$ be the ordering on A^+ defined by:

$$x > y \quad \Leftrightarrow \quad \Big[\ell(x) > \ell(y) \ \text{ or } \ \big[\ell(x) = \ell(y) \ \text{ and } \ m(x) > m(y) \big] \Big].$$

Prove yourself that $\leq$ is a monoid ordering on A compatible with R and without infinite falling chains. In order for theorem 59 to apply it remains to prove (58) which is also left as an exercise.

Application of the diamond lemma for rings shows that the set of reduced monomials is a basis for $U(L)$. The result follows. □

Exercise (3.17) Let K be a field of characteristic $p > 2$. Let T be the K-algebra presented by generators x,y,z and relations

$$[x,y] = x, \quad [y,z] = -z, \quad [x,z] = x^2/2, \quad x^p = 0, \quad y^p = y, \quad z^p = 0.$$

Prove that T has dimension p^3 with basis $\big\{ x^a\, y^b\, z^c \;\big|\; a,b,c \in \{0,1,\ldots,p-1\} \big\}$.

Hint: first find a formula for the nth power of the derivation of $K[x]$ taking x to $x^2/2$. Here derivation means a K-linear map D: $K[x] \to K[x]$ such that $D(ab) = a(Db) + (Da)b$ for all a,b.

4 Tensor products

4.1 Tensor products

Let R be a ring, not necessarily with 1.

Definition 61. A **left R-module** is an abelian group V (written additively) along with a map $R \times V \to V$: $(a, x) \mapsto ax$ such that

- We have $(ab)x = a(bx)$ for all $a, b \in R$ and $x \in V$.
- If R has 1 then $1x = x$ for all $x \in V$.
- We have $a(x + y) = ax + ay$ for all $a \in R$, $x, y \in V$.
- We have $(a + b)x = ax + bx$ for all $a, b \in R$, $x \in V$.

A **right R-module** is an abelian group V (written additively) along with a map $V \times R \to V$: $(x, a) \mapsto xa$ such that

- We have $x(ab) = (xa)b$ for all $a, b \in R$ and $x \in V$.
- If R has 1 then $x1 = x$ for all $x \in V$.
- We have $(x + y)a = xa + ya$ for all $a \in R$, $x, y \in V$.
- We have $x(a + b) = xa + xb$ for all $a, b \in R$, $x \in V$.

Remark 62. Let R be a commutative ring and V a left R-module. Then we can turn V into a right R-module by defining $xa := ax$ for all $a \in R$, $x \in V$. This doesn't work if R is not commutative.

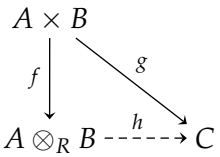
Exercise (4.1) Define the opposite R^{op} of a ring R. Prove that R^{op} is again a ring. Prove that a left R-module is 'the same' as a right R^{op}-module. Find an example of a ring R such that every left R-module is free but some right R-module is not.

Definition 63. Let A be a right R-module and B a left R-module. Let C be a $\mathbb{Z}$-module. A map $f\colon A \times B \to C$ is called **middle linear** if

$$\begin{aligned} f(a + a', b) &= f(a, b) + f(a', b) && \text{for all } \ a, a' \in A, \ \ b \in B \\ f(a, b + b') &= f(a, b) + f(a, b') && \text{for all } \ a \in A, \ \ b, b' \in B \\ f(ar, b) &= f(a, rb) && \text{for all } \ a \in A, \ \ r \in R, \ \ b \in B. \end{aligned}$$

Definition 64. Let A be a right R-module and B a left R-module. A **tensor product (of A, B over R)** consists of a $\mathbb{Z}$-module $A \otimes_R B$ and a middle linear map $f\colon A \times B \to A \otimes_R B$ such that, if C is a $\mathbb{Z}$-module and $g\colon A \times B \to C$ is middle linear then there exists a unique $\mathbb{Z}$-linear $h\colon A \otimes_R B \to C$ such that $g = hf$.

Usually we write $a \otimes b$ instead of $f(a, b)$.



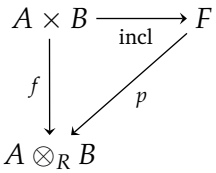
Exercise (4.2) (Uniqueness of tensor products). Let A be a right R-module and B a left R-module. Assume that (T, f) and (U, g) are two tensor products. Prove that there exists a unique isomorphism of $\mathbb{Z}$-modules $h\colon T \to U$ such that $g = hf$.

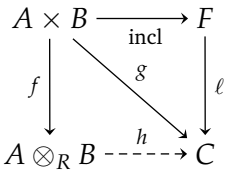
Proposition 65. *Let A be a right R-module and B a left R-module. Then there exists a tensor product $f\colon A \times B \to A \otimes_R B$.*

Proof. Let F be a free $\mathbb{Z}$-module with basis $A \times B$. Let $K \subset F$ be the $\mathbb{Z}$-submodule generated by X where

$$\begin{aligned} X = &\big\{(a+a',b)-(a,b)-(a',b) \;\big|\; a,a' \in A,\;\; b \in B\big\} \\ &\cup \big\{(a,b+b')-(a,b)-(a,b') \;\big|\; a \in A,\;\; b,b' \in B\big\} \\ &\cup \big\{(ar,b)-(a,rb) \;\big|\; a \in A,\;\; r \in R,\;\; b \in B\big\}. \end{aligned}$$

We put $A \otimes_R B = F/K$. Let $p\colon F \to F/K$ be the natural map: $p(x) = x + K$. We define $f\colon A \times B \to A \otimes_R B$ by $f(a,b) = p(a,b) = (a,b) + K$.





We claim that $f\colon A \times B \to A \otimes_R B$ is a tensor product. It is clear that $A \otimes_R B$ is a $\mathbb{Z}$-module and that f is middle linear.

In order to prove that the universal property is satisfied, assume that C is a $\mathbb{Z}$-module and $g\colon A \times B \to C$ middle linear. We must prove that there exists a unique $\mathbb{Z}$-linear map $h\colon A \otimes_R B \to C$ such that $g = hf$.

Proof of uniqueness. This follows immediately from the fact that $A \otimes_R B$ is generated as $\mathbb{Z}$-module by the image of f, and that h is $\mathbb{Z}$-linear.

Proof of existence. Let $\ell\colon F \to C$ be the $\mathbb{Z}$-linear map defined by $\ell(a,b) = g(a,b)$ for all $(a,b) \in A \times B$. Then $K \subset \ker(\ell)$ because g is middle linear. So $\ker(p) \subset \ker(\ell)$. So there exists a unique $\mathbb{Z}$-linear map $h\colon A \otimes_R B \to C$ such that $\ell = hp$. But then $g = hf$ as required. □

Not every element of $A \otimes_R B$ is of the form $a \otimes b$. But every element of $A \otimes_R B$ can be written as a finite sum $\sum_i a_i \otimes b_i$ where $(a_i, b_i) \in A \times B$.

Exercise (4.3) Using only the universal property, prove that $A \otimes_R B$ is generated as $\mathbb{Z}$-module by $\{a \otimes b \mid (a,b) \in A \times B\}$.

The following identities are immediate from the definition:

$$\begin{aligned} (a+a') \otimes b &= a \otimes b + a' \otimes b && \text{for all } a,a' \in A,\;\; b \in B \\ a \otimes (b+b') &= a \otimes b + a \otimes b' && \text{for all } a \in A,\;\; b,b' \in B \\ ar \otimes b &= a \otimes rb && \text{for all } a \in A,\;\; r \in R,\;\; b,b' \in B. \end{aligned}$$

Example 66. Let $n > 0$. Prove: $(\mathbb{Z}/n\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q} = 0$.

Solution. Let $a \in \mathbb{Z}/n\mathbb{Z}$ and $b \in \mathbb{Q}$. Then

$$a \otimes b = a \otimes n(\frac{b}{n}) = (an) \otimes \frac{b}{n} = 0 \otimes \frac{b}{n} = 0. \qquad \square$$

Example 67. Most of the time tensor products are handled by their universal property. Here is a simple typical example.

Let A, B be $\mathbb{Z}$-modules and $p\colon A \to \mathbb{Z}$, $q\colon B \to \mathbb{Z}$ homomorphisms of $\mathbb{Z}$-modules. Prove that there exists a unique linear map $h\colon A \otimes_{\mathbb{Z}} B \to \mathbb{Z}$ such that

$$h(a \otimes b) = (pa)(qb) \;\text{ for all } (a,b) \in A \times B.$$

Solution. Define $g\colon A \times B \to \mathbb{Z}$ by $g(a,b) = (pa)(qb)$. We claim that g is middle linear. Indeed, for $a, a' \in A$, $b \in B$, $r \in \mathbb{Z}$

$$\begin{aligned} g(a+a',b) &= p(a+a')\,q(b) = (pa+pa')(qb) \\ &= (pa)(qb) + (pa')(qb) = g(a,b) + g(a',b) \\ g(ar,b) &= (p(ar))(qb) = ((pa)r)(qb) \\ &= (pa)(r(qb)) = (pa)(q(rb)) = g(a,rb). \end{aligned}$$

The remaining case is similar. This proves that g is middle linear. By the universal property of tensor products there is a unique $\mathbb{Z}$-linear $h\colon A \otimes B \to \mathbb{Z}$ such that $h(a \otimes b) = g(a,b) = (pa)(qb)$. □

Exercise (4.4) Let R be a unital ring and A a unital left R-module. Prove that there exists an isomorphism of unital left R-modules $A \to R \otimes_R A$ defined by $a \mapsto 1 \otimes a$.

4.2 Extended tensor products

Definition 68. Let R, S be rings. An (R,S)-bimodule is a set A which is at the same time a left R-module and a right S-module such that addition in V is the same both times and $r(as) = (ra)s$ for all $r \in R$, $a \in A$, $s \in S$. We simply write ras for this.

Let A be a module over a commutative ring R. Then we can consider A as an (R,R)-bimodule (and will do so tacitly) by putting $ras = (rs)a$ for all $r, s \in R$ and $a \in A$.

