MATH 6122 lecture notes

Transcribed and formatted by John M. Campbell
jmaxwellcampbell@gmail.com

1 January 5th lecture

1.1 Contact information

Instructor: Nantel Bergeron

bergeron@yorku.ca

www.math.yorku.ca/bergeron

1.2 Preliminaries

In a general way, we can think about algebra as basically being about "the study of structure".

Often, if you put a structure on some mathematical object, say by endowing a set with an operation, such an object thus becomes "algebraic" in some sense.

What can we do with such a structure? How can we classify structures of a specified form?

1.2.1 Preliminaries from MATH 6121

The following subjects were explored in MATH 6121.

1. Linear algebra
   - Basic concepts related to linear algebra are used in virtually every area in mathematics.
   - Often, seemingly difficult problems in mathematics may be "reduced" in some way using linear algebra.
   - To illustrate this idea, think about how graphs of transcendental functions may be approximating using lines, by applying results in the field of elementary calculus.
   - The "theme" of reducing a more difficult problem using linear algebra is also encountered in the field of in Galois theory.
2. Group theory
   - Recall that a group G can act upon a set X through a group action, thus endowing X with the structure of a G-set.
   - Similarly, a group G may linearly act upon an abelian group A, yielding the structure of a left G-module.
   - The field of representation theory deals with homomorphisms of groups to general linear groups, thus extending the concept of a group action on a set.
3. Ring theory

- The following ring-theoretic objects and concepts were explored in MATH 6121.
- Fields
- Integral domains
- Principal ideal domains
- Euclidean domains
- Unique factorization domains
- Ideals (e.g., principal ideals, maximal ideals, etc.)
- The Chinese Remainder Theorem
- Gröbner bases

1.3 Evaluation

As indicated on the course webpage, students in MATH 6122 will be evaluated based on the following aspects.

1. Participation
   - Ideally, we should try to absorb the subject matter introduced in MATH 6122 by talking with one another.
   - Mathematics is, increasingly, a very participatory discipline: to understand the material presented in MATH 6122, we should discuss and exchange ideas concerning this material.
   - The participation component outlined above may be used to "bonify"[1] one of the items given below.
2. Projects/homework
3. (Tentative) midterm
4. Oral presentation
   - It often takes up to 10 hours or more of hard work to prepare for a 1-hour talk in mathematics.
   - Be mindful about anticipating questions concerning the subject matter of your presentation.
5. Comprehensive exam
   - In a way, one may think of doctoral qualifying exams as being analgous to job interviews.

The average of the best three of the last four items will be considered.

Virtually nobody excels in *all* of the above components. Intuitively, if you're sufficiently proficient in three of these areas, then this is very representative of your strength with respect to the subject matter of MATH 6122.

Even in mathematics, the process of grading is very subjective. In a very similar way, the process of writing a mathematical proof is often very subjective.

[1] See `https://en.wiktionary.org/wiki/bonify`.

Compared to MATH 6121, there is less of an emphasis on applications of algebra in MATH 6122.

In terms of the presentation of the subject matter of MATH 6122, there will be a little bit more of an emphasis on formality.

However, there is a cost to excessive formality: proofs become unreadible as they become unnecessarily formal.

1.4 Basic concepts in category theory

A **category** in the mathematical sense informally consists of a specified kind of "data".

More formally, a category consists of a **class**[2] $\mathscr{C}$ of mathematical **objects**.

What do we mean by "class" in this context? What do we mean by "object" in this context?

Informally, a class may be much "bigger" than a set.

Example 1.1. For example, there is no such thing as "the set of all sets"[3], but it makes sense to consider the *class* of all sets.

Example 1.2. Similarly, there is no such thing as "the set of all finite sets", but it makes sense to consider the *class* of all finite sets.

Informally, one may think of classes as being "meta"[4] mathematical objects, in the sense that a class may be a new collection of objects "above" sets.

$$\text{Set} \Longrightarrow \text{Class}$$
$$\text{Set} \not\Longleftarrow \text{Class}$$

Example 1.3. It would make sense to consider the class $\mathbb{N}$ of all natural numbers, since we know that $\mathbb{N}$ is a set.

