

We assume some amount of set theory.

ordered tuples and finite cartesian product

The definitions given here are not good for intuition. The main purpose is to provide (robust?) set-theoretic *implementations* of familiar algebraic constructions. This is a key distinction to be made—I am essentially assuming the reader is familiar with most if not all of the concepts and is able to recognize that the definitions (stroke implementations) adequately capture the necessary functionality.

A mathematical concept in the mind is characterized by some *information*—that being the information necessary to understand the concept. In my usage “information” does not exist in the mathematical world, but rather it exists in each individual mathematicians mind. We hope that this information generally agrees across minds, and in such cases we consider the information characterizing a mathematical object to be the information which is common in the minds of the mathematical community at large. It is this standard of information to which we will hold definitions.

In order to capture the information of a mathematical concept, we will use *data*—something which does exist in the mathematical world. Again, I have my own usage of the word “data,” which is luckily more concrete than that of “information.” My usage will hopefully become more clear as you read on, but suffice it to say that data is a specific mathematical construction intended to represent the information of some mathematical concept.

To be a bit more opaque, I will employ an analogy and some precise yet non-mathematical terminology. We can consider mathematical concepts like fictional characters. When we gives names to these concepts, there is no actual referent (though Salmon and I would prefer designatum, here) to which the name applies (refers/designates you get the idea). (Unfortunately, my choice of the word “concept” for a mathematical audience now conflicts with the point I am making because we can of course refer to concepts, as I have been doing.) If you’re willing to take my word for it—which you absolutely should not—the sort thing I have been calling a “concept” is better described in other terms, namely “sense.” For normal sorts of things, you can think of the sense of a name as the tether between the name itself and the referent. The name (word) “goose” has some sense attached to it which allows us to pick out the actual animal, i.e., the goose. One can think of the sense of the word “goose” as that thing which allows you to read and understand that it refers to the goose.

Anyway, definitions are gonna look like this:

A **whimpe** W is given by the following data:

- (1) an aggle-poogge A ,
- (2) a buzzo B with impermeable flingos,
- (3) a crundo C (called the *crun* inside W),

such that

- (i) A and B are equivalent as aggle-poogges,
- (ii) each dellon of C is also a dellon of A .

Say W is a whimpe or $W = (A, B, C)$ is a whimpe.

In other words, definitions of mathematical objects will be given as set-theoretic implementations in terms of collections of data satisfying certain axioms. Then to name such an object, we write it as the ordered tuple of data.

If A and B are sets, a subset $F \subseteq A \times B$ is called **functional** if for each $a \in A$ there is exactly one $b \in B$ such that $(a, b) \in F$.

A **function** f is given by the following data:

- (1) a set A called the *domain* of f (denoted “ $\text{dom } f$ ”),
- (2) a set B called the *codomain* of f (denoted “ $\text{codom } f$ ”),
- (3) a functional subset $F \subseteq A \times B$ called the *graph* of f .

We say that f is a function *from* A *to* B , denoted $f : A \rightarrow B$ or $A \xrightarrow{f} B$.

Given $a \in A$, the unique element $b \in B$ such that $(a, b) \in F$ is called the **value** of f at a , often denoted by $f(a)$, though sometimes denoted by fa or f_a . This is can also be called the evaluation of f at a or the image of a under f .

This definition adapted from [Ronald Brown, TOPOLOGY AND GROUPOIDS: A Geometric Account of General Topology, Homotopy Types and the Fundamental Groupoid]

We make a brief distinction here between our specific *definition* of the word “function” and the (more general) conceptual *notion* of a function. It is impossible to say in words precisely what the latter is, but we can make reference to it by the role it serves in the mathematical world. At one point or another—hopefully rather early in their career—a mathematician will acquire the correct notion of a function. The sense in which the notion is *correct* is that it is consistent with the notions of the vast majority of mathematicians.

We might ask the mathematician, “What is a function?” To which they might respond, “A function from A to B is a rule which assigns, to each element of A , an element of B .” You—the reader—can now act as an impartial third party to me—the author—and this other mathematician I have manufactured. With any luck, you are able to read and understand both this definition and my own definition of the word “function.” Moreover, I hope you agree that they both refer to the same *thing*—that being the notion of a function.

The goal of the above definition is that any sufficiently experienced mathematician will agree that I am using the word “function” consistently with broader mathematics, even if some of the specifics are different. In other words, my definition is attempting to capture the notion of a function by the set-theoretic data which characterizes it.

To be explicit, we are not defining functions per se, rather we are setting up a correspondence between functions $f : A \rightarrow B$ and triples of data (A, B, F) satisfying our definition of function.

In a completely set theoretic construction, we would identify every function f with its corresponding triple of data, i.e., $f = (A, B, F)$. In which case, we are essentially claiming that there is a bijection between functions in the usual sense and their corresponding triples.

$g = (C, D, G)$ is a

The justification for this sort of definition is that it ensures two functions $f : A \rightarrow B$ and $f' : A' \rightarrow B'$ are equal

The domain of f can be recovered from its graph F as follows:

$$\text{dom } f = \{a \mid (a, b) \in F \text{ for some } b\} = A.$$

On the other hand, the codomain of f cannot be recovered in this way. Instead, we find the following subset of the codomain called the **image** of f :

$$\text{im } f := \{b \mid (a, b) \in F \text{ for some } a\} \subseteq B.$$

The domain of f and the evaluation can also be used to find the image as follows:

$$\text{im } f = \{f(a) \mid a \in A\} \subseteq B.$$

Lastly, the graph of f can be recovered from the domain and the evaluations as follows:

$$\Gamma_f := \{(a, f(a)) \mid a \in A\} = F.$$

If desired, B^A is used to denote the set of all functions from A to B .

Let S be a set. We define the following functions:

the **identity** function $\text{id}_S : S \rightarrow S$ where $a \mapsto a$,

the **diagonal** function $\Delta_S : S \rightarrow S \times S$ where $a \mapsto (a, a)$,

the unnamed (component interchange) function $\lambda_S : S \times S \rightarrow S \times S$ where $(a, b) \mapsto (b, a)$.

Let S be a (nonempty?) set and n be a nonnegative integer.

The n **th cartesian power** of S is the set of all n -tuples of elements of S , denoted

$$S^n = \underbrace{S \times S \times \cdots \times S}_{n \text{ times}} = \{(a_1, \dots, a_n) \mid a_i \in S\}.$$

By convention, we take $S^0 = \{()\} = \{\emptyset\}$ (the set containing only the empty tuple/set).

An n -**ary operation** on S is a function $S^n \rightarrow S$.

Notably, a 0-ary (nullary) operation is a function $f : \{\emptyset\} \rightarrow S$. In other words, f picks out a single element of S , namely $f(\emptyset) \in S$. In fact, there is a bijective correspondence between the elements of S and the nullary operations on S , given by

$$\begin{aligned} S &\longleftrightarrow \{\text{nullary operations on } S\}, \\ a &\longleftrightarrow (\emptyset \mapsto a). \end{aligned}$$

Under this correspondence, we can consider distinguished elements of a set to be nullary operations, and vice versa. This is not a super important point, but simply makes the following definitions more concise, maybe. Is it worth it? Who is to say?

We want more than static sets—we want to be able to do stuff with the sets. Similar to our definition of “function,” we want to define the term “algebraic structure.” Put in an unhelpfully circular way, an algebraic structure is the sort of mathematical construction inside of which we can perform algebraic activities. In the fundamental cases, it consists of a set and some rules for how we can manipulate the elements of the set, e.g., operations. This paragraph is devoid of meaning. I am going to provide a set-theoretic implementation now.