Proposition 69. *Let A be an (S,R)-bimodule and B an (R,T)-bimodule.*

(a) *Let $s \in S$, $t \in T$. Then there exists a $\mathbb{Z}$-linear map $A \otimes_R B \to A \otimes_R B$ taking $a \otimes b$ to $(sa) \otimes (bt)$ for all $(a,b) \in A \times B$.*

(b) *The $\mathbb{Z}$-module $A \otimes_R B$ becomes an (S,T)-bimodule by putting $s(a \otimes b)t = (sa) \otimes (bt)$ for all $s \in S$, $(a,b) \in A \times B$, $t \in T$.*

(c) *Let R be a commutative ring and A, B be R-modules. Then $A \otimes_R B$ becomes an R-module by putting $r(a \otimes b) = (ra) \otimes b$ for all $r \in R$, $(a,b) \in A \times B$.*

Proof. (a). Consider the map $g\colon A \times B \to A \otimes_R B\colon (a,b) \mapsto (sa) \otimes (bt)$. Prove yourself that g is middle linear. Therefore there exists $\mathbb{Z}$-linear $h\colon A \otimes_R B \to A \otimes_R B$ such that $g = hf$, that is, $(sa) \otimes (bt) = h(a \otimes b)$.

(b). Easy exercise.

(c). Regard A, B as (R,R)-bimodules and apply (b). □

Definition 70. Let A be an (S,R)-bimodule and B an (R,T)-bimodule.

(a) A map $f\colon A \times B \to C$ is **extended middle linear** if it is middle linear and $f(sa,bt) = s\,f(a,b)\,t$ for all $s \in S$, $(a,b) \in A \times B$, $t \in T$.

(b) An **extended tensor product (for A, B, R, S, T)** is an (S,T)-bimodule U and an extended middle linear map $f\colon A \times B \to U$ such that if C is an (S,T)-bimodule and $g\colon A \times B \to C$ is extended middle linear then there exists a unique homomorphism $h\colon U \to C$ of (S,T)-bimodules such that $g = hf$.

Exercise (4.5) Let A be an (S,R)-bimodule and B an (R,T)-bimodule. Let $f\colon A \times B \to A \otimes_R B$ be their tensor product (here we ignore S, T). Make $A \otimes_R B$ into an (S,T)-bimodule as in proposition 69(b). Prove that f is an extended tensor product as well.

Proposition 71. *Let K be a field. Let U be a vector space over K with basis $(u_i \mid i \in I)$ and V with basis $(v_j \mid j \in J)$. Recall that by proposition 69(c) $U \otimes_K V$ is again a vector space over K. Then $U \otimes_K V$ has the basis $(u_i \otimes v_j \mid (i,j) \in I \times J)$.*

Proof. Let W be a vector space with basis $I \times J$. Define $f\colon U \times V \to W$ by

$$f(\sum_i a_i u_i, \sum_j b_j v_j) = \sum_{ij} a_i b_j (i,j).$$

We must prove that (W, f) is an extended tensor product (equivalently, that it's a tensor product but that's slightly harder). Let X be a vector space and $g\colon U \times V \to X$ be extended middle linear. We must prove that there exists a unique K-linear $h\colon W \to X$ such that $g = hf$.

Proof of existence. Define $h(i,j) = g(u_i, v_j)$ for all $(i,j) \in I \times J$ and extend by linearity. Let $a_i, b_j \in K$ for all i, j. Then

$$\begin{aligned} hf(\sum_i a_i u_i, \sum_j b_j v_j) = h \sum_{ij} a_i b_j (i,j) &= \sum_{ij} a_i b_j g(u_i, v_j) \\ &= \sum_{ij} g(a_i u_i, b_j v_j) = g(\sum_i a_i u_i, \sum_j b_j v_j) \end{aligned}$$

as promised.

Proof of uniqueness. Note that W is spanned by $I \times J$. Since h is linear, it is determined as soon as $h(i,j)$ is for all $(i,j) \in I \times J$. But $h(i,j) = hf(u_i, v_j) = g(u_i, v_j)$. □

Let R, S be rings and $p\colon R \to S$ a ring homomorphism. We make S into an (S,R)-bimodule by putting $sxr = s * x * (pr)$ where $*$ denotes multiplication in S. If moreover A is a left R-module then $S \otimes_R A$ is a left S-module by proposition 69(b). This is known as **extension of scalars** or **base change**.

Exercise (4.6) Let A, B be modules over a commutative ring R. Prove that there exists an isomorphism $A \otimes_R B \to B \otimes_R A$ given by $a \otimes b \mapsto b \otimes a$.

Exercise (4.7) Prove $(A \oplus B) \otimes C \cong A \otimes C \oplus B \otimes C$ whenever A, B are right R-modules and C is a left R-module.

4.3 Products of categories

Let C, D be categories. The **product** $C \times D = E$ is defined to be the following category. We put $\mathrm{Ob}(E) = \mathrm{Ob}(C) \times \mathrm{Ob}(D)$ (cartesian product). Moreover $E((U,V),(W,X)) = C(U,W) \times D(V,X)$ (cartesian product). Composition of morphisms is defined by

$$(p,q)(r,s) = \begin{cases} (pr, qs) & \text{if } pr, qs \text{ are defined,} \\ \text{undefined} & \text{otherwise.} \end{cases}$$

Likewise for products of more than two categories.

4.4 Functoriality

Let ${}_R\mathbf{Mod}$ denote the category of left R-modules and their homomorphisms. Likewise for $\mathbf{Mod}_S$ and ${}_R\mathbf{Mod}_S$.

Sometimes we write A_R and ${}_RB$ and ${}_RC_S$ if A is a right R-module, B is a left R-module and C is an (R,S)-bimodule.

Fix rings R, S, T. Recall products of categories from section 4.3. We shall define a functor

$$F\colon {}_S\mathbf{Mod}_R \times {}_R\mathbf{Mod}_T \to {}_S\mathbf{Mod}_T. \tag{72}$$

On objects we put $F(A,B) = A \otimes_R B$. Then $F(A,B)$ is an (S,T)-bimodule by exercise 4.5.

Let $(p,q)\colon (A,B) \to (A',B')$ be a morphism in ${}_S\mathbf{Mod}_R \times {}_R\mathbf{Mod}_T$. Recall that this just means that $p\colon A \to A'$ and $q\colon B \to B'$ are homomorphisms.

Define $g\colon A \times B \to A' \otimes_R B'$ by $g(a,b) = (pa) \otimes (qb)$. We claim that g is extended middle linear. Here is one part of the proof:

$$\begin{aligned} g(a+a',b) &= (p(a+a')) \otimes (qb) = (pa+pa') \otimes (qb) \\ &= (pa) \otimes (qb) + (pa') \otimes (qb) = g(a,b) + g(a',b). \end{aligned}$$

Prove the remaining parts yourself.

Since $A \otimes_R B$ is an extended tensor product by exercise 4.5, there exists a unique (S,T)-linear $h\colon A \otimes_R B \to A' \otimes_R B'$ such that $g = hf$. We put $F(p,q) := h$ which is also often written $p \otimes q$. So $(p \otimes q)(a \otimes b) = pa \otimes qb$ for all $(a,b) \in A \times B$.

Exercise (4.8) Prove $(p \otimes q)(r \otimes s) = pr \otimes qs$ for all morphisms $(p,q),(r,s)$ of ${}_S\mathbf{Mod}_R \times {}_R\mathbf{Mod}_T$. Finish the proof that F is a functor.

Exercise (4.9) Let R, S be rings and $p\colon R \to S$ a ring homomorphism. Make extension of scalars into a functor ${}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$.

4.5 Homsets of modules

A close cousin to the tensor product is obtained from homsets. Let R, S, T be rings. There are functors

$$G\colon ({}_R\mathbf{Mod}_S)^{\mathrm{op}} \times {}_R\mathbf{Mod}_T \to {}_S\mathbf{Mod}_T \qquad H\colon ({}_T\mathbf{Mod}_R)^{\mathrm{op}} \times {}_S\mathbf{Mod}_R \to {}_S\mathbf{Mod}_T.$$

Let's define H. On objects $H(A,B) = \mathbf{Mod}_R(A,B)$, the set of homomorphisms of right R-modules $A \to B$.

Exercise (4.10)

(a) Make $H(A,B)$ into a $\mathbb{Z}$-module.

(b) Make $H(A,B)$ into an (S,T)-bimodule.

Let $(f,g)\colon (A,B) \to (A',B')$ be a morphism in $({}_T\mathbf{Mod}_R)^{\mathrm{op}} \times {}_S\mathbf{Mod}_R$. That is,

$$f \in {}_T\mathbf{Mod}_R(A',A), \qquad g \in {}_S\mathbf{Mod}_R(B,B').$$

We must define a morphism $h = H(f,g)\colon H(A,B) \to H(A',B')$, that is,

$$h\colon \mathbf{Mod}_R(A,B) \to \mathbf{Mod}_R(A',B').$$

So let $p \in \mathbf{Mod}_R(A,B)$. We define $hp := gpf \in \mathbf{Mod}_R(A',B')$:

$$A' \xrightarrow{f} A \xrightarrow{p} B \xrightarrow{g} B'.$$

Exercise (4.11)

(a) Prove that $H(f,g)$ is a homomorphism of (S,T)-bimodules.

(b) Prove that H is a functor.

4.6 Tensor products and adjoint functors

Proposition 73. *Let $A \in \mathrm{Ob}(\mathbf{Mod}_R)$, $B \in \mathrm{Ob}({}_S\mathbf{Mod}_R)$, $C \in \mathrm{Ob}(\mathbf{Mod}_S)$. This proposition is about an isomorphism of right S-modules*

$$\mathrm{Hom}_S(A \otimes_R B, C) \cong \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C)).$$

(More about it will be proved in proposition 77).

(a) *The set $D := \mathrm{Hom}_S(B, C)$ becomes an object in $\mathbf{Mod}_R$ by putting $(fr)x = f(rx)$ and $(f+g)x = fx + gx$ for all $f, g \in D$, $r \in R$, $x \in B$.*

(b) *Also $P := \mathrm{Hom}_S(A \otimes_R B, C)$ and $Q := \mathrm{Hom}_R(A, D)$ are objects in $\mathbf{Mod}_S$.*

(c) *There is an isomorphism of right S-modules $\lambda\colon F \to G$ with inverse ϕ defined by*

$$((\lambda f)a)b := f(a \otimes b), \qquad (\phi g)(a \otimes b) := (ga)b. \tag{74}$$

Proof. (a). For $f \in D$, $r, s \in R$, $x \in B$ we have

$$((fr)s)x = (fr)(sx) = f(r(sx)) = f((rs)x) = (f(rs))x$$

which shows $(fr)s = f(rs)$ as required. Prove $(f+g)r = fr + gr$ yourself.