Although we may think of classes as being new "meta" objects, we may use familiar set-theoretic notation with respect to classes.

For example, given a class $\mathscr{C}$, the expression $A \in \mathscr{C}$ is used to indicate that A is a member of $\mathscr{C}$, i.e., that A is an object in $\mathscr{C}$.

Informally, we can think of category theory as being based upon the use of concepts in mathematics based on sets and the "pushing" of these concetps to a new, abstract level.

• For a category $\mathscr{C}$, for all $A, B \in \mathscr{C}$, there exists a set $\text{Hom}_{\mathscr{C}}(A, B)$.

Remark 1.4. Observe that $\text{Hom}_{\mathscr{C}}(A, B)$ is required to be a set.

Notation: for $f \in \text{Hom}_{\mathscr{C}}(A, B)$, f is a **morphism** from A to B.

This is also denoted as

$$A \xrightarrow{f} B$$

[2] See https://en.wikipedia.org/wiki/Class_(set_theory).
[3] See http://mathworld.wolfram.com/RussellsAntinomy.html.
[4] See https://en.wikipedia.org/wiki/Meta.

or as

$$f\colon A \to B,$$

with $\mathrm{Dom}(f) = A$ and $\mathrm{Codom}(f) = B$.

The domain and codomain of a function f should be somehow "hidden" somewhere in the notation for f.

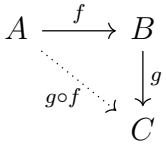
For example, it doesn't make sense to try to define a function as "x squared", since we need to specify a domain and a codomain.

Remark 1.5. In the field of category theory, there are specific kinds of arrow symbols to denote specific kinds of morphisms.

• For all objects A, B and C in a category $\mathscr{C}$, there is a mapping

$$\circ_{A,B,C} = \circ\colon \mathrm{Hom}_{\mathscr{C}}(A, B) \times \mathrm{Hom}_{\mathscr{C}}(B, C) \to \mathrm{Hom}_{\mathscr{C}}(A, C)$$

whereby $(f, g) \mapsto g \circ f$. This is also denoted in the following manner, so that for all morphisms f and g, the following diagram commutes.



Observe that we are abusing notation by omitting the indices of $\circ_{A,B,C}$ and using the simplified notation given by the symbol $\circ$.

The following axioms must be satisfied.

■ For all $A \in \mathscr{C}$, the set $\mathrm{Hom}_{\mathscr{C}}(A, A)$ is nonempty, with an element $1_A \in \mathrm{Hom}_{\mathscr{C}}(A, A)$ such that:

$$\forall B\ \forall f \in \mathrm{Hom}_{\mathscr{C}}(A, B)\ f \circ 1_A = f,$$
$$\forall C\ \forall g \in \mathrm{Hom}_{\mathscr{C}}(C, A)\ 1_A \circ g = g.$$

■ For all morphisms f, g, and h, the associative equality

$$(f \circ g) \circ h = f \circ (g \circ h)$$

holds whenever defined with respect to composition.

Remark 1.6. Intuitively, these axioms are somewhat reminiscent of the group axioms. Interestingly, we can formalize this idea, using a certain type of a category, with morphisms consisting of endomorphisms. Recall that an endomorphism[5] is basically a morphism from a mathematical object to itself. We explore this concept in the following subsection.

[5] See https://en.wikipedia.org/wiki/Endomorphism.

1.5 Examples of categories

1.5.1 Groups as categories

Let G be a group, and let $*$ denote the underlying binary operation on G. Observe that we are abusing notation somewhat in the sense that it may be more proper to express this group using the following notation: $(G, *)$.

Now, let $\bullet$ denote some fixed mathematical object. For example, we may let $\bullet = \varnothing$.

Write $\mathscr{C} = \{\bullet\}$.

Also, let $\mathrm{Hom}_{\mathscr{C}}(\bullet, \bullet) = G$, where G denotes the underlying set of the ordered tuple $(G, *)$ given above.