An **algebraic structure** A (simple/on a set?) is given by the following data:

1. a set S , called the *underlying set* of A (denoted “ $|A|$ ”),
2. some operations α, β, \dots of any arity on S .

We say $A = (S, \alpha, \beta, \dots)$ is an algebraic structure.

There will usually only be finitely many operations on S and in any case there isn’t, we will use more compact notation.

A **magma** M is given by the following data:

- a set S ,
- a binary operation $f : S \times S \rightarrow S$.

We say $M = (S, f)$ is a magma.

A magma M is (naturally) an algebraic structure (S, f) .

It is common convention to notate the binary operation with a symbol called a (binary) *operator*—common examples include the following:

$$+ \quad \times \quad \cdot \quad * \quad \star \quad \circ$$

This is of course not a comprehensive catalog, though it covers most of the basic cases. If we choose the star ‘ \star ’ to represent our binary operation, we write ‘ $a \star b$ ’ to mean the image in S under f of the pair $(a, b) \in S \times S$. In other words, f describes a rule which takes two elements $a, b \in A$ and produces a third element of S , denoted

$$a \star b = f(a, b).$$

This new element $a \star b \in S$ might be called many different things depending on the actual context.

We will say things like “ S is a set with a binary operation \star ” or “ \star is a binary operation on the set S .” For brevity, we will also write “ (S, \star) is a magma” or possibly “ (S, f) is a magma” if we want to emphasize the fact that the binary operation is a function $S \times S \rightarrow S$.

In the broader mathematical world, it is common to consider only a single binary operation on a set at one time—there are many sets with ‘canonical’ operations—which can lead to the set alone being taken as proxy for the magma. For example, to refer to what we call “the magma (S, \star) ,” one might instead say “the set S *equipped with* a binary operation \star .” The difference here is subtle and a passing glance is not likely to reveal a discrepancy beyond the obvious linguistic one. And indeed there is no difference to one interfacing with mathematics in its most pure conceptual form. But you and I—dear reader—are confined to the relentlessly imperfect and finite bounds of language. When we do mathematics, we must undertake the impossible challenge of justifying that the sense connecting our mathematical referents to our mathematical language is justified, but can only do so either in the very same mathematical language or in some natural language. (The latter is what a mathematician might call ‘intuition’ (for the more cultured ‘being loosey goosey’ or ‘feeding the geese’)).

I trailed off, but the minor point is that it is unreasonable to be fully explicit all of the time. And while there are sometimes good reasons to ‘compress’ mathematical data into containers not designed for it, there should be a way to unpack that data when necessary (in my opinion of course). I would also say that neither formality nor explication exist solely on single axis of ‘less’ or ‘more,’ where one must simply pick a single point along that axis. A thinner dictionary can be seen as either ‘clean and elegant’ or ‘intuitive and superficial,’ while a thicker one as either ‘rigorous and complete’ or ‘cluttered and illegible’ (find more creative or meaningful adjectives). A proof on either end of this can also be more or less transparent/opaque/illuminating/aesthetic/motivating. (Hot take things have many aspects and rarely does a single aspect determine its quality.)

We are rarely interested in a general binary operation and will most often require it to have some additional structure. In such cases, however, we will need to define a particular binary operation and prove that it has the desired structure. For this reason—I would argue—it is worth having the language to talk about general binary operations.

(There is a diversion here where I lament about having to prove certain elementary properties of objects without having the proper language to even talk about the way in which those objects possess those properties. To make matters worse, it is often the case that the desired result is essentially some form of “niceness” in the sense that we are showing that some hypothetical bad situation never occurs. In which case, when we are using the object for its intended purpose, we can sweep certain technical nuances under the rug. So because the goal is to be able to ignore the nuance, one has to synthesize a complete model of this nuance only to discard it the moment it reveals its own unimportance.)

An **algebraic structure** A is given by (some or all of) the following data:

- (1) an *underlying* algebraic structure, denoted explicitly by \underline{A} unless otherwise specified,
- (2) some *auxiliary* algebraic structures/objects,
- (3) some homomorphisms between these algebraic structures.

An algebraic structure **class/type** is a *signature* of data for constructing an algebraic structure. The signature prescribes the following: whether or not and from which category an underlying object is required, whether or not and from which category any auxiliary objects are required, whether or not and from which category any morphisms are required. Additionally, the signature prescribes some *coherence conditions* which must be satisfied by the supplied data.

In other words, an algebraic structure class/type describes a format/template for constructing a more narrow sort of object. Any algebraic object which conforms to the template, is said to be of the class/type in question.

Whenever an algebraic object A of type \mathcal{A} has an underlying structure \underline{A} , then we very closely identify

hey bud these are just categories. just use categories

A **magma** M is a type of algebraic structure given by the following data:

- (1) an underlying set \underline{M} ,
 - (2) a binary operation on \underline{M} (a function $\underline{M} \times \underline{M} \rightarrow \underline{M}$).
-

Let $M = (\underline{M}, \odot)$ and $N = (\underline{N}, \otimes)$ be magmas.

In order to notate an expression containing multiple applications of the operation, we use parenthesis, e.g.,

$$a \star (b \star c) = f(a, f(b, c)) \quad \text{and} \quad (a \star b) \star c = f(f(a, b), c).$$

In general, it is not well-defined to write an expression like ‘ $a \star b \star c$,’ as it is possible that the result is dependent on the order in which we apply the operation. In cases where the this order does not matter, we can make sense of such notation.

A binary operation \star on a set S is called **associative** if for all $a, b, c \in S$ we have

$$(a \star b) \star c = a \star (b \star c)$$

A magma (S, \star)

- (ass) is **associative** if $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in S$,
- (id) has **identity** if there exists $e \in S$ such that $e \star a = a \star e = a$ for all $a \in S$,
- (inv) has **inverses** if for every $a \in S$ there exists $b \in S$ such that $ab = ba = e$,
- (comm) is **commutative** if $a \star b = b \star a$ for all $a, b \in S$.

A magma (S, \star) satisfying certain properties typically has a more specific name. We say (S, \star) is a

- **semigroup** if (ass) it is associative,
- **monoid** if (ass, id) it is associative and has an identity,
- **group** if (ass, id, inv) it is associative, has an identity, and has inverses,

Most of these will simply take “commutative” as an adjective, though we usually say **abelian group** to mean a commutative group, i.e.,

- **abelian group** if (ass, id, inv, comm) it is associative, has an identity, has inverses, and is commutative.

Chart:

	ass	id	inv	comm
magma	-	-	-	-
semigroup	x	-	-	-
monoid	x	x	-	-
comm. monoid	x	x	-	x
group	x	x	x	-
abelian group	x	x	x	x

semigroup bad, just add identity to get monoid.

“you can define lots of things, but that doesn’t mean you should study them.” - Dave Morrison

A **monoid** is given by the following data:

- (1) s set S ,
- (2) a distinguished element $e \in S$,

(3) a binary operation \star on S ,

such that

- (i) (ass) $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in S$,
- (ii) (id) $e \star a = a \star e = a$ for all $a \in S$.

In which case, we say (S, e, \star) is a **monoid**.

Let (S, e, \cdot) be a monoid. (For simplicity, write $ab = a \cdot b$ for all $a, b \in S$.)