(b). Exercise.

(c). Define λ and ϕ by (74). First we prove that ϕ is well-defined. Fix $g \in Q$. Define $\ell\colon A \times B \to C$ by $\ell(a, b) = (ga)b$. We claim that ℓ is extended middle linear. Here is part of the proof. Let $(a, b) \in A \times B$, $r \in R$. Then

$$\begin{aligned}
\ell(ar, b) &= (g(ar))b && \text{by definition of } \ell \\
&= ((ga)r)b && \text{because } g \in \mathrm{Mor}(\mathbf{Mod}_R) \\
&= (ga)(rb) && \text{by the definition of } D \text{ as } R\text{-module} \\
&= \ell(a, rb) && \text{by definition of } \ell.
\end{aligned}$$

Prove the other parts yourself. So ℓ is extended middle linear. So there exists a unique S-linear $h\colon A \otimes_R B \to C$ such that $h(a \otimes b) = (ga)b$ for all $(a, b) \in A \times B$. Then $\phi g = h$ and hence ϕ is well-defined.

Prove yourself that λ and ϕ are S-linear.

Finally we prove that λ and ϕ are mutual inverses:

$$\begin{aligned}
((\lambda\phi g)a)b &= (\phi g)(a \otimes b) = (ga)b \\
(\phi\lambda f)(a \otimes b) &= ((\lambda f)a)b = f(a \otimes b).
\end{aligned}$$

□

Example 75. Let C be a category. We shall construct a functor

$$F = C(-,-)\colon C^{\mathrm{op}} \times C \to \mathbf{Sets}.$$

On objects $F(U, V) = C(U, V)$. Let $(p, q)\colon (U, V) \to (W, X)$ be a morphism. This just means $p \in C(W, U)$ and $q \in C(V, X)$. All categories are on the right. We put $h(F(p, q)) = phq$ for all $h \in C(U, V)$. Prove yourself that this makes F into a functor.

Definition 76. Let C, D be categories and let $F\colon C \to D$ and $G\colon D \to C$ be functors. We say that (F, G) is an **adjoint pair** and F is **left adjoint** to G and G is **right adjoint** to F if there exists a **natural isomorphism**

$$\alpha\colon C(U, G(V)) \to D(F(U), V)$$

which means the following:

- A bijection $\alpha_{U,V}$: $C(U, G(V)) \to D(F(U), V)$ is given whenever $U \in \mathrm{Ob}(C)$ and $V \in \mathrm{Ob}(D)$.
- If U is fixed then $\alpha_{U,-}$ is a natural transformation $C(U, G(-)) \to D(F(U), -)$ (note that both are functors $D \to$ **Sets**).
- If V is fixed then $\alpha_{-,V}$ is a natural transformation $C(-, G(V)) \to D(F(-), V)$ (note that both are functors $C^{\mathrm{op}} \to$ **Sets**).

Another way to say that (F, G) is an adjoint pair is that the functors P, Q defined below are naturally isomorphic. Use the same notation as above. Define the functors P, Q: $C^{\mathrm{op}} \times D \to$ **Sets** as follows. On objects, $P(U, V) = C(U, G(V))$ and $Q(U, V) = D(F(U), V)$. Moreover (respectively) P, Q are compositions of (respectively) G, F and the functor from example 75.

Proposition 77. *Let R, S be rings and fix $B \in \mathrm{Ob}({}_S\mathbf{Mod}_R)$. Recall the isomorphisms*

$$\alpha_{A,C}\colon \mathrm{Hom}_S(A \otimes_R B, C) \to \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C))$$

from proposition 73. These combine into a natural isomorphism α. In other words, there is an adjoint pair (F, G) given by

$$F = - \otimes B\colon \mathbf{Mod}_R \to \mathbf{Mod}_S \qquad G = \mathrm{Hom}_R(B, -)\colon \mathbf{Mod}_S \to \mathbf{Mod}_R.$$

Proof. Due to proposition 73 all that remains to be proved is that for A (respectively, C) fixed α_{A-} (respectively, α_{-C}) is a natural transformation. Do this yourself. □

Example 78. Let F: **Sets** $\to$ **Groups** be defined by $X \mapsto F(X)$ (the free group) and G: **Groups** $\to$ **Sets** the forgetful functor. Then (F, G) is an adjoint pair.

Exercise (4.12) Prove that left adjoint functors preserve coproducts.

Exercise (4.13) Let F: **Groups** $\to$ **Ab** be the abelianisation functor (exercise 2.28). Let G: **Ab** $\to$ **Groups** be the inclusion. Prove that (F, G) is an adjoint pair.

Exercise (4.14) Let A, B be sets and $R \subset A \times B$ a relation. Let P: **Sets** $\to$ **Sets** be the powerset functor. Then $P(A), P(B)$ are ordered by inclusion. We view $P(A)$ and $P(B)$ as categories. Define f: $P(A) \to P(B)^{\mathrm{op}}$ and g: $P(B)^{\mathrm{op}} \to P(A)$ by

$$f(X) = \{y \in B \mid xRy \text{ for all } x \in X\}$$
$$g(Y) = \{x \in A \mid xRy \text{ for all } y \in Y\}.$$

(a) Prove that (f, g) is an adjoint pair.
(b) Prove $fgf = f$.
(c) Find an adjoint pair (F, G) where $FGF \neq F$.

Exercise (4.15) Let C be a category. Let F: $C \to C \times C$ be the diagonal functor, defined by $F(A) = (A, A)$ whenever A is an object or morphism in C. Prove that F has a right adjoint G if and only if C admits finite products. Moreover, if it has, then $G(V, W)$ is a product of V, W.

4.7 Tensor products of algebras

Proposition 79. *Let A be a right R-module, B an (R, S)-bimodule, and C a left S-module. Then there exists an isomorphism*

$$(A \otimes_R B) \otimes_S C \to A \otimes_R (B \otimes_S C)\colon\ (a \otimes b) \otimes c \mapsto a \otimes (b \otimes c).$$

Proof. Fix $c \in C$. Define $g\colon A \times B \to A \otimes_R (B \otimes_S C)$ by $g(a,b) = a \otimes (b \otimes c)$. It is easy to see that g is middle linear. So there exists $h\colon A \otimes_R B \to A \otimes_R (B \otimes_S C)$ defined by $h(a \otimes b) = a \otimes (b \otimes c)$.

This gives us a map $f\colon (A \otimes_R B) \times C \to A \otimes_R (B \otimes_S C)$ taking $(a \otimes b, c)$ to $a \otimes (b \otimes c)$. Prove yourself that f is middle linear. So there exists a $\mathbb{Z}$-linear map $\ell\colon (A \otimes_R B) \otimes_S C \to A \otimes_R (B \otimes_S C)$ taking $(a \otimes b) \otimes c$ to $a \otimes (b \otimes c)$.

Likewise there exists a $\mathbb{Z}$-linear map $m\colon A \otimes_R (B \otimes_S C) \to (A \otimes_R B) \otimes_S C$ taking $a \otimes (b \otimes c)$ to $(a \otimes b) \otimes c$. Clearly ℓ and m are inverses to each other. □

Remark 80. A priori a **multiple tensor product**

$$A_1 \otimes \cdots \otimes A_n$$

is only defined if brackets have been inserted, for example $(A_1 \otimes (A_2 \otimes A_3)) \otimes A_4$. Proposition 79 however allows us to omit the brackets. Likewise for elements of the form $a_1 \otimes \cdots \otimes a_n \in A_1 \otimes \cdots \otimes A_n$.

Exercise (4.16) In this exercise all modules and tensor products are over a commutative ring R. Since brackets can be omitted there must be such a thing as a universal property for $A_1 \otimes \cdots \otimes A_n$. Find it. Note that middle linear should be replaced by multilinear. A map $f\colon A_1 \times \cdots \times A_n \to C$ is called **multilinear** if f is linear in any component when the others are fixed.

Definition 81. Let R be a ring. An ***R*-algebra** consists of a ring A and a ring homomorphism $p\colon R \to A$.

Proposition 82. *Let R be a unital commutative ring. All our modules, multilinear maps and tensor products are over R. Let $p\colon R \to A$ and $q\colon R \to B$ be unital R-algebras. Then $C := A \otimes B$ becomes a unital ring by putting $(a \otimes b)(a' \otimes b') := aa' \otimes bb'$. We have a unital ring homomorphism $r\colon R \to C$ defined by $rx = px \otimes 1$. So C is an R-algebra.*

Proof. Define $g\colon A \times B \times A \times B \to C$ by $g(a,b,a',b') = aa' \otimes bb'$. Prove yourself that g is multilinear. By the universal property of multiple tensor products (exercise 4.16) there exists a unique linear $h\colon A \otimes B \otimes A \otimes B = C \otimes C \to C$ such that $h(a \otimes b \otimes a' \otimes b') = aa' \otimes bb'$ for all $a, a' \in A$, $b, b' \in B$. In particular, there exists a unique bilinear map $m\colon C \times C \to C\colon (a \otimes b, a' \otimes b') \mapsto aa' \otimes bb'$.

That m is associative is proved as follows:

$$\begin{aligned}((a \otimes b)(c \otimes d))(e \otimes f) &= (ac \otimes bd)(e \otimes f) = (ac)e \otimes (bd)f \\ &= a(ce) \otimes b(df) = (a \otimes b)(ce \otimes df) = (a \otimes b)((c \otimes d)(e \otimes f)).\end{aligned}$$

This proves that C is a ring. Clearly $1 \otimes 1$ is a unit in C.

It remains to prove that $r\colon R \to C$ is a unital ring homomorphism. Well, $r1 = 1 \otimes 1$ and

$$\begin{aligned}r(x+y) &= p(x+y) \otimes 1 = (px+py) \otimes 1 = px \otimes 1 + py \otimes 1 = rx + ry \\ r(xy) &= p(xy) \otimes 1 = (px)(py) \otimes 1 = (px \otimes 1)(py \otimes 1) = (rx)(ry).\end{aligned}$$ □

Exercise (4.17) Let R be a commutative ring. Prove $R[x] \otimes_R R[y] \cong R[x,y]$.

Exercise (4.18) Let A, B be modules over a commmutative ring R. Let $\mathrm{End}(A)$ be the ring of endomorphisms of A as R-module. We make $\mathrm{End}(A)$ into an R-algebra by equipping it with the ring homomorphism $p\colon R \to \mathrm{End}(A)$, $(px)y = xy$ for all $(x,y) \in R \times A$. Prove $\mathrm{End}(A \otimes_R B) \cong \mathrm{End}(A) \otimes_R \mathrm{End}(B)$ as R-algebras.