It may be convenient to abuse notation by writing $\circ$ in place of $\circ_{\bullet,\bullet,\bullet}$, with

$$\circ = \circ_{\bullet,\bullet,\bullet} \colon \mathrm{Hom}_{\mathscr{C}}(\bullet, \bullet) \times \mathrm{Hom}_{\mathscr{C}}(\bullet, \bullet) \to \mathrm{Hom}_{\mathscr{C}}(\bullet, \bullet)$$

so that

$$\circ \colon G \times G \to G$$

is equal to the underlying binary operation on $(G, *)$, with

$$(g, h) \mapsto g * h$$

under $\circ$.

This shows us that, in a sense, "*a group can be seen as a category*".

Remark 1.7. In a somewhat similar way, a partially ordered set can be seen as a category.

Now, let us verify that $\mathscr{C} = \mathscr{C}_G$ forms a category using the category axioms.

■ We have that $1_\bullet \in \mathrm{Hom}_{\mathscr{C}}(\bullet, \bullet)$, letting

$$1_\bullet = e_G \in G,$$

with $\bullet \in \mathrm{ob}(\mathscr{C}) = \{\bullet\}$.

■ By the group associativity axiom, we have that:

$$\forall f, g, h \in \mathrm{Hom}_{\mathscr{C}}(\bullet, \bullet) \;\; (f \circ g) \circ h = f \circ (g \circ h)\,.$$

1.5.2 The category of groups

The category of groups is often denoted as **Grp** or as **Group**.

Let $\mathscr{C} = \mathbf{Grp}$ be such that $\mathrm{ob}(\mathscr{C})$ is the class of all groups.

For groups G and H in $\mathrm{ob}(\mathbf{Grp})$, we have that:

$$\begin{aligned}
\mathrm{Hom}_{\mathscr{C}}(G, H) &= \{f \colon G \to H \text{ is a function from } G \text{ to } H \;:\; f \text{ is a group homomorphism}\} \\
&= \left\{f \in H^G \;:\; f \text{ is a group homomorphism}\right\} \\
&= \left\{f \in H^G \;:\; \forall h, g \in G \; f(hg) = f(h)f(g)\right\}.
\end{aligned}$$

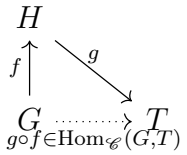
It is important to note that since H^G is a set, the collection

$$\left\{f \in H^G \ : \ \forall h, g \in G \ f(hg) = f(h)f(g)\right\}$$

must also be a set. Formally, this may be justified by appealing to the **axiom schema of specification** in **Zermelo–Fraenkel set theory**.

Recall that the composition of two group homomorphisms is a group homomorphism. This is a very basic result in the field of group theory.

■ For all $G, H, T \in \text{ob}(\mathbf{Grp})$, the following diagram commutes, for all morphisms f and g, with domains and codomains as indicated below.



Remark 1.8. Category theory may be regarded as a form of "meta-mathematics" or "meta-algebra" in the sense that the discipline of category theory may be regarded as "mathematics about mathematics" or "algebra about algebra".

■ $\forall G \in \text{ob}(\mathbf{Grp})$, there exists an element 1_G in $\text{Hom}_{\mathscr{C}}(G, G)$, since the identity mapping

$$\text{Id}_G \colon G \to G$$

is a group homomorphism, and therefore must be in $\text{Hom}_{\mathscr{C}}(G, G)$. It is a very basic lemma in group theory that identity mappings on groups are group homomorphisms.

■ We have that

$$(f \circ g) \circ h = f \circ (g \circ h)$$

when the above equality is well-defined. In general, the well-defined composition of functions is associative.

1.6 Other examples of categories

Example 1.9. Given a field K, the category $\mathscr{C}$ such that $\text{ob}(\mathscr{C})$ is the class of all vector spaces over K and such that the morphisms of $\mathscr{C}$ are precisely K-linear transformations is denoted as **K-Vect** or as $\mathbf{Vect}_K$[6].

Example 1.10. Similarly, **R-Mod** denotes the category of left R-modules, given a ring R.

Example 1.11. The category of sets[7] is denoted as **Set**. In this case, the morphisms are just functions.