Given $a, b \in S$ such that $ab = e$, we say that a is a **left inverse** of b and b is a **right inverse** of a . If in addition $ba = e$, then we say that a is an **inverse** of b , and vice versa. Equivalently, we might say

- a and b are inverses (of each other),
- a is inverse to b ,
- a and b are inverse (to one another).

Additionally, we say that a and b are **invertible** in the monoid.

(One must be careful when using the word “invertible,” as it is relative to both the underlying set and the operation—e.g., every element of \mathbb{Z} is invertible with respect to addition, though only 1 and -1 are invertible with respect to multiplication.)

Note a and b are inverses if and only if one is both a left and right inverse of the other.

In general mathematics, it is more common to hear the phrase “ a is *the* inverse of b ” rather than “ a is *an* inverse of b .” Indeed, in most nice cases, there is only one inverse. In turns out that this uniqueness holds in any monoid, as we will now demonstrate.

Proposition 1. If $a, b, c \in S$ are such that $ab = ca = e$, then $b = c$.

Proof. $b \stackrel{(\text{id})}{=} eb = (ca)b \stackrel{(\text{ass})}{=} c(ab) = ce \stackrel{(\text{id})}{=} c.$ □

In particular, the common value of b and c is an inverse of a . It follows that an element of a monoid is invertible whenever it has both a left and a right inverse—the proposition implies that the two are equal.

Corollary 1. Inverses are unique.

Proof. If b and c are both inverses of a , the proposition implies $b = c$. □

Hence, every invertible element of the monoid in fact has a unique inverse. If $a \in S$ is invertible, then we denote **the inverse** of a might be denoted by one of the following

$$-a \quad a^{-1} \quad \frac{1}{a} \quad \bar{a} \quad a'$$

Let (G, e, \cdot) be a group, i.e., a monoid with all elements invertible. Since the inverses in a monoid are unique, so too are the inverses in a group. And since every element has an inverse, there is a well-defined function

$$\begin{aligned}\iota : G &\longrightarrow G, \\ g &\longmapsto g^{-1},\end{aligned}$$

where g^{-1} is *the* inverse of g in the group. This function has the following properties:

- (i) $\iota \circ \iota = \text{id}_G$
- (ii) $\iota(g \cdot h) = \iota(h) \cdot \iota(g)$, i.e., $(gh)^{-1} = h^{-1}g^{-1}$

Let $G = (S, e, \cdot)$ be a group. We can define a new binary operation \odot on S as follows:

$$g \odot h := h \cdot g \quad \text{or} \quad \mu_{\odot} = \mu \circ \lambda_G.$$

Denote the algebraic structure $G^{\text{op}} = (S, e, \odot)$. We claim G^{op} is a group. Indeed (S, \odot) is a magma and $e \in S$ is a distinguished element, so we have the required data. (unless i later require the inversion map for groups) We check the axioms now:

- (ass) $(g \odot h) \odot k = k \cdot (h \cdot g) = (k \cdot h) \cdot g = g \odot (h \odot k)$,
- (id) $g \odot e = e \cdot g = g = g \cdot e = e \odot g$,
- (inv) $g \odot g^{-1} = g^{-1} \cdot g = e = g \cdot g^{-1} = g^{-1} \odot g = e$, where g^{-1} is the inverse of g in G .

Hence, G^{op} is a group, called the *opposite group* of G .

If $\iota : S \rightarrow S$ is the inversion function of G , then we have

$$\iota(g \cdot h) = \iota(h) \cdot \iota(g) = \iota(g) \odot \iota(h).$$

That is, ι specifies a group homomorphism (what's that bud?) $G \rightarrow G^{\text{op}}$. In fact, this is an isomorphism and $(G^{\text{op}})^{\text{op}} = G$.

Let X and Y be sets.

If there is a suitable ‘zero’ element $0 \in Y$, then the **support** of a function $f : X \rightarrow Y$ is the set

$$\text{supp } f = \text{supp}(f) := \{x \in X \mid f(x) \neq 0\} = f^{-1}(Y \setminus \{0\}) = X \setminus f^{-1}(0).$$

As a pseudo-definition, say f has **finite support** when $\text{supp}(f)$ is a finite set.

Recall that the support of a partial function is the subset of its domain on which it is defined.

Then f induces a partial function \tilde{f} from X to $Y \setminus \{0\}$. Then the support of f in the above sense is the same as the support of \tilde{f} as a partial function.

The upshot is that the “support” of a function usually refers to the subset of the domain whose values we actually care about. In algebraic contexts, this is almost always used with respect to a zero element.

Recall that the set of functions from X to Y is denoted by Y^X .

When Y is a suitable codomain, we denote by $Y^{(X)}$ the set of (partial) functions $X \rightarrow Y$ with finite support.

To be extremely pedantic, let

$$\mathcal{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

denote the set of integers. I emphasize that this is a set with no additional structure. It doesn't matter which specific set-theoretic structure it has—choose your favorite.

We define a binary operation $+$ on \mathcal{Z} such that $a + b$ is ‘the sum of a and b ,’ for all $a, b \in \mathcal{Z}$. This seems a little circular, and could definitely be formalized better. We define the abelian group $\mathbb{Z} = (\mathcal{Z}, 0, +)$, called the additive group of integers.

Typically, the term “addition” is reserved for any operation on a set that is sufficiently similar to the usual addition of integers. In particular, \mathbb{Z} addition is an abelian group. In fact, there is a sense in which addition over the integers is the most fundamental nontrivial abelian group.

Let X be a set.

A **formal sum** in X is given by the data of a function $c : X \rightarrow \mathbb{Z}$, written as

$$c = \sum_{x \in X} c_x \cdot x.$$

The value $c_x = c(x) \in \mathbb{Z}$ is called the **coefficient** of x . When we interpret c as a function $X \rightarrow \mathbb{Z}$, it is called the *coefficient function*. The notation is meant to suggest multiplying the coefficient $c(x) \in \mathbb{Z}$ with the element $x \in X$, and taking the sum over all such products.

Since \mathbb{Z} is an abelian group under addition, the set of functions \mathbb{Z}^X is also an abelian group under componentwise addition:

$$(a + b)(x) = a(x) + b(x).$$

Equivalently, this gives us an addition on the set of formal sums, with

$$a + b = \sum_{x \in X} a_x \cdot x + \sum_{x \in X} b_x \cdot x = \sum_{x \in X} (a + b)_x \cdot x = \sum_{x \in X} (a_x + b_x) \cdot x.$$

For each $a \in X$, there is a characteristic function $\chi_a : X \rightarrow \mathbb{Z}$ defined by

$$\chi_a(x) = \begin{cases} 1 & x = a, \\ 0 & x \neq a. \end{cases}$$

A **finite formal sum** in X is a formal sum $\sum_{x \in X} c_x x$ with only finitely many nonzero coefficients, i.e., $c_x \neq 0$ for finitely many $x \in X$. (function $c : X \rightarrow \mathbb{Z}$ has finite support.)

The set of finite formal sums in X may be denoted as any of the following:

$$\mathbb{Z} \cdot X \quad \mathbb{Z}X \quad \mathbb{Z}[X] \quad \mathbb{Z}^{(X)}$$

A **formal sum** in S is a symbolic object which suggests some form of addition over the elements of S , but no specific operation is present. Intuitively, we want to build notation for ‘the most general sort of addition’ over the elements of S .

The formal sum of two elements $a, b \in S$ is written as “ $a + b$ ” or “ $b + a$ ”. Ideally, we would want to interpret these expressions as the same thing. In other words, we are imagining the operation to be commutative.