4.8 Tensor algebras

Let R be a unital commutative ring. All modules, multilinear maps and tensor products are over R.

Let M be an R-module. For $k \geq 0$ we put $T^k(M) = M \otimes \cdots \otimes M$ (k factors). For $k = 0$ this means by definition $T^0(M) = R$.

Put

$$T(M) = \bigoplus_{k \geq 0} T^k(M).$$

By remark 80 there exists a unique bilinear map $T^k(M) \times T^\ell(M) \to T^{k+\ell}(M)$ such that

$$(a_1 \otimes \cdots \otimes a_k, a_{k+1} \otimes \cdots \otimes a_{k+\ell}) \mapsto a_1 \otimes \cdots \otimes a_{k+\ell}$$

whenever $a_i \in M$ for all i. This map is written $(a,b) \mapsto a \otimes b$ or simply $(a,b) \mapsto ab$. Extending it by bilinearity gives a bilinear map called **multiplication** $T(M) \times T(M) \to T(M)$ written $(a,b) \mapsto ab$.

Proposition 83. *The multiplication in $T(M)$ is associative, so that $T(M)$ is a ring. Moreover it has a unit $1 \in R = T^0(M)$ and there is a unital ring homomorphism $p\colon R \to T(M)$ which identifies R with $T^0(M)$.*

Proof. Clear. □

We call $T(M)$ the **tensor algebra** or **free (noncommutative) algebra on M**.

Example 84. In the above, assume that M is free with R-basis X. Let X^+ be the free monoid on X and let $p\colon X^+ \to T(M)$ be the monoid homomorphism defined by extending id_X. Then $T(M)$ is a free R-module with basis $p(X^+)$ (use the obvious generalisation of proposition 71 to free modules). Note also that p is injective. In this situation $T(M)$ is also known as the ring of **noncommutative polynomials in X**.

Definition 85. A **$\mathbb{Z}_{\geq 0}$-grading** or just **grading** on a ring R consists of $\mathbb{Z}$-submodules $R_k \subset R$ for all $k \geq 0$ such that R is the direct sum $R = \bigoplus_{k \geq 0} R_k$ and such that $R_k R_\ell \subset R_{k+\ell}$ for all k, ℓ. A **graded ring** is a ring along with a grading on it. Elements of R_k are said to be **homogeneous of degree k**.

For example, $T(M)$ admits the grading of the submodules $T^k(M)$.

4.9 Symmetric and exterior algebras

All our modules and linear maps are over a commutative ring R.

Definition 86. Let M be a module. The **symmetric algebra** is $S(M) := T(M)/C(M)$ where $C(M)$ is the ideal generated by $\{a \otimes b - b \otimes a \mid a, b \in M\}$. Equivalently, $C(M)$ is the smallest ideal in $T(M)$ such that $T(M)/C(M)$ is commutative.

Example 87. Let M be a free R-module with basis $(x_1, \ldots, x_n)$. Then $S(M) \cong R[x_1, \ldots, x_n]$, the ring of polynomials in $x_1, \ldots, x_n$.

Definition 88. Let M be a module. The **exterior algebra** is $\wedge(M) := T(M)/A(M)$ where $A(M)$ is the ideal generated by $\{a \otimes a \mid a \in M\}$.

Example 89. Let $a, b \in M$. Then $ab + ba \in A(M)$ because

$$ab + ba = (a+b)^2 - a^2 - b^2 \in A(M).$$

If 2 is invertible in R then $A(M)$ is generated by $\{ab + ba \mid a, b \in M\}$.

Definition 90. Let $S^k(M)$ denote the image of $T^k(M)$ in $S(M)$. Let $\wedge^k(M)$ denote the image of $T^k(M)$ in $\wedge(M)$.

So the $S^k(M)$ and $\wedge^k(M)$ provided gradings on $S(M)$ and $\wedge(M)$.

If $a \in \wedge^k(M)$ and $b \in \wedge^\ell(M)$ then $ba = (-1)^{k\ell}ab$. This is known as **graded-commutative** or **super-commutative**.

Exercise (4.19) Let M be a free module with basis X. Let Y be the image of X in $\wedge(M)$ and choose a total ordering $<$ on Y. Then $\wedge^k(M)$ is a free module with basis

$$\big(y_1 \cdots y_k \;\big|\; y_i \in Y \text{ for all } i,\ y_i < y_{i+1} \text{ for all } i\big).$$

5 Homological algebra

In this chapter all categories are on the right unless specified otherwise.

5.1 Short exact sequences

Definition 91. A finite sequence of R-modules and homomorphisms

$$M_0 \xrightarrow{d_0} M_1 \xrightarrow{d_1} \cdots \xrightarrow{d_{n-1}} M_n$$

is said to be **exact at M_k** if $\mathrm{im}(d_{k-1}) = \ker(d_k)$. It is said to be **exact** if it is exact at M_k whenever $0 < k < n$. It is said to be a **(cochain) complex at M_k** if $\mathrm{im}(d_{k-1}) \subset \ker(d_k)$, that is, $d_{k-1}\,d_k = 0$. It is said to be a **complex** if it is a complex at M_k whenever $0 < k < n$. Likewise if the sequence extends infinitely far to the left or right or both.

A **short exact sequence** is an exact sequence of R-modules and homomorphisms

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0.$$

Exactness means: f is injective, $\mathrm{im}(f) = \ker(g)$, and g is surjective.

Definition 92. A **morphism of complexes** is a commutative diagram

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & A_1 & \longrightarrow & A_2 & \longrightarrow & A_3 & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & B_1 & \longrightarrow & B_2 & \longrightarrow & B_3 & \longrightarrow & \cdots
\end{array}$$

such that the rows are complexes. The rows may not extend infinitely far in one or both directions, but we assume that every column contains an arrow.

Lemma 93: Short 5-lemma. *Let*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow[f]{} & B & \xrightarrow[g]{} & C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & & \\
0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0
\end{array}$$

be a morphism of short exact sequences.

(a) *If a, c are injective then so is b.*

(b) *If a, c are surjective then so is b.*

(c) *If a, c are bijective then so is b.*

Proof. (a). Suppose a, c to be injective and let $x \in B$ be such that $xb = 0$. Then $0 = xbg' = xgc$. But c is injective so $xg = 0$. But the top row is exact so there exists $y \in A$ such that $x = yf$. Then $yaf' = yfb = xb = 0$. But f' is injective to $ya = 0$. But a is injective so $y = 0$. So $x = yf = 0f = 0$. This proves that b is injective.

(b). Suppose a, c to be surjective and let $z \in B'$. Now c is surjective so there exists $w \in C$ such that $wc = zg'$. But g is surjective so there exists $x \in B$ such that $xg = w$. Then $xbg' = xgc = wc = zg'$. So $xb - z \in \ker(g') = \mathrm{im}(f')$, say $xb - z = vf'$ with $v \in A'$. But a is surjective so there exists $y \in A$ such that $v = ya$. Then $xb - z = vf' = yaf' = yfb$. So $z = (x - yf)b$. This proves that b is surjective.

(c). This follows from (a) and (b). □

Given A, C, how many short exact sequences $0 \to A \to B \to C \to 0$ are there?

Exercise (5.1) (Split complexes over a field). Let K be a field. Let B_n, H_n be vector spaces over K for all n. Put $A_n = B_n \times H_n \times B_{n+1}$ for all $n \in \mathbb{Z}$ and define $d_n \colon A_n \to A_{n+1}$ by

$$d_n(a, b, c) = (c, 0, 0) \quad \text{for all } (a, b, c) \in B_n \times H_n \times B_{n+1}.$$

Prove that A is a cochain complex. Prove that every cochain complex over K is isomorphic to one of these.

Definition 94. A short exact sequence is said to **split** or **be split** if it is isomorphic to one of the following form:

$$0 \longrightarrow A \xrightarrow{f} A \oplus C \xrightarrow{g} C \longrightarrow 0 \tag{95}$$

where $xf = (x, 0)$ and $(x, y)g = y$ for all $x \in A$, $y \in C$.

Lemma 96. *Consider a short exact sequence*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0.$$

The following are equivalent:

(a) *It splits.*

(b) *There exists a submodule $D \subset B$ such that $B = Af \oplus D$.*

(c) *There exists a homomorphism $s \colon C \to B$ called a* **section** *such that $sg = \mathrm{id}_C$.*

(d) *There exists a homomorphism $h \colon B \to A$ called a* **retraction** *such that $fh = \mathrm{id}_A$.*

Proof. Note first that (a) $\Leftrightarrow$ (b) is trivial.

Proof of (b) $\Rightarrow$ (c). Assume $B = Af \oplus D$. By the first isomorphism theorem there exists an isomorphism $B/\ker(g) \to \mathrm{im}(g) \colon x + \ker(g) \mapsto xg$. This gives an isomorphism $t \colon D = B/Af = B/\ker(g) \to C$. The inverse s to t has the required properties.

Proof of (c) $\Rightarrow$ (b). Put $D = Cs$. We claim $B = Af \oplus D$.

Proof of $B = Af + D$. Let $x \in B$. Put $y = xgs \in D$. Then $(x - y)g = xg - xgsg = xg - xg1 = 0$. By exactness $x - y \in Af$. This proves $x \in Af + D$ and hence $B = Af + D$.

Proof of $Af \cap D = 0$. Let $x \in Af \cap D$. Since $x \in D$ there exists $y \in C$ with $x = ys$. Then $xg = ysg = y1 = y$. Since $x \in Af$ we can write $x = zf$ with $z \in A$. Then $y = xg = zfg = z0 = 0$. So $x = ys = 0s = 0$. This proves $Af \cap D = 0$ and finishes the proof of (c) $\Rightarrow$ (b).

Proof of (b) $\Rightarrow$ (d). Define h: $B = Af \oplus D \to A$ by $(xf, y)h = x$ for all $x \in A$, $y \in D$. This is well-defined because f is injective. Clearly $fh = \mathrm{id}_A$ as required.

Proof of (d) $\Rightarrow$ (b). Exercise. □

Example 97. Let R be a unital ring. Prove that every short exact sequence of left R-modules of the form

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} R \longrightarrow 0$$

splits.