Informally a **concrete category** consists of "sets with some structure".

We will later explore examples of categories which are not concrete.

For example, conside the poset $(\mathbb{N}, |)$, letting $|$ denote the binary relation on $\mathbb{N}$ given by divisibility. For $n, m \in \mathbb{N}$, define $\text{Hom}_{\mathbb{N}}(n, m)$ so that:

$$\text{Hom}_{\mathbb{N}}(n, m) = \begin{cases} \{(n, m)\} & \text{if } n \mid m \\ \varnothing & \text{if } n \nmid m \end{cases}.$$

[6]See https://en.wikipedia.org/wiki/Category_of_modules.
[7]See https://en.wikipedia.org/wiki/Category_of_sets.

MATH 6122 lecture notes

Transcribed and formatted by John M. Campbell
jmaxwellcampbell@gmail.com

2 January 10th lecture

2.1 Administrative notes

A free book on category theory is available through the website indicated below.

https://arxiv.org/pdf/1612.09375v1.pdf

Recall that class participation is important with respect to the grading scheme for MATH 6122.

Typsetting lecture notes using typsetting languages such as LaTeX is often a very effective way of learning the material presented during lectures.

There is an important property concerning categories, which is sometimes regarded as being axiomatic, which we did not previously discuss: it is important to note that $\mathrm{Hom}_{\mathscr{C}}(A, B)$ and $\mathrm{Hom}_{\mathscr{C}}(C, D)$ must be disjoint if $A \neq C$ or $B \neq D$.

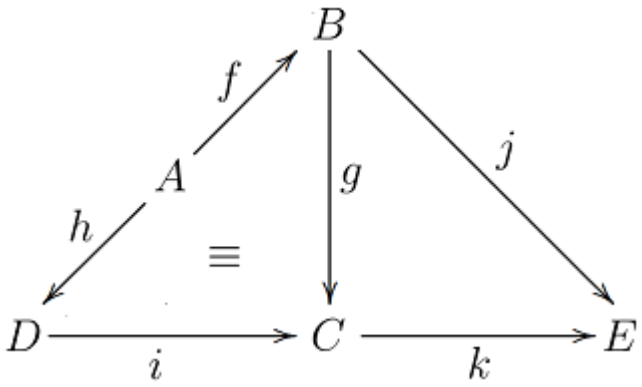
2.2 Commutative diagrams

Recall the following axioms of a category:

■ For all A in a category $\mathscr{C}$, there exists an identity morphism 1_A in $\mathrm{Hom}_{\mathscr{C}}(A, A)$.

■ The associative equality whereby $f \circ (g \circ h) = (f \circ g) \circ h$ holds when defined.

Now, consider the diagram illustrated below.



The symbol $\equiv$ given above indicates that the above diagram is a **commutative diagram**.

We say "the diagram commutes" $\longleftrightarrow$ *any two paths in the directed graph with the same start and end give the same morphism.* For example, consider the following three subdiagrams of a commutative diagram.

$$A \xrightarrow{f} B \xrightarrow{j} E \qquad j \circ f$$

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{k} E \qquad k \circ g \circ f$$

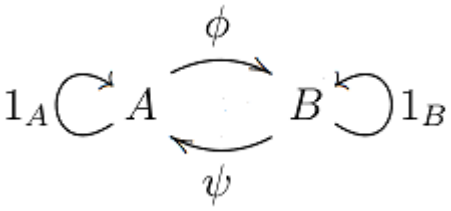
$$A \xrightarrow{h} D \xrightarrow{i} C \xrightarrow{k} E \qquad k \circ i \circ h$$

In this situation, we have that $j \circ f = k \circ g \circ f = k \circ i \circ h$.