The formal sum of three elements $a, b, c \in S$ is written as “ $a + b + c$ ” (or any permutation of the order). With this notation—in particular, not putting parentheses—we are imagining the operation to be associative.

Let $A = (\mathcal{A}, 0, +)$ be an abelian group.

A **ring** R is an algebraic structure with the following data:

- (1) distinguished elements $0, 1 \in |R|$,
- (2) a binary operation $+$ called *addition* such that $(|R|, 0, +)$ is an abelian group,
- (3) a binary operation \cdot called *multiplication* such that $(|R|, 1, \cdot)$ is a monoid,

such that the two operations satisfy the following distributivity properties:

- (i) (dist) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$,
- (ii) (dist) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

By convention, the *order of operations* in a ring puts multiplication before addition. Because of this, we can omit parentheses the order of operations can be deduced. Moreover, we typically write the multiplication without the operator, though sometimes use it for clarity. On the other hand, we always write the operator for addition. For example, we can write the following

$$(a \cdot b) + (c \cdot d) = ab + cd.$$

The additive inverse of $a \in R$ is denoted by $-a$, and we replace the plus sign with a minus sign when adding an inverse, e.g.,

$$a + (-b) = a - b.$$

The multiplicative inverse of $a \in R$, when it exists, is denoted by a^{-1} .

- (i) $\mu(a, \alpha(b, c)) = \alpha(\mu(a, b), \mu(a, c))$, i.e.,

$$\begin{array}{ccccc}
 R \times R \times R & \xrightarrow{\Delta_R \times \text{id}_R \times \text{id}_R} & R \times R \times R \times R & \xrightarrow{\text{id}_R \times \lambda_R \times \text{id}_R} & R \times R \times R \times R \\
 \downarrow \text{id}_R \times \alpha & & & & \downarrow \mu \times \mu \\
 R \times R & \xrightarrow{\mu} & R & \xleftarrow{\alpha} & R \times R \\
 & & R^3 \xrightarrow{\Delta \times \text{id} \times \text{id}} R^4 \xrightarrow{\text{id} \times \lambda \times \text{id}} R^4 & & \\
 & & \downarrow \text{id} \times \alpha & & \downarrow \mu \times \mu \\
 & & R^2 \xrightarrow{\mu} R \xleftarrow{\alpha} R^2 & &
 \end{array}$$

- (ii) $\mu(\alpha(a, b), c) = \alpha(\mu(a, c), \mu(b, c))$, i.e.,

$$\begin{array}{ccccc}
 R^3 & \xrightarrow{\text{id} \times \text{id} \times \Delta} & R^4 & \xrightarrow{\text{id} \times \lambda \times \text{id}} & R^4 \\
 \downarrow \alpha \times \text{id} & & & & \downarrow \mu \times \mu \\
 R^2 & \xrightarrow{\mu} & R & \xleftarrow{\alpha} & R^2
 \end{array}$$

A **ring** is given by the following data:

- (1) a set R ;
- (2) a binary operation $+$ on R called *addition*;
- (3) a binary operation \cdot on R called *multiplication*;

such that

- (i) R is an abelian group under addition:
 - (a) (associativity) $(a + b) + c = a + (b + c)$,
 - (b) (identity) $0 \in R$ called *zero* such that $0 + a = a + 0 = a$,
 - (c) (invertibility) for all $a \in R$ there exists an $-a \in R$ such that $a + (-a) = 0$,
 - (d) (commutativity) $a + b = b + a$;
 - (ii) R is a monoid under multiplication:
 - (a) (associativity) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
 - (b) (identity) $1 \in R$ called *one* such that $a \cdot 1 = 1 \cdot a = a$;
 - (iii) multiplication is distributive over addition:
 - (a) (left distributivity) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$,
 - (b) (right distributivity) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.
-

Proposition 2. In a ring R we have the following properties:

- (a) $0 \cdot a = a \cdot 0 = 0$,
- (b) $(-1) \cdot a = a \cdot (-1) = -a$,
- (c) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$,
- (d) $(-1) \cdot (-1) = 1$,
- (e) $(-a) \cdot (-b) = ab$.

Proof. beebop

- (a) $0a \stackrel{(+id)}{=} (0 + 0)a \stackrel{(dist)}{=} 0a + 0a$ implies $0 = 0a$ by cancellation.
 $a0 \stackrel{(+id)}{=} a(0 + 0) \stackrel{(dist)}{=} a0 + a0$ implies $0 = a0$ by cancellation.
- (b) $a + (-1)a \stackrel{(\cdot id)}{=} 1a + (-1)a \stackrel{(dist)}{=} (1 - 1)a \stackrel{(+inv)}{=} 0a \stackrel{(a)}{=} 0$ implies $(-1)a = -a$ by additive inverse uniqueness.
 $a + a(-1) \stackrel{(\cdot id)}{=} a1 + a(-1) \stackrel{(dist)}{=} a(1 - 1) \stackrel{(+inv)}{=} a0 \stackrel{(a)}{=} 0$ implies $a(-1) = -a$ by additive inverse uniqueness.
- (c) $-(ab) \stackrel{(b)}{=} (-1)ab \stackrel{(b)}{=} (-a)b \stackrel{(b)}{=} a(-1)b \stackrel{(b)}{=} a(-b)$.
- (d) $(-1)(-1) \stackrel{(b)}{=} -(-1)$ but $-(-1) = 1$ by additive inverse uniqueness.
- (e) $(-a)(-b) \stackrel{(b)}{=} a(-1)(-1)b \stackrel{(d)}{=} a1b \stackrel{(\cdot id)}{=} ab$.

□

A ring R is **local** if any of the following equivalent conditions are satisfied:

- R has a unique maximal left ideal;
- R has a unique maximal right ideal;
- For all $a, b \in R$, if $a + b$ is a unit then either a or b is a unit.

A module (over a commutative ring) is given by the following data:

- (1) a commutative ring R ,
- (2) an abelian group M ,
- (3) a function $\mu : R \times M \rightarrow M$ such that
 - (i) $\mu(1, x) = x$ or equivalently $\mu(1, -) = \mu|_{1 \times M} = \text{id}_M$
 - (ii) $\mu(ab, x) = \mu(a, \mu(b, x))$ or equivalently the following diagram commutes

$$\begin{array}{ccc}
 R \times R \times M & \xrightarrow{\text{id}_R \times \mu} & R \times M \\
 \mu_R \times \text{id}_M \downarrow & & \downarrow \mu \\
 R \times M & \xrightarrow{\mu} & M
 \end{array}$$

Let R be a commutative ring.

An **R -module** is given by the following data:

- (1) an abelian group M written additively, i.e., identity is 0 and binary operation is +,
- (2) a ring homomorphism $\mu : R \rightarrow \text{End}(M)$, called *scalar multiplication*.
- (3) a \mathbb{Z} -module homomorphism $\mu : R \otimes_{\mathbb{Z}} M \rightarrow M$, called *scalar multiplication*.

We usually write $r \cdot m$ for the evaluation $\mu(r)(m)$.

Let R be a ring.

A **left R -module** is given by the following data:

- an abelian group M , written additively, i.e., identity is 0 and binary operation is +;
- a function $\mu : R \times M \rightarrow M$ called *scalar multiplication* (write $r \cdot m = \mu(r, m)$);

such that

- $1 \cdot m = m$ for all $m \in M$;
- $r \cdot (m + n) = (r \cdot m) + (r \cdot n)$ for all $r \in R$ and $m, n \in M$;
- $(r + s) \cdot m = (r \cdot m) + (s \cdot m)$ for all $r, s \in R$ and $m \in M$;
- $r \cdot (s \cdot m) = (rs) \cdot m$ for all $r, s \in R$ and $m \in M$.