Solution. Since g is surjective, there exists $x \in B$ such that $xg = 1$ where 1 is the unit of R. Define a section s: $R \to B$ by $rs = rx$ for all $r \in R$.

Let's first prove that s is a map of R-modules. Well, for all $a, b, r \in R$ we have $(ra)s = (ra)x = r(ax) = r(as)$ and clearly $(a+b)s = as + bs$. So s is a map of R-modules.

We shall prove that $sg = \mathrm{id}_R$. For all $r \in R$

$$\begin{aligned} rsg &= (rx)g && \text{by definition of } s \\ &= r(xg) && \text{because } g \text{ is a map of } R\text{-modules} \\ &= r1 && \text{because } xg = 1 \\ &= r && \text{because 1 is the unit in } R. \end{aligned}$$

So $sg = \mathrm{id}_R$. By lemma 96 our sequence splits. □

Example 98. Nonsplit short exact sequences exist. Here is an example with base ring $R = \mathbb{Z}$:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{g} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

where f is multiplication by 2 and g is the natural map.

5.2 Exact functors

Definition 99. A functor ${}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ (not necessarily covariant) is said to be **left exact** if it takes exact sequences of the form $0 \to A \to B \to C$ to exact sequences. It is said to be **right exact** if it takes exact sequences of the form $A \to B \to C \to 0$ to exact sequences. It is **exact** if it is both left and right exact.

Exercise (5.2) Prove that a covariant functor T: ${}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ is left exact (respectively, right exact) if and only if exactness of $0 \to A \to B \to C \to 0$ implies that

$$0 \to TA \to TB \to TC \quad \text{(respectively, } TA \to TB \to TC \to 0\text{)}$$

is exact.

In particular, a functor is exact if and only if it takes short exact sequences to short exact sequences.

Most functors are left exact or right exact but not both.

Proposition 100. *Let D be a left R-module. Then the functor* $\mathrm{Hom}(D,-)\colon {}_R\mathbf{Mod} \to {}_R\mathbf{Mod}$ *is left exact.*

Proof. Consider an exact sequence of the form

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C.$$

The functor $F = \mathrm{Hom}(D,-)$ takes it to

$$0 \longrightarrow \mathrm{Hom}(D,A) \xrightarrow{f'} \mathrm{Hom}(D,B) \xrightarrow{g'} \mathrm{Hom}(D,C) \tag{101}$$

where $pf' = p \circ f$ and $qg' = q \circ g$ for all p, q. We must prove that (101) is exact.

Proof of exactness at $\mathrm{Hom}(D,A)$. We must prove that f' is injective. Let $p \in \ker(f')$, that is, $p\colon D \to A$ is a homomorphism and $pf = 0$. Then $xpf = 0$ for all $x \in D$. But f is injective so $xp = 0$ for all $x \in D$. So $p = 0$. So f' is injective as required.

It remains to prove $\mathrm{im}(f') \supset \ker(g')$. Let $q \in \ker(g')$. We define $p \in \mathrm{Hom}(D,A)$ as follows. Let $x \in D$. Then $0 = x(qg') = (xq)g$ so $xq \in \ker(g) = \mathrm{im}(f)$, say $xq = (xp)f$. Note that xp is well-defined because f is injective. At this point $p\colon D \to A$ is a map of sets and we should prove that it is a homomorphism. Well, for $x, y \in D$ and $a, b \in R$ we have

$$\begin{aligned}((ax+by)p)f &= (ax+by)q = a(xq) + b(yq) \\ &= a((xp)f) + b((yp)f) = (a(xp) + b(yp))f\end{aligned}$$

and f is injective so $(ax+by)p = a(xp) + b(yp)$. This finishes the definition of p. For all $x \in D$ then $xq = (xp)f = x(pf')$ so $q = pf'$ as required. □

Example 102. The functor $\mathrm{Hom}(D,-)\colon {}_R\mathbf{Mod} \to {}_R\mathbf{Mod}$ may not be exact as is shown by the example with $R = \mathbb{Z}$, $D = \mathbb{Z}/2\mathbb{Z}$ and the functor is applied to the exact sequence

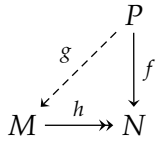
$$0 \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{g} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

where f is multiplication by 2 and g is the natural map.

5.3 Projective modules

Let P be an R-module. We know that the functor $\mathrm{Hom}(P,-)$ is left exact by proposition 100. For which P is it exact?

Definition 103. An R-module P is **projective** if for any surjection of R-modules $h\colon M \to N$ and any map of R-modules $f\colon P \to N$ there exists $g\colon P \to M$ such that $f = gh$.



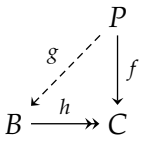
Proposition 104. *Let P be an R-module. Then the following are equivalent:*

(1) *The R-module P is projective.*

(2) *The functor* $T = \mathrm{Hom}(P,-)\colon {}_R\mathbf{Mod} \to {}_R\mathbf{Mod}$ *is exact.*

(3) *There exists an R-module Q such that $P \oplus Q$ is a free R-module. We say that P is a* **summand** *of a free module.*

Proof. Proof of (1) $\Rightarrow$ (2). By proposition 100 the functor T is left exact. It remains to show that it takes surjective morphisms to surjective morphisms. So let $h\colon B \to C$ be surjective. Let $f \in \mathrm{Hom}(P, C)$.



By the definition of projective modules there exists $g \in \mathrm{Hom}(P, B)$ such that $f = gh$, that is, $T(h)\colon \mathrm{Hom}(P, B) \to \mathrm{Hom}(P, C)$ takes g to f. So $T(h)$ is surjective.

Proof of (2) $\Rightarrow$ (3). Every module is a quotient of a free one. Let F be a free R-module and $h\colon F \to P$ a surjective homomorphism. Let K denote its kernel. Then we have a short exact sequence

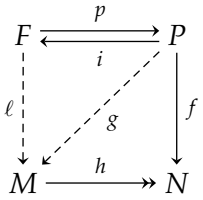
$$0 \longrightarrow K \longrightarrow F \xrightarrow{h} P \longrightarrow 0.$$

Since T is exact and h is surjective the map $T(h)\colon \mathrm{Hom}(P, F) \to \mathrm{Hom}(P, P)\colon g \mapsto gh$ is surjective too. In particular the identity id_P is in the image of $T(h)$, say $\mathrm{id}_P = gh$ with $g \in \mathrm{Hom}(P, F)$. So g is injective. Consider the short exact sequence

$$0 \longrightarrow P \xrightarrow{g} F \longrightarrow F/P \longrightarrow 0.$$

It has property (d) of lemma 96 so it satisfies (a), that is, P is a summand of F.

Proof of (3) $\Rightarrow$ (1). Assume that P is a summand of a free module F. So there exist homomorphisms $i\colon P \to F$ and $p\colon F \to P$ such that $ip = \mathrm{id}_P$. Let a surjection of R-modules $h\colon M \to N$ and a map of R-modules $f\colon P \to N$ be given.



Let X be a basis of F. For each $x \in X$ let $y_x \in M$ be such that $y_x h = xpf$; this is possible because h is surjective.

Since X is a basis of F there exists a unique homomorphism $\ell\colon F \to M$ such that $x\ell = y_x$ for all $x \in X$. Note $\ell h = pf$.

Put $g := i\ell\colon P \to M$. Then $f = \mathrm{id}_P f = (ip)f = i(pf) = i(\ell h) = (i\ell)h = gh$. This proves that P is projective as required. □

Exercise (5.3) Let P be an R-module. Prove that P is projective if and only if every short exact sequence of R-modules of the form

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} P \longrightarrow 0$$

splits.

Exercise (5.4) In this exercise you prove that a free module may have two bases of different sizes. Let V be a vector space over a field K of infinite countable dimension and put $R = \mathrm{End}_K(V)$. Prove $V \cong V \otimes V$ and deduce that $R \cong R \oplus R$ as left R-modules.

5.4 Right exactness of $(D \otimes -)$

Exercise (5.5) Let D be an R-module. Prove that $\mathrm{Hom}(-, D)$: ${}_R\mathbf{Mod} \to {}_R\mathbf{Mod}$ is right exact.

Lemma 105. *A sequence of R-modules and their homomorphisms*

$$A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is exact if and only if $\mathrm{Hom}(-, D)$ *takes it to an exact sequence for all R-modules D.*

Proof. 'Only if' is exercise 5.5: right exactness of $\mathrm{Hom}(-, D)$. We prove 'if'.

All our categories are on the right. Let D be an R-module, to be specified later, and $T = \mathrm{Hom}(-, D)$. Then

$$\mathrm{Hom}(A, D) \xleftarrow{Tf} \mathrm{Hom}(B, D) \xleftarrow{Tg} \mathrm{Hom}(C, D) \longleftarrow 0 \tag{106}$$

is exact. We have $q(Tf) = fq$ and $r(Tg) = gr$ for all q, r.

Proof that g is surjective. Put $D = C/Bg$ and let p: $C \to D$ be the natural map. Then

$$\begin{aligned} 0 &= gp && \text{by construction} \\ &= p(Tg) && \text{by definition of } T. \end{aligned}$$

Exactness of (106) implies that Tg is injective and so $p = 0$. Therefore $Bg = C$ and g is surjective.

Proof that $fg = 0$. Exercise. Use $D := C$ and $\mathrm{id}_C \in TC$.

Proof that $\mathrm{im}(f) \supset \ker(g)$. Exercise. Use $D := B/Af$. □

Exercise (5.6) Fill in the details in the above proof.