A **right R -module** is given by the following data:

- an abelian group M , written additively, i.e., identity is 0 and binary operation is +;

- a function $\mu : M \times R \rightarrow M$ called *scalar multiplication* (write $m \cdot r = \mu(m, r)$);

such that

- $m \cdot 1 = m$ for all $m \in M$;
- $(m + n) \cdot r = (r \cdot m) + (r \cdot n)$ for all $r \in R$ and $m, n \in M$;
- $m \cdot (r + s) = (r \cdot m) + (s \cdot m)$ for all $r, s \in R$ and $m \in M$;
- $(m \cdot s) \cdot r = m \cdot (sr)$ for all $r, s \in R$ and $m \in M$.

Let $R = (\mathcal{R}, 0, 1, +, \cdot)$ be a ring.

We construct a the **opposite ring** $R^{\text{op}} = (\mathcal{R}, 0, 1, +, \cdot^{\text{op}})$, where

$$r \cdot^{\text{op}} s = s \cdot r$$

Let R be a ring and M be an abelian group.

A left R -module structure on M is equivalently a ring homomorphism $\lambda : R \rightarrow \text{End}(M)$, with

$$r \cdot m = \lambda(r)(m)$$

A right R -modules over M is a ring homomorphism $R^{\text{op}} \rightarrow \text{End}(M)$.

Let A and B be rings. Let M be an abelian group.

An **A - B -bimodule structure** on M consists of

- A left A -module structure on M ;
- A right B -module structure on M ;

such that

- $a(mb) = (am)b$.

This data, denoted ${}_A M_B$ is called an A - B -bimodule.

If M is an R - R -bimodule, simply say M is an R -bimodule.

Let R be a ring.

The **center** of R is the set

$$Z(R) = \{r \in R \mid ax = xr \text{ for all } x \in R\}.$$

$Z(R)$ is a commutative subring of R .

R is commutative if and only if $Z(R) = R$.

It is not in general true that $Z(R)$ is a maximal commutative subring of R .

Let R be a commutative ring.

An **associative unital R -algebra** consists of

- A ring A ;
- A ring homomorphism $\varphi : R \rightarrow Z(A)$.

We will consider all algebras to be associative unital until further notice.

If K is a field, a K -algebra is equivalently a K -vector space V with the structure of a ring such that

$$a(xy) = x(ay) = (ax)y$$

for all $a \in K$ and $x, y \in V$.

Let (A, φ) and (B, ψ) be R -algebras

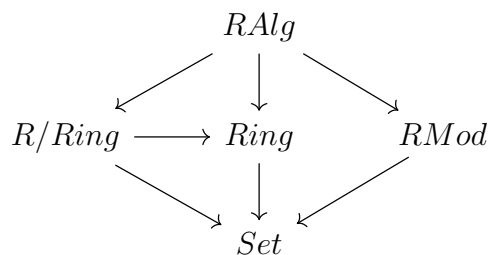
An **R -algebra homomorphism** is a ring homomorphism $f : A \rightarrow B$ such that

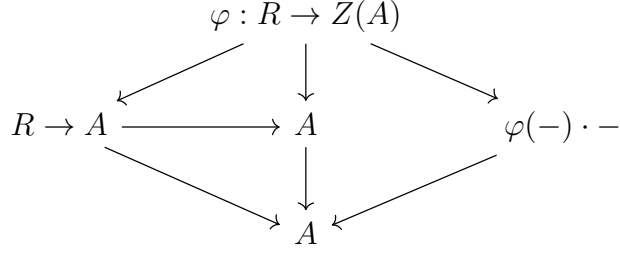
$$f(\varphi(r)a) = \psi(r)f(a)$$

for all $r \in R$ and $a \in A$.

There is a category $R\text{-Alg}$ of R -algebras and R -algebra homomorphisms.

There are forgetful functors





Let R be a commutative ring.

An **associative unital R -algebra** is equivalently any of the following:

- A monoid object of $R\text{-Mod}$ with respect to the tensor product of R -modules;
 - An R -module V with R -linear maps $p : V \otimes V \rightarrow V$ and $i : R \rightarrow V$ satisfying associative and unit laws;
 - A ring A with a ring homomorphism $R \rightarrow A$ whose image is in the center of A .
-

Let R be a ring and let I and J be sets.

An $I \times J$ -**matrix over R** consists of a function $A : I \times J \rightarrow R$. Call $a_{ij} = A(i, j) \in R$ the (i, j) entry of A , write

$$A = [a_{ij}]_{I \times J}.$$

For $I' \subseteq I$ and $J' \subseteq J$ the restriction $A|_{I' \times J'} = [a_{ij}]_{I' \times J'}$ is called a **submatrix** of A .

For $i \in I$, the restriction $A|_{i \times J} = [a_{ij}]_{i \times J}$ is called a **row** of A .

For $j \in J$ the restriction $A|_{I \times j} = [a_{ij}]_{I \times j}$ is called a **column** of A .

Denote the collection of such matrices by either of the following:

$$R^{I \times J} = M_{I \times J}(R).$$

Something about finiteness.

Get pointwise addition on $R^{I \times J}$, so is abelian group.

For $A \in R^{I \times J}$ and $B \in R^{J \times K}$, there is a function

$$\begin{aligned}
AB : I \times K &\longrightarrow \Sigma_J R \\
(i, k) &\longmapsto \sum_{j \in J} a_{ij} b_{jk}
\end{aligned}$$

If either A is row finite or B is column finite, each formal sum has finitely many nonzero entries, so is a well-defined element of R . In which case, AB is an $I \times K$ -matrix.

“It is easy but tedious to show that where this product is defined, it is associative and that it distributes over addition on both the right and left.”

The identity matrix $[\delta_{ij}] \in R^{J \times J} = M_J(R)$ is row and column finite and serves as the identity for the partial binary operation of multiplication.

Both the collections column finite and row finite square matrices are rings.

Let R be a ring.

An element $e \in R$ is called an **idempotent** if $e^2 = e$. (e.g. 0 and 1).

A pair of idempotents $e_1, e_2 \in R$ are **orthogonal** if $e_1 e_2 = e_2 e_1 = 0$.

An idempotent $e \in R$ is **primitive** if $e \neq 0$ and for every pair of orthogonal idempotents $e_1, e_2 \in R$, $e = e_1 + e_2$ implies $e_1 = 0$ or $e_2 = 0$. (e is not the sum of two nonzero orthogonal idempotents.)

A left (right) ideal of R is **primitive** if it is of the form Re (eR) for some primitive idempotent $e \in R$.

If $e \in R$ is an idempotent, so is $1 - e$:

$$(1 - e)^2 = 1 - e - e + e^2 = 1 - e - e + e = 1 - e.$$

Each nonzero idempotent $e \in R$ determines a ring

$$eRe = \{ere \mid r \in R\},$$

whose addition and multiplication are the restriction of that in R , and whose identities are $0 = e0e$ and $e = e1e$. If $e \neq 1$, then eRe is not a subring of R and if e is not central then the natural map $R \rightarrow eRe$ need not be a ring homomorphism.