Proposition 107. *Let D be a right R-module. Then the functor* $(D \otimes -)$: ${}_R\mathbf{Mod} \to {}_{\mathbb{Z}}\mathbf{Mod}$ *is right exact.*

Proof. Let

$$A \longrightarrow B \longrightarrow C \longrightarrow 0 \tag{108}$$

be an exact sequence of morphisms in ${}_R\mathbf{Mod}$. Let E be a left R-module. The functor $\mathrm{Hom}(-, E)$ is right exact by exercise 5.5 so takes (108) to an exact sequence

$$\mathrm{Hom}(A, E) \longleftarrow \mathrm{Hom}(B, E) \longleftarrow \mathrm{Hom}(C, E) \longleftarrow 0. \tag{109}$$

The functor $\mathrm{Hom}(D, -)$ is left exact by proposition 100 so takes (109) to an exact sequence

$$\mathrm{Hom}(D, \mathrm{Hom}(A, E)) \leftarrow \mathrm{Hom}(D, \mathrm{Hom}(B, E)) \leftarrow \mathrm{Hom}(D, \mathrm{Hom}(C, E)) \leftarrow 0.$$

Recall that there is a natural isomorphism

$$\alpha\colon \mathrm{Hom}(-, \mathrm{Hom}(-, -)) \cong \mathrm{Hom}(- \otimes -, -)$$

which is a natural isomorphism α between two functors (or trifunctors)

$$\mathbf{Mod}_R \times {}_R\mathbf{Mod} \times {}_R\mathbf{Mod} \to {}_{\mathbb{Z}}\mathbf{Mod}.$$

Therefore

$$\mathrm{Hom}(D \otimes A, E) \leftarrow \mathrm{Hom}(D \otimes B, E) \leftarrow \mathrm{Hom}(D \otimes C, E) \leftarrow 0 \tag{110}$$

is exact. We must prove that the maps in (110) are what we think. Do this yourself.

This holds for all E so by lemma 105

$$D \otimes A \longrightarrow D \otimes B \longrightarrow D \otimes C \longrightarrow 0 \tag{111}$$

is exact. Therefore $(D \otimes -)$ is right exact. □

5.5 *Derived functors*

Definition 112. Let M be a cochain complex

$$\cdots \longrightarrow M_1 \xrightarrow{d_1} M_2 \xrightarrow{d_2} M_3 \longrightarrow \cdots .$$

For $k \in \mathbb{Z}$ we define the **cohomology modules** $H^k(M) = \ker(d_k)/\operatorname{im}(d_{k-1})$.

Exercise (5.7) Let R be a ring. Let D be the category of cochain complexes of modules over R and their morphisms. Let $(A, a), (B, b)$ be objects of D and $f\colon A \to B$ a morphism in D.

(a) Prove $\ker(a_n)f \subset \ker(b_n)$ and $\operatorname{im}(a_n)f \subset \operatorname{im}(b_n)$ for all n. Deduce that f induces a (unique) map $H^n(f)\colon H^n(A) \to H^n(B)$.

(b) Prove that H^n is a functor $D \to R$-mod.

Definition 113. Let A be an R-module. A **projective resolution** of A is an exact sequence of R-modules and their homomorphisms

$$\cdots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{e} A \longrightarrow 0 \tag{114}$$

such that P_k is projective for all $k \geq 0$. It is a **free resolution** if P_k is free for all $k \geq 0$.

We know that every free module is projective. Therefore every free resolution is a projective resolution.

Proposition 115. *Every R-module A admits a free resolution.*

Proof. To simplify notation we write $A_0 := A$ and shall construct a free resolution of the form

$$\cdots \xrightarrow{e_3} A_2 \xrightarrow{e_2} A_1 \xrightarrow{e_1} A_0 \xrightarrow{e_0} 0. \tag{116}$$

We do this recursively. Let $n > 0$ and assume that A_k and e_k have been defined whenever $n > k \geq 0$.

Every module is a quotient of a free one. Let A_n be a free module and $e_n\colon A_n \to \ker(e_{n-1})$ be surjective. The target object of e_n is however defined to be A_{n-1}; this is possible because $\ker(e_{n-1})$ is a submodule of A_{n-1}.

This finishes the construction of a free resolution (116). Exactness is clear. □

Example 117. Let $R = \mathbb{Z}$. Then there is free resolution

$$0 \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{g} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0 \tag{118}$$

where f is multiplication by 2 and g is the natural map.

Unproved Theorem/Definition 119. *Let T: **R-mod** $\to$ **S-mod** be a right exact covariant or left exact contravariant functor. Let A be an R-module and choose a projective resolution* (114)*. Let P denote the complex*

$$\cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow 0$$

*(no A). Then $H^n(TP)$ depends only on A, not the projective resolution. The **nth derived functor** L_nT: **R-mod** $\to \mathbb{Z}$**-mod** takes A to $H^n(TP)$.* □

Definition 120. The nth left derived functor of $\mathrm{Hom}(-, D)$ is written $\mathrm{Ext}^n(-, D)$.

To summarise one may write $\mathrm{Ext}^n(A, D) = H^n(\mathrm{Hom}(P, D))$.

Remark 121. The group $\mathrm{Ext}^1(C, A)$ is in bijection with the set of isomorphism classes of short exact sequences $0 \to A \to B \to C \to 0$. Such a short exact sequence (or B) is also called an **extension of C by A**.

Example 122. Let us calculate $\mathrm{Ext}^n(A, A)$ where $A = \mathbb{Z}/2$ and the base ring is $R = \mathbb{Z}$. We have the free resolution (118). Removing the last A and applying the functor $\mathrm{Hom}(-, A)$ yields

$$0 \xleftarrow{d_2=0} A \xleftarrow{d_1=0} A \xleftarrow{d_0=0} 0.$$

So:

- $\mathrm{Ext}^0(A, A) = \ker(d_1) = A$.
- $\mathrm{Ext}^1(A, A) = \ker(d_2)/\operatorname{im}(d_1) = A$.
- $\mathrm{Ext}^k(A, A) = 0$ for $k \geq 2$.

Definition 123. The nth left derived functor of $(D \otimes_R -)$ is written $\mathrm{Tor}_n(D, -)$.

Remark 124. If A is a $\mathbb{Z}$-module then A is torsion free (that is, $(A, +)$ has no non-trivial element of finite order) if and only if $\mathrm{Tor}^1(A, B) = 0$ for every R-module B.

Example 125. Let's calculate $\mathrm{Tor}_k(A, A)$ where $A = \mathbb{Z}/2$ and the base ring is $R = \mathbb{Z}$. A projective resolution is (118). Removing the last A and applying the functor $A \otimes -$ gives

$$0 \xrightarrow{d_2=0} A \xrightarrow{d_1=0} A \xrightarrow{d_0=0} 0.$$

So:

- $\mathrm{Tor}_0(A, A) = \ker(d_0)/\operatorname{im}(d_1) = A$.
- $\mathrm{Tor}_1(A, A) = \ker(d_1)/\operatorname{im}(d_2) = A$.
- $\mathrm{Tor}_k(A, A) = 0$ for $k \geq 2$.

5.6 The long exact sequence

Definition 126. A **short exact sequence** of complexes is a sequence of complexes and their morphisms

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0 \tag{127}$$

such that, for all $k \in \mathbb{Z}$, the sequence in degree k

$$0 \longrightarrow A_k \xrightarrow{f_k} B_k \xrightarrow{g_k} C_k \longrightarrow 0$$

is exact.

This means that we have a commutative diagram

$$\begin{array}{ccccccc}
 & & 0 & 0 & 0 & & \\
 & & \downarrow & \downarrow & \downarrow & & \\
\cdots & \longrightarrow & A_{k-1} & \longrightarrow A_k & \longrightarrow A_{k+1} & \longrightarrow & \cdots \\
 & & \downarrow & \downarrow & \downarrow & & \\
\cdots & \longrightarrow & B_{k-1} & \longrightarrow B_k & \longrightarrow B_{k+1} & \longrightarrow & \cdots \\
 & & \downarrow & \downarrow & \downarrow & & \\
\cdots & \longrightarrow & C_{k-1} & \longrightarrow C_k & \longrightarrow C_{k+1} & \longrightarrow & \cdots \\
 & & \downarrow & \downarrow & \downarrow & & \\
 & & 0 & 0 & 0 & &
\end{array}$$

where the rows are complexes and the columns exact.

Unproved Theorem 128. *With any short exact sequence of complexes* (127) *is associated a* **long exact sequence**

$$0 \to H^0(A) \to H^0(B) \to H^0(C) \to H^1(A) \to H^1(B) \to H^1(C) \to \cdots . \qquad \square$$

We won't prove this theorem but we shall construct the maps.

Construction of $H^n(A) \to H^n(B)$.

$$\begin{array}{ccccc}
A_{n-1} & \xrightarrow{a_n} & A_n & \xrightarrow{a_{n+1}} & A_{n+1} \\
\downarrow{\scriptstyle f_{n-1}} & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n+1}} \\
B_{n-1} & \xrightarrow{b_n} & B_n & \xrightarrow{b_{n+1}} & B_{n+1}
\end{array}$$

We claim that $\ker(a_{n+1})f \subset \ker(b_{n+1})$ and $\operatorname{im}(a_n)f \subset \operatorname{im}(b_n)$.

In the following we omit some of the indices. Let $x \in \ker(a_{n+1})$. Then $0 = xaf = xfb$ so $xf \in \ker(b_{n+1})$.

Let $x \in \operatorname{im}(a_n)$, say, $x = ya$ where $y \in A_{n-1}$. Then $yfb = yaf = xf$ so $xf \in \operatorname{im}(b_n)$.

This proves our claims. It follows that f_n induces a map $\ker(a_{n+1})/\operatorname{im}(a_n) \to \ker(b_{n+1})/\operatorname{im}(b_n)$, that is, $H^n(A) \to H^n(B)$.

Likewise for $H^n(B) \to H^n(C)$.

For a homomorphism of R-modules $f\colon M \to N$ we define $\operatorname{coker}(f) := N/Mf$. The map $H^n(C) \to H^{n+1}(A)$ will be defined as soon as the map $\ker(c) \to \operatorname{coker}(a)$ in the following lemma is constructed.

Unproved Lemma 129: Snake lemma. *Let*

$$\begin{array}{ccccccc}
 & & A & \xrightarrow[f]{} & B & \xrightarrow[g]{} & C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & & \\
0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & &
\end{array}$$

be a commutative diagram with exact rows. Then there exists an exact sequence

$$\ker(a) \to \ker(b) \to \ker(c) \xrightarrow{d} \operatorname{coker}(a) \to \operatorname{coker}(b) \to \operatorname{coker}(c). \qquad \square$$

The definitions of all maps in the snake lemma are obvious except for d which is defined as follows.

Let $x \in \ker(c)$. But g is surjective, say, $x = yg$. Then $0 = xc = ygc = ybg'$. So $yb \in \ker(g')$. But the bottom row is exact, say $yb = zf'$. We set $xd = z + \mathrm{im}(a)$.

Next we prove that d is well-defined. First note that f' is injective, so there is only one choice of z.

Let y_1 be another choice such that $x = y_1 g$. Then $(y - y_1)g = 0$. Say $y_1 b = z_1 f'$. We have $y - y_1 \in \mathrm{im}(f)$, say, $y - y_1 = wf$. Then $(z - z_1)f' = (y - y_1)b = wfb = waf'$. So $z - z_1 = wa \in \mathrm{im}(a)$ so d is well-defined.