If e is central, then the map $\tau_e : r \mapsto ere$ is a surjective ring homomorphism $R \rightarrow eRe$ with kernel $(1 - e)R(1 - e)$.

Let $R = \prod_A R_\alpha$ be the cartesian product of rings. For $\alpha \in A$, the element $e_\alpha = (\delta_{\alpha\beta}^{R_\beta})_{\beta \in A}$ is a central idempotent of R and there is an isomorphism $e_\alpha R e_\alpha \rightarrow R_\alpha$ given by the restriction of the projection π_α .

Let R be a ring and $1 \leq m \leq n$ be integers. Consider the matrix $e = [a_{ij}]$ defined by

$$a_{ij} = \begin{cases} 1 & \text{if } i = j \leq m, \\ 0 & \text{otherwise.} \end{cases}$$

Put another way,

$$e = \begin{bmatrix} I_m & 0 \\ 0 & 0 \end{bmatrix}.$$

Then e is a nonzero idempotent and there is a ring isomorphism

$$eM_n(R)e \cong M_m(R).$$

The same is true for any e with exactly m nonzero entries, all of which are 1's on the diagonal.

Let R be a ring.

An element $r \in R$ is called **nilpotent** if $r^n = 0$ for some $n \in \mathbb{Z}_{>0}$. The **nilpotent index/degree** of a nilpotent r is the smallest $n \in \mathbb{Z}_{>0}$ such that $r^n = 0$:

$$\min\{n \in \mathbb{Z}_{>0} \mid r^n = 0\}.$$

A subset $A \subseteq R$ is **nilpotent** if there exists $n \in \mathbb{Z}_{>0}$ such that

$$a_1 a_2 \cdots a_n = 0$$

for all sequences $a_1, \dots, a_n \in A$.

A subset $A \subseteq R$ is **nil** if each of its elements is nilpotent.

Remarks/exercises.

0 is the only element which is both idempotent and nilpotent.

$M_n(R)$ has many nilpotents.

If $x \in R$ is nilpotent then $1 - x$ is a unit.

Let $\varphi : R \rightarrow S$ be a surjective ring homomorphism. If $a \in R$ is a unit, central, idempotent, or nilpotent, respectively, then so is $\varphi(a) \in S$. How about converses?

Let R be a ring and $n \geq 2$ and integer. For each ideal $I \trianglelefteq R$ set

$$M_n(I) = \{[a_{ij}] \in M_n(R) \mid a_{ij} \in I\}.$$

The map $I \mapsto M_n(I)$ defines an isomorphism between the lattices of ideals in R and $M_n(R)$.

If $I \trianglelefteq R$, then has ring isomorphism $M_n(R)/M_n(I) \cong M_n(R/I)$.

Let R be a ring. There is a unique ring homomorphism $\chi : \mathbb{Z} \rightarrow R$. The kernel of χ is of the form $n\mathbb{Z}$ for some unique $n \geq 0$; this n is the **characteristic** of R .

Let $p \in \mathbb{N}$ be a prime. For each $n \in \mathbb{N}$ the ideals of $\mathbb{Z}/p^n\mathbb{Z}$ form a chain and each proper ideal is nilpotent. Then the product

$$R = \prod_{n \geq 1} \mathbb{Z}/p^n\mathbb{Z}.$$

has a nil ideal that is not nilpotent.

Proper coverage of modules goes here.

left/right modules, bimodules, etc.

A module M is called...

- **decomposable** if $M = N \oplus N'$ with N and N' nonzero
(A **direct decomposition** of M is any direct sum $M = \bigoplus_{\alpha \in A} M_\alpha$);
 - **indecomposable** if M is not decomposable;
 - **simple** if it has no nonzero proper submodules, i.e., $N \leq M$ implies $N = 0$ or $N = M$;
(sometimes “irreducible” for rep theory reasons i think. we’ll see if that’s useful.)
 - **completely decomposable** if $M = \bigoplus_{\alpha \in A} M_\alpha$ with each M_α indecomposable
(called an **indecomposable decomposition**);
 - **semisimple** if $M = \bigoplus_{\alpha \in A} M_\alpha$ with each M_α simple
(called a **semisimple decomposition**);
-

Let M be a left R -module.

For $X \subseteq M$, the **left annihilator** of X in R is

$${}_R\text{Ann}(X) = \{r \in R \mid rx = 0 \text{ for all } x \in X\}.$$

(Notation pending). For $A \subseteq R$ the **right annihilator** of A in M is

$$\text{Ann}_M(A) = \{x \in M \mid ax = 0 \text{ for all } a \in A\}.$$

Let M be an (R, S) -bimodule, $X \subseteq M$ and $A \subseteq R$. Then ${}_R\text{Ann}(X)$ is a left ideal of R and $\text{Ann}_M(A)$ is a submodule of M_S . Moreover if $X \leq {}_R M$ then ${}_R\text{Ann}(X) \trianglelefteq R$. If A is a right ideal of R then $\text{Ann}_M(A) \leq {}_R M_S$. If R is commutative, then ${}_R\text{Ann}(X) \trianglelefteq R$ and $\text{Ann}_M(A) \leq {}_R M_S$.

Suppose ${}_R M = N \oplus N'$ and $\pi_N : M \rightarrow N$ is the natural projection. Define $e_N \in \text{End}({}_R M)$ by $x \mapsto \pi_N(x)$. Then $\pi_N|_N = \text{id}_N$, e_N is an idempotent endomorphism of M , i.e.,

$$e_N = e_N^2 \in \text{End}({}_R M)$$

and $N = M e_N$.

Let e be an idempotent in $\text{End}({}_R M)$. Then $\text{id} - e$ is an idempotent in $\text{End}({}_R M)$ such that

$$\ker e = \text{im}(\text{id} - e) \quad \text{and} \quad \text{im } e = \ker(\text{id} - e)$$

and $M = Me \oplus M(\text{id} - e)$.

Suppose $M = \bigoplus_{\alpha \in A} M_\alpha$. Then for each $a \in A$

$$M = M_\alpha \oplus \sum_{\beta \neq \alpha} M_\beta,$$

so by some result, there is a unique idempotent $e_\alpha \in \text{End}({}_R M)$ with

$$M_\alpha = \text{im } e_\alpha \quad \text{and} \quad \ker e_\alpha = \sum_{\beta \neq \alpha} M_\beta.$$

Moreover the collection of idempotents $\{e_\alpha\}$ is orthogonal and for all $x \in M$ we have $xe_\alpha = 0$ for all but finitely many $\alpha \in A$ with $x = \sum_{\alpha \in A} xe_\alpha$.

A finite orthogonal set of idempotents $e_1, \dots, e_n \in R$ is **complete/full** if $e_1 + \dots + e_n = 1$.

Let M_1, \dots, M_n be submodules of M . Then $M = M_1 \oplus \dots \oplus M_n$ if and only if there exists a (necessarily unique) complete set e_1, \dots, e_n of orthogonal idempotents in $\text{End}({}_R M)$ with $M_i = Me_i$.

For a ring R , there are three natural “regular” modules to consider: ${}_R R$, R_R , and ${}_R R_R$.

Some results to be shown and expanded upon.

A left ideal I of a ring R is a direct summand of ${}_R R$ if and only if there is an idempotent $e \in R$ such that $I = Re$.

If $e \in R$ is an idempotent, then so is $1 - e$, and Re and $R(1 - e)$ are direct complements of each other, i.e., ${}_R R = Re + R(1 - e)$.

Any direct decomposition of ${}_R R$ has only finitely many nonzero summands. (look at $\pi_\alpha(1)$)

Let I_1, \dots, I_n be left ideals of R (equiv $I_i \leq {}_R R$?). TFAE:

- $R = I_1 \oplus \dots \oplus I_n$;
- Each $r \in R$ has a unique expression $r = r_1 + \dots + r_n$ with $r_i \in I_i$.
- There is a (necessarily unique) complete set of orthogonal idempotents $e_1, \dots, e_n \in R$ with $I_i = Re_i$.

If $e_1, \dots, e_n \in R$ is a complete set of orthogonal idempotents, then

$${}_R R = Re_1 \oplus \dots \oplus Re_n \quad \text{and} \quad R_R = e_1 R \oplus \dots \oplus e_n R.$$

Let $e \in R$ be a nonzero idempotent. TFAE:

- e is a primitive idempotent;
- Re is a primitive left ideal of R ;
- eR is a primitive right ideal of R ;
- Re is an indecomposable direct summand of ${}_R R$;
- eR is an indecomposable direct summand of R_R ;
- The ring eRe has exactly one nonzero idempotent, namely e .

${}_R R = I_1 \oplus \dots \oplus I_n$ with each I_i a primitive left ideal of R if and only if there exists a complete set of orthogonal primitive idempotents $e_1, \dots, e_n \in R$ such that $I_i = Re_i$.

Something about ring direct sums.

Let \mathcal{U} be a collection of modules. A module M is **(finitely) generated** by \mathcal{U} if there is a (finite) collection $\{U_\alpha\}_{\alpha \in A} \subseteq \mathcal{U}$ and an epimorphism $\bigoplus_{\alpha \in A} U_\alpha \rightarrow M$.

In case $\mathcal{U} = \{U\}$ is a singleton, say U (finitely) generates M ; which means there is an epimorphism $U^{(A)} \rightarrow M$ for some (finite) index set A .

If a module ${}_R M$ has a spanning set $X \subseteq M$, then there is an epimorphism $R^{(X)} \rightarrow M$. Moreover, R finitely generates M if and only if M has a finite spanning set.

A left R -module T is simple if and only if $T \cong R/\mathfrak{m}$ for some maximal left ideal \mathfrak{m} of R .

Suppose ${}_R M = \sum_{\alpha \in A} T_\alpha$ with each T_α simple. For every submodule $K \leq M$ there is a subset $B \subseteq A$ such that $M = K \oplus \bigoplus_{\beta \in B} T_\beta$.

Taking $N = 0$, we deduce that a module spanned by simple submodules is semisimple.

If M is semisimple, then every short exact sequence $0 \rightarrow K \rightarrow M \rightarrow N \rightarrow 0$ splits.

A few more, but big conclusion is...

Let M be a left R -module. TFAE:

- M is semisimple;
- M is generated by simple modules;
- M is the sum of some simple submodules;
- M is the sum of all its simple submodules;
- every submodule of M is a direct summand;
- every short exact sequence $0 \rightarrow K \rightarrow M \rightarrow N \rightarrow 0$ splits.

All semisimple modules, noetherian modules, and artinian modules have indecomposable decompositions.

However, not all modules admit indecomposable decompositions. For example, consider the ring of continuous functions $R = C^0(\mathbb{Q}, \mathbb{R})$, then the left regular module ${}_R R$ has no indecomposable direct summands.

Let M be a module.

Two direct decompositions

$$M = \bigoplus_{\alpha \in A} M_\alpha = \bigoplus_{\beta \in B} N_\beta$$

are said to be **equivalent** if there is a bijection $\sigma : A \rightarrow B$, called an **equivalence map**, such that $M_\alpha \cong N_{\sigma(\alpha)}$. It is easy to check that, as one should expect, this is indeed an equivalence relation.

Suppose $M = \bigoplus_{\alpha \in A} M_\alpha = \bigoplus_{\beta \in B} N_\beta$ and a function $\sigma : A \rightarrow B$. Then these two decompositions are equivalent if and only if there is an automorphism f such that $f(M_\alpha) = N_{\sigma(\alpha)}$.

It is in general not the case that any two indecomposable decompositions of a given module are equivalent. For example, let I and J be two left ideals of a ring R such that $R = I + J$, then $I \oplus J \cong R \oplus (I \cap J)$ as left R -modules.

A decomposition $M = \bigoplus_{\alpha \in A} M_\alpha$ is said to **complement (maximal) direct summands** if for every (maximal) direct summand K of M there is a subset $B \subseteq A$ such that

$$M = \left(\bigoplus_{\beta \in B} M_\beta \right) \oplus K.$$

This is a generalization of a property of semisimple modules.

A decomposition which complements all direct summands is necessarily indecomposable.

Suppose $M = \bigoplus_{\alpha \in A} M_\alpha$ is a decomposition that complements (maximal) direct summands. If $f : M \rightarrow M'$ is an isomorphism, then

$$M' = \bigoplus_{\alpha \in A} f(M_\alpha)$$

is a decomposition that complements (maximal) direct summands.

In particular, if a decomposition of M complements (maximal) direct summands, then so does any equivalent decomposition.

Lemma:

Let $M = \bigoplus_{\alpha \in A} M_\alpha$ be a decomposition that complements maximal direct summands. If we have another decomposition

$$M = N_1 \oplus \cdots \oplus N_n \oplus K$$

with each N_i indecomposable, then there exist $\alpha_i \in A$ such that $M_{\alpha_i} \cong N_i$ and for $\ell = 1, \dots, n$,

$$M = M_{\alpha_1} \oplus \cdots \oplus M_{\alpha_\ell} \oplus N_{\ell+1} \oplus \cdots \oplus N_n \oplus K.$$

Lemma:

Let $M = \bigoplus_{\alpha \in A} M_\alpha$ be a decomposition that complements (maximal) direct summands. For any subset $B \subseteq A$, $N = \bigoplus_{\beta \in B} N_\beta$ is a decomposition that complements (maximal) direct summands.

Moreover, if M has a decomposition that complements direct summands, then so does every direct summand of M .

Anderson & Fuller (1992): “*Incidentally, it is apparently not known whether the last assertion holds...for decompositions just complementing maximal direct summands.*” (should check if this has been resolved.)

Theorem:

If a module M has an indecomposable decomposition that complements maximal direct summands, then all indecomposable decompositions of M are equivalent.

Corollary:

If a module M has an indecomposable decomposition that complements (maximal) direct summands, then every indecomposable decomposition of M complements (maximal) direct summands.

If R is a local ring, then 0 and 1 are its only idempotents.

Azumaya Theorem:

Let $M = \bigoplus_{\alpha \in A} M_\alpha$ be a decomposition. If each endomorphism ring $\text{End}(M_\alpha)$ is local, then this is an indecomposable decomposition and

- every nonzero direct summand of M has an indecomposable direct summand;
- the decomposition $M = \bigoplus_{\alpha \in A} M_\alpha$ complements maximal direct summands and this is equivalent to every indecomposable decomposition of M .

Corollary:

Let $M = M_1 \oplus \cdots \oplus M_n$ be a finite decomposition. If each $\text{End}(M_i)$ is local, then the decomposition complements direct summands.

Lemma:

If M is an indecomposable module of finite length, then $\text{End}(M)$ is a local ring.