6 Representation theory

For a field K and a group G let KG denote the group algebra. We are interested in the KG-modules.

In this chapter all rings are unital.

6.1 Some ring theory

Definition 130. A nonzero R-module M is said to be **simple** if it has no submodules other than 0 and itself. A left R-module is **semisimple** if it is a direct sum of simple modules.

Exercise (6.1) Let M, N be simple left R-modules and $f\colon M \to N$ a homomorphism. Then $\ker(f)$ is a submodule of M and $\mathrm{im}(f)$ a submodule of N.

Proposition 131: Schur's lemma. *Let M, N be simple left R-modules. Then any homomorphism $f\colon M \to N$ is zero or an isomorphism.*

Proof. Suppose $f \neq 0$. Then $\mathrm{im}(f)$ is a nonzero submodule of N. But N is simple so $\mathrm{im}(f) = N$, that is, f is surjective.

Also, $\ker(f)$ is a submodule of M different from M. But M is simple so $\ker(f) = 0$, that is, f is injective. So f is an isomorphism. □

Definition 132. A ring R is **semisimple** if R as left module over R is semisimple.

Definition 133. A nonzero left ideal $I \subset R$ is said to be **minimal** if it is simple as left R-module.

So a nonzero left ideal $I \subset R$ is minimal if 0 and I are the only left ideals of R contained in I. A ring is semisimple if and only if it is a direct sum of minimal left ideals.

Example 134. Let K be a field and $R = M(n, K)$. For $1 \leq j \leq n$, let $I_j \subset R$ be the set of matrices without nonzero columns except possibly the jth. Then I_j is a minimal ideal of R. Also, $R = \bigoplus_j I_j$ so R is semi-simple.

Proposition 135. *A left R-module M is semisimple if and only if every submodule of M is a summand.*

Proof. Proof of $\Rightarrow$. Suppose M is semisimple: $M = \bigoplus_{j \in J} S_j$ with S_j simple submodules of M. For any subset $I \subset J$ write $S_I = \bigoplus_{j \in I} S_j$.

Let $B \subset M$ be a submodule. Using Zorn's lemma, prove yourself that there exists a maximal $K \subset J$ such that $B \cap S_K = 0$.

We claim $M = B \oplus S_K$. Clearly $B \cap S_K = 0$. The claim will follow if we prove $S_j \subset B \oplus S_K$ for all $j \in J$.

Suppose first $j \in K$. Then $S_j \subset S_K$ and the claim follows.

Suppose finally $j \notin K$. Since K is maximal there exists nonzero $b \in B \cap (S_K + S_j)$. Write $b = x + y$, $x \in S_K$, $y \in S_j$. Then $y \neq 0$ because otherwise $b \in B \cap S_K = 0$. Also $y = b - x \in S_j \cap (B + S_K)$. But S_j is simple so $S_j = Ry \subset B + S_K$, again proving the claim.

Proof of $\Leftarrow$. Assume that every submodule of M is a summand. First we prove:

$$\text{Every nonzero submodule of } M \text{ contains a simple submodule.} \tag{136}$$

Let $B \subset M$ be a nonzero submodule. Choose $b \in B \setminus \{0\}$. Using Zorn's lemma, prove yourself that there exists a maximal submodule $C \subset B$ with respect to the condition $b \notin C$. Let C' be a submodule of M such that $M = C \oplus C'$. Put $D = B \cap C'$. Then $B = C \oplus D$. We shall prove that D is simple. Suppose it is not.

By the above argument applied to D instead of B there are nonzero modules D', D'' such that $D = D' \oplus D''$. We shall prove

$$b \notin (C \oplus D') \cap (C \oplus D''). \tag{137}$$

Suppose otherwise, say, $b = c + d' = c' + d''$, $c, c' \in C$, $d' \in D'$, $d'' \in D''$. Then $c - c' = d'' - d' \in C \cap D = 0$ so $d' = d'' \in D' \cap D'' = 0$ so $b = c \in C$, a contradiction. This proves (137). So $b \notin C \oplus D'$ or $b \notin C \oplus D''$. This contradicts the choice of C. Thus D is a simple submodule of B, which proves (136).

We are ready to prove that M is semisimple. Using Zorn's lemma, prove yourself that there is a maximal semisimple submodule $U \subset M$. Let V be such that $M = U \oplus V$. Suppose $V \neq 0$. Then V contains a simple submodule S. But then $U \oplus S$ is semisimple and larger than U, contradicting maximality of U. Therefore $V = 0$ and $M = U$ is semisimple. □

6.2 Group algebras

Theorem 138: Maschke's theorem. *Let G be a finite group and K a field whose characteristic doesn't divide $\#G$. Then KG is semisimple.*

Proof. Let I be an ideal of KG. By proposition 135 we will be done if we prove that the short exact sequence of KG-modules $0 \to I \to KG \to KG/I \to 0$ splits.

Since KG and I are finite-dimensional vector spaces over K there exists a vector space $V \subset KG$ over K such that $KG = I \oplus V$. Let $p\colon KG \to I$ denote the projection map, that is, $p(x + y) = x$ for all $(x, y) \in I \times V$. Define $q\colon KG \to KG$ by

$$q(x) = \frac{1}{\#G} \sum_{g \in G} g^{-1} p(gx).$$

Clearly $q(KG) \subset I$. Also $q(x) = x$ for all $x \in I$ because

$$q(x) = \frac{1}{\#G} \sum_{g \in G} g^{-1} p(gx) = \frac{1}{\#G} \sum_{g \in G} g^{-1} gx = \frac{1}{\#G} \sum_{g \in G} x = x.$$

In other words q is a retraction (see lemma 96). Finally we prove that q is a homo-

morphism of KG-modules. Indeed, for $h \in G$ and $x \in KG$ we have

$$\begin{aligned} q(hx) &= \frac{1}{\#G} \sum_{g \in G} g^{-1} p(g(hx)) && \text{by definition of } q \\ &= \frac{1}{\#G} \sum_{g \in G} g^{-1} p((gh)x) && \text{by associativity in } KG \\ &= \frac{1}{\#G} \sum_{f \in G} hf^{-1} p(fx) && \text{by the bijection } G \to G\colon g \mapsto gh \\ &= h\frac{1}{\#G} \sum_{f \in G} f^{-1} p(fx) = h\,q(x). \end{aligned}$$ □

Example 139. Let $G = \{1, s\}$ be a group of two elements. Let K be a field with $\mathrm{char}(K) \neq 2$. By Maschke's theorem KG is semisimple. Let's prove that directly. Put $I = K(1+s)$, $J = K(1-s)$. Then $KG = I \oplus J$ and I, J are minimal left ideals. Where does our argument use that $\mathrm{char}(K) \neq 2$? In fact, if $\mathrm{char}(K) = 2$ then KG is not simple because the only left ideals are $0, K(1+s), KG$.

Definition 140. A **representation (defined over a field K)** of a group G is a group homomorphism $\rho\colon G \to \mathrm{Aut}(V)$ for some vector space V over K.

Suppose $\rho\colon G \to \mathrm{Aut}(V)$ is a representation and V is a vector space over K. Then V becomes a KG-module by putting $gx = (\rho g)x$ for all $g \in G$, $x \in V$. This defines a bijection between the class of KG-modules and the class of representations of G defined over K. From now on we don't distinguish the two.

Proposition 141.

(a) *Every submodule of a semisimple module is semisimple.*

(b) *Every quotient of a semisimple module is semisimple.*

(c) *If R is a semisimple ring then every R-module is semisimple.*

Proof. (a). Let $C \subset B \subset M$ be modules with M semisimple. By proposition 135 there exists a submodule D of M such that $M = C \oplus D$. Let $p\colon M \to C$ be the projection defined by $p(c+d) = c$ for all $(c,d) \in C \times D$. Then $q := p|_B\colon B \to C$ is a retraction of the short exact sequence $0 \to C \to B \to B/C \to 0$ which hence splits. This holds for all C so proposition 135 implies that B is semisimple.

(b). Let N be a quotient of a semisimple module M. Then there is a short exact sequence $0 \to K \to M \to N \to 0$. By part (a) this sequence splits. So N is isomorphic to a submodule of M. By (a) then N is semisimple.

(c). Let R be a semisimple ring. Then every free R-module is semisimple. Every R-module is a quotient of a free one hence is semisimple itself by (b). □

Corollary 142. *Let G be a finite group and K a field whose characteristic doesn't divide $\#G$. Then every KG-module is semisimple.*

Proof. Immediate from propositions 138 (Maschke) and 141(c). □

Example 143. Let V be a complex vector space with basis $(v_1, \ldots, v_n)$. Then S_n acts on V by permutating the basis. This makes V into a $\mathbb{C}S_n$-module. It is not simple, because it has the submodule $\mathbb{C}(v_1 + \cdots + v_n)$. By corollary 141 however V is semisimple. In an exercise you will find its simple submodules.

Proposition 144. *Let R be a semisimple ring. Write $R = \bigoplus_i M_i$ where M_i are minimal left ideals. Then every simple left R-module is isomorphic to M_j for some j.*

Proof. Let B be a simple left R-module. Then $0 \neq B \cong \mathrm{Hom}(R, B) \cong \bigoplus_i \mathrm{Hom}(M_i, B)$. By Schur's lemma (proposition 131) the latter is 0 unless $B \cong M_j$ for some j. □

Corollary 145. *Let G be a finite group and K be a field whose characteristic doesn't divide $\#G$. Then there are only finitely many simple KG-modules up to isomorphism.*

Proof. Easy using propositions 138 (Maschke) and 144. □

6.3 Artin-Wedderburn

Let R be a ring. Recall that ${}_R\mathbf{Mod}$ is the category of left R-modules. We take this to be a category on the right.