Krull-Schmidt Theorem:

Let M be a nonzero module of finite length. Then M has a finite indecomposable decomposition

$$M = M_1 \oplus \cdots \oplus M_n$$

such that for every other indecomposable decomposition

$$M = N_1 \oplus \cdots \oplus N_k,$$

$n = k$ and there is a permutation σ such that $M_{\sigma(i)} \cong N_i$ and for $\ell = 1, \dots, n$,

$$M = M_{\sigma(1)} \oplus \cdots \oplus M_{\sigma(\ell)} \oplus N_{\ell+1} \oplus \cdots \oplus N_n.$$

In fact, the decomposition $M = M_1 \oplus \cdots \oplus M_n$ complements direct summands.

Let D be a division ring (nonzero inverses/noncommutative field) and $n \in \mathbb{N}$.

Let

$$C_n(D) = M_{n \times 1}(D) = \begin{bmatrix} D \\ \vdots \\ D \end{bmatrix} \quad \text{and} \quad R_n(D) = M_{1 \times n}(D) = [D \quad \cdots \quad D]$$

denote the sets of $n \times 1$ column and $1 \times n$ row matrices with entries in D . Considering these as right and left D -vector spaces,

$$C_n(D) = (D_D)^n \quad \text{and} \quad R_n(D) = ({}_D D)^n.$$

Moreover, the usual matrix multiplications are ring isomorphisms

$$\lambda : M_n(D) \longrightarrow \text{End}(C_n(D)_D) \quad \text{and} \quad \ell : M_n(D) \longrightarrow \text{End}({}_D R_n(D)).$$

So $C_n(D)$ and $R_n(D)$ are left and right $M_n(D)$ -modules respectively.

In fact, both are simple $M_n(D)$ -modules; let E_1, \dots, E_n be the primitive diagonal idempotents of $M_n(D)$. Then as a left $M_n(D)$ -module

$$M_n(D) = M_n(D)E_1 \oplus \cdots \oplus M_n(D)E_n \cong C_n(D) \oplus \cdots \oplus C_n(D)$$

and as a right $M_n(D)$ -module

$$M_n(D) = E_1 M_n(D) \oplus \cdots \oplus E_n M_n(D) \cong R_n(D) \oplus \cdots \oplus R_n(D).$$

In particular, both left and right regular modules of $M_n(D)$ are generated by a simple module. By some result, every left $M_n(D)$ -module is generated by the simple $M_n(D)$ -module $C_n(D)$ and every right $M_n(D)$ -module is generated by the simple $M_n(D)$ -module $R_n(D)$.

Let R be a ring, M a nonzero left R -module, and $n \in \mathbb{N}$. Write endomorphisms of both M and $M^{(n)} = M^{\oplus n}$ as right operators, and we also write the natural inclusions and projections

$$\iota_i : M \rightarrow M^{(n)} \quad \text{and} \quad \pi_i : M^{(n)} \rightarrow M$$

on the right. For each $\alpha = [\alpha_{ij}] \in M_n(\text{End}(M))$ define $\rho(\alpha) \in \text{End}(M^{(n)})$ componentwise by

$$(x\rho(\alpha))\pi_j = \sum_{i=1}^n x\pi_i\alpha_{ij}.$$

Then $x\rho(\alpha)$ is simply the usual matrix product

$$x\rho(\alpha) = \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} \begin{bmatrix} \alpha_{ij} \end{bmatrix}$$

where the elements x of $M^{(n)}$ are considered as row matrices $x = \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix}$ over M . By the properties of ordinary matrix multiplication, we deduce that $M^{(n)}$ is a bimodule

$${}_R M^{(n)}_{M_n(\text{End}(M))}$$

via ρ , i.e.,

$$\rho : M_n(\text{End}(M)) \longrightarrow \text{End}(M^{(n)})$$

is a ring homomorphism. In fact, one can check that this is an isomorphism.

Schur Lemma:

If ${}_R T$ is a simple module, then $\text{End}({}_R T)$ is a division ring.

Wedderburn Theorem:

The ring R has as simple left generator if and only if R is isomorphic to the full submatrix ring $M_n(D)$ for some division ring D and some $n \in \mathbb{N}$. Moreover, if ${}_R T$ is a simple left generator for R , then as a ring $R \cong M_n(D)$ with $D = \text{End}({}_R T)$ and $n = \text{length}({}_R R)$ or

$$R \cong M_{\text{length}({}_R R)}(\text{End}({}_R T))$$

For a ring R TFAE:

- R has a simple left generator;
- R is a simple and left artinian;
- For some simple ${}_R T$, ${}_R R \cong T^{(n)}$ for some n ;
- R is simple and ${}_R R$ is semisimple.

Moreover, each of these is equivalent to the dual result (swap left and right).

In particular, for simple rings the conditions of left artinian, right artinian, and artinian are equivalent.

A ring satisfying these equivalent conditions is called a **simple artinian ring**.

A ring R is **semisimple** if the left regular module ${}_R R$ is semisimple.

Every simple artinian ring is semisimple.

Any ring direct sum of semisimple rings is also semisimple.

Wedderburn-Artin Theorem:

A ring is semisimple if and only if it is a finite (ring) direct sum of simple artinian rings.

More Structure:

Let R be a semisimple ring. Then R contains a finite set T_1, \dots, T_m of minimal left ideals which comprise an irredundant set of representatives of the simple left R -modules. Moreover, for each such set the homogeneous components

$$\text{Tr}(T_i) = RT_iR$$

are simple artinian rings and R is the direct sum

$$R = RT_1R \dot{+} \dots \dot{+} RT_mR.$$

Finally, T_i is a simple generator for the ring RT_iR and

$$RT_iR \cong M_{n_i}(D_i)$$

where $n_i = \text{length}(RT_iR)$ and $D_i = \text{End}({}_R T_i)$.

For a ring R TFAE:

- R is semisimple;
 - R has a semisimple left generator;
 - Every short exact sequence $0 \rightarrow K \rightarrow M \rightarrow N \rightarrow 0$ of left R -modules splits (equiv to every mono/epi in $R\text{-Mod}$ splitting);
 - Every left R -module is semisimple;
-

Maschke Theorem:

If G is a group of order n and K is a field whose characteristic does not divide n , then the group ring KG is semisimple.

Theorem:

If R be a simple ring of m elements, then

- $Z(R) = \mathbb{F}_{p^n}$ for some prime p and some n ;

- $m = (p^n)^{k^2}$ for some k ;
- $R \cong M_k(\mathbb{F}_{p^n})$.

As a corollary, there is a natural bijection between the finite semisimple rings (up to isomorphism) and the set of all finite sequences (ordered? surely not)

$$(p_1, n_1, k_1), \dots, (p_\ell, n_\ell, k_\ell)$$

of triples of natural numbers with each p_i prime.

$$\{\text{finite semisimple rings}\}/\text{iso} \longleftrightarrow \bigsqcup_{\ell \in \mathbb{N}} (\mathbb{N}_{\text{prime}} \times \mathbb{N} \times \mathbb{N})^\ell$$

If D is a division ring and M_D is a right D -vector space, then M_D is free, so the ring $\text{End}(M_D)$ of endomorphisms of M_D is isomorphic to the ring of column finite matrices over D . That is, if $\{x_i\}_{i \in I}$ is a basis for M_D then the mapping

$$\begin{aligned} \text{End}(M_D) &\longrightarrow \text{CFM}_I(D) \\ a &\longmapsto [a_{ij}] \end{aligned}$$

defined by

$$a(x_j) = \sum_{i \in I} x_i a_{ij} \quad \text{and} \quad a_{ij} = \pi_i(a(x_j)).$$