Lemma 146. *Let M be a left R-module. The set ${}_R\mathbf{Mod}(M, M)$ can be turned into a ring by putting $x(p+q) := xp + xq$ and $x(pq) := (xp)q$ for all $x \in M$ and $p, q \in {}_R\mathbf{Mod}(M, M)$.*

Proof. Do yourself. □

Lemma 147. *Let R be a ring. Note that R can be viewed as a left R-module, so that ${}_R\mathbf{Mod}(R, R)$ is a ring by the previous lemma. For $y \in R$ let fy be the map $R \to R$ defined by $x(fy) = xy$ for all $x \in R$. Then f is an isomorphism of rings $R \to {}_R\mathbf{Mod}(R, R)$.*

Proof. The following must be proved:

(1) $fy \in {}_R\mathbf{Mod}(R, R)$ for all $y \in R$.
(2) $f(yz) = (fy)(fz)$ for all $y, z \in R$.
(3) $f(y+z) = fy + fz$ for all $y, z \in R$.
(4) $f(1) = \mathrm{id}_R$.
(5) f is injective.
(6) f is surjective.

We shall only do (2) and (6), leaving the others to you.

Proof of (2). Let $x, y, z \in R$. Then

$$\begin{aligned} x((fy)(fz)) &= (x(fy))(fz) && \text{by definition of composition in } {}_R\mathbf{Mod}(R, R) \\ &= (xy)(fz) && \text{by definition of } f \\ &= (xy)z && \text{by definition of } f \\ &= x(yz) && \text{by associativity in } R \\ &= x(f(yz)) && \text{by definition of } f. \end{aligned}$$

This holds for all x and so $(fy)(fz) = f(yz)$ for all $y, z \in R$.

Proof of (6). Let $g \in {}_R\mathbf{Mod}(R, R)$. Let 1 denote the unit in R and put $y := 1g$. Then for all $x \in R$

$$\begin{aligned} xg &= (x1)g && \text{because 1 is the unit of } R \\ &= x(1g) && \text{because } g \text{ is a homomorphism of left } R\text{-modules} \\ &= xy. \end{aligned}$$

Therefore $g = fy$, proving that f is surjective. □

Here are some semisimple (unital) rings: Group rings KG if G is finite and $\mathrm{char}(K) \nmid \#G$. Also $M(n,K)$ for any field K. Also $M(n,D)$ for any division ring D. Also finite direct sums of such. We can't take infinite direct sums because that wouldn't contain a unit.

Theorem 148: Artin-Wedderburn. *Let R be a semisimple ring. Then*

$$R \cong M(n_1, D_1) \times \cdots \times M(n_k, D_k)$$

for some positive integers n_i and division rings D_i.

Proof. Since R is semisimple there are minimal left ideals $(M_i \mid i \in I)$ such that $R = \bigoplus_{i\in I} M_i$. We shall prove that I is finite. There are $m_i \in M_i$ for all i such that $K := \{i \in I \mid m_i \neq 0\}$ is finite and

$$1 = \sum_{k\in K} m_k.$$

Let $i \in I \setminus K$ and $x \in M_i$. Then

$$x = x1 = \sum_{k\in K} xm_k \in \sum_{k\in K} M_k$$

which implies $x = 0$. This is true for all $x \in M_i$ so $M_i = 0$, a contradiction (minimal ideals aren't zero). So $I = K$ and I is finite.

Let $\sim$ be the equivalence relation on I defined by $i \sim j$ if and only if $M_i \cong M_j$. Let $J = I/\!\sim$. For $j \in J$ write $B_j = \bigoplus_{i\in j} M_i$. Then

$$\begin{aligned} R &\cong {}_R\mathbf{Mod}(R,R) && \text{by lemma 147} \\ &\cong {}_R\mathbf{Mod}(\textstyle\bigoplus_i B_i, \bigoplus_j B_j) \cong \bigoplus_{ij} {}_R\mathbf{Mod}(B_i, B_j) \\ &\cong \textstyle\bigoplus_j {}_R\mathbf{Mod}(B_j, B_j) && \text{by Schur's lemma.} \end{aligned}$$

Fix $i \in j \in J$. Put $D_j := {}_R\mathbf{Mod}(M_i, M_i)$ and $n_j = \#j$. Every nonzero element of D_j is an isomorphism $M_i \to M_i$ of R-modules so D_j is a division ring. Prove yourself ${}_R\mathbf{Mod}(B_j, B_j) \cong M(n_j, D_j)$. The proof is finished. □

Lemma 149. *Let K be an algebraically closed field. Let D be a division ring with $K \subset D$ and $\dim_K(D) < \infty$. Then $D = K$.*

Proof. Let $y \in D$. We begin by showing that $K[y]$ is a division ring. It is clearly a K-algebra. Let $z \in K[y] \setminus \{0\}$. Then multiplication by z defines an injective K-linear map $L_z\colon K[y] \to K[y]$. But $\dim_K K[y] < \infty$ so L_z has an inverse. So z has an inverse in $K[y]$.

Let $K[x]$ denote the ring of polynomials. Then there exists a unique homomorphism of K-algebras $f\colon K[x] \to D$ such that $f(x) = y$. Put $I = \ker(f)$. By the first isomorphism theorem $K[x]/I \cong K[y]$. But $K[y]$ is a division ring whence so is $K[x]/I$. Prove yourself that this implies that I is generated as ideal by an irreducible polynomial $g \in K[x]$. But K is algebraically closed so g is of degree 1 and $y \in K$. □

Corollary 150. *Let G be a finite group and K an algebraically closed field whose characteristic doesn't divide $\#G$. Then there are positive integers n_i such that*

$$KG \cong M(n_1, K) \times \cdots \times M(n_k, K) \tag{151}$$

as K-algebras. They satisfy

$$\#G = n_1^2 + \cdots + n_k^2. \tag{152}$$

Proof. By proposition 138 (Maschke) KG is semisimple. By proposition 148 (Artin-Wedderburn) we can write

$$KG \cong M(n_1, D_1) \times \cdots \times M(n_k, D_k)$$

for some division rings D_i. A look at the proof of Artin-Wedderburn shows that there is a natural embedding $K \subset D_i$, and that D_i is of finite dimension over K. By lemma 149 we find $D_i = K$.

Comparing dimensions in (151) shows (152). □

Example 153. Let $n > 0$ and $C_n = \langle g \mid g^n \rangle$ a cyclic group. The above result implies $\mathbb{C}[C_n] \cong \bigoplus_{i=1}^r M(n_i, \mathbb{C})$ for some r and n_i. But $\mathbb{C}[C_n]$ is commutative, so $n_i = 1$ for all i. So $\mathbb{C}[C_n] \cong \bigoplus_{i=1}^n \mathbb{C}$.

Let's prove this directly as well. Let $\omega = \exp(2\pi i/n)$. All our sums are over $\mathbb{Z}/n\mathbb{Z}$. For $1 \le k \le n$ put $x_k = \sum_{i=1}^n \omega^{ik} g^i$ by a slight abuse of notation. Note $\sum_i \omega^{id} = 0$ for all $d \in \mathbb{Z} \smallsetminus n\mathbb{Z}$. Therefore

$$\begin{aligned} x_k\, x_\ell &= \sum_{i,j} \omega^{ik} g^i\, \omega^{j\ell} g^j = \sum_{i,j} \omega^{ik} g^i\, \omega^{(j-i)\ell} g^{j-i} \\ &= \sum_{i,j} \omega^{j\ell + i(k-\ell)} g^j = n\, \delta_{k\ell} \sum_j \omega^{j\ell} g^j = n\, \delta_{k\ell}\, x_k. \end{aligned}$$

Moreover, $(x_1, \ldots, x_n)$ are independent over $\mathbb{C}$ because if $\sum_{k=1}^n a_k x_k = 0$ ($a_k \in \mathbb{C}$) then multiplying with x_ℓ reveals $a_\ell = 0$.

It follows that there is a ring isomorphism $f\colon \mathbb{C}^n \to \mathbb{C}[C_n]$ given by

$$f(y_1, \ldots, y_n) = \sum_{i=1}^n \frac{x_i\, y_i}{n}.$$

6.4 Character tables

What is k in corollary 150?

Let G be a finite group and $x, y \in G$. The **conjugacy class** of x in G is $x^G = \{g^{-1} x g \mid g \in G\}$. If $x^G = y^G$ then we say that x, y are conjugate in G. We write $k(G)$ for the number of conjugacy classes of G. The **class sum** $Z(x)$ is defined to be the sum of the elements of x^G. So $Z(x) = Z(y)$ if x, y are conjugate in G. The **centre** of a ring R is

$$Z(R) = \big\{a \in R \;\big|\; ab = ba \text{ for all } b \in R\big\}.$$

Lemma 154. *Let G be a finite group and K a field. Then the class sums form a K-basis of $Z(KG)$.*

Proof. Let $g, x \in G$. Then $x \mapsto g^{-1} x g$ defines a permutation $x^G \to x^G$. Therefore $Z(x)$ commutes with g. This holds for all $g \in G$ so $Z(x)$ is central in KG.

It is clear that the class sums are independent. To prove that they span $Z(KG)$, let $x \in Z(KG)$, say,

$$x = \sum_{g \in G} a(g)\, g$$

for some function $a\colon G \to K$. For all $h \in G$ we have $x = h^{-1} x h$, that is,

$$\sum_{g \in G} a(g)\, g = \sum_{g \in G} a(hgh^{-1})\, g.$$

It follows that a is constant on conjugacy classes. So x is a linear combination of class sums. □

Corollary 155. *Let G be a finite group and K an algebraically closed field whose characteristic doesn't divide $\#G$. Then there are positive integers n_i such that*

$$KG \cong M(n_1, K) \oplus \cdots \oplus M(n_k, K) \tag{156}$$

as K-algebras, and $k = k(G)$.

Proof. By corollary 150 we can write (156) as K-algebras. It remains to prove that $k = k(G)$. Let I_j be the identity matrix in $M(n_j, K)$. Then the centre of the right-hand side of (156) has basis $(I_1, \ldots, I_k)$ and is therefore of dimension k. The centre of the left-hand side of (156) has dimension $k(G)$ by lemma 154. So $k = k(G)$ as required. □

Definition 157. Let V be a finite-dimensional KG-module. For $g \in G$ we let $\chi_V(g)$ denote the trace (over K) of the g-action on V. This gives a map $\chi_V \colon G \to K$ known as the **character** of V.

Conjugate elements of $\mathrm{GL}(n, K)$ have the same trace. Therefore characters are constant on conjugacy classes. Sometimes we write $\chi_V(C)$ instead of $\chi_V(g)$ if C is the conjgacy class containing g.

Let G be a finite group. The **character table** of G is a table whose columns are the conjugacy classes, whose rows are the irreducible representations of G up to isomorphism, recording the values of the characters.

Example 158. The character table of S_3 is

	1	(123)	(12)
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2	-1	0

.