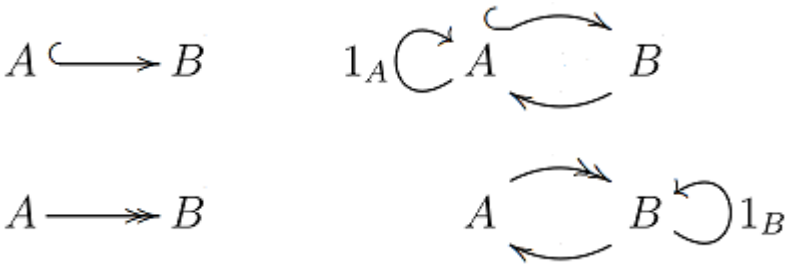
2.3 Isomorphisms

Given a category $\mathscr{C}$, and objects A and B in $\mathrm{ob}(\mathscr{C})$, the objects A and B are said to be **isomorphic** if there exist morphisms ϕ and ψ such that the

diagram illustrated below commutes. This is denoted by: $A \cong B$.



Recall that arrows in commutative diagrams are sometimes "decorated" in order to denote specific kinds of morphisms.



It is important to note that morphisms of the former kind are not the same as monomorphisms, and morphisms of the latter type are not necessarily epimorphisms.

Observe that we are not using any specific elements in domains or codomains, with respect to the above definitions. Informally, many concepts in category theory involve this idea of using morphisms instead of specific members in domains, codomains, etc.

In a **concrete category**, the above definitions could be reformulated by appealing to individual elements in domains, codomains, etc.

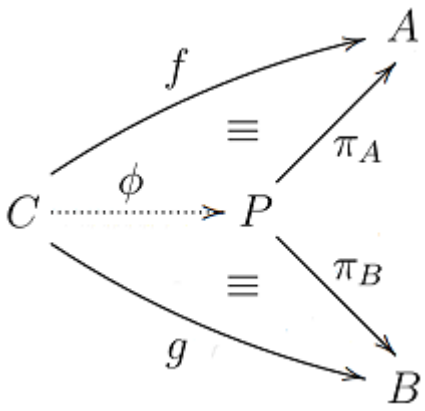
2.4 Products

Let $\mathscr{C}$ be a category. Throughout the following discussion, it may be useful to simply think of $\mathscr{C}$ as being a category you may already be familiar with, such as **Set** or **Grp**.

A **product** of A and B in $\mathscr{C}$, if it exists according to the following construction, may be defined in the following manner, and consists of:

- $P \in \mathscr{C}$;
- $\pi_A \colon P \to A$; and
- $\pi_B \colon P \to B$,

such that there exists a unique morphism $\phi \colon C \to P$ such that the following diagram commutes, where $C \in \mathrm{ob}\,(\mathscr{C})$ is arbitrary.



This means that for all objects C in $\mathscr{C}$, and for each morphism $f \colon C \to A$, and each morphism $g \colon C \to B$, there exists a unique morphism $\phi \colon C \to P$ such that $\pi_A \circ \phi = f$ and $\pi_B \circ \phi = g$. We remark that the morphisms denoted π_A and π_B are referred to as **projection morphisms**.

Does this definition make sense? Is the construction described above well-defined?

Question 1: "Can we do it?" (Existence)

Question 2: Is it well-defined, up to isomorphism? (Uniqueness)

The definition given above is very elegant: observe that we are not using any specific elements in any domains or codomains.

Given a category $\mathscr{C}$, we may or may not be able to find products, using the above construction.

For some categories, products may exist only for a certain subclass of objects.

For each category, we have to *work* to show the existence of a product.

2.4.1 Cartesian products

Recall that **Set** denotes the category of sets.

What are products in **Set**, with respect to the construction outlined above?

In this case, products are given by Cartesian products, but we also need to define the projection morphisms π_A and π_B.

Given two objects A and B in $\mathrm{ob}\,(\mathbf{Set})$, it may be regarded as axiomatic that $A \times B \in \mathrm{ob}\,(\mathbf{Set})$.

We thus define $\pi_A \colon P \to A$ so that $(a, b) \mapsto a$, and $\pi_B \colon P \to B$ so that $(a, b) \mapsto b$.

Given a morphism $f \in \mathrm{Hom}_{\mathbf{Set}}(C, A)$ together with a morphism

$$g \in \mathrm{Hom}_{\mathbf{Set}}(C, B),$$

we may define the Cartesian product

$$f \times g \colon C \times C \to A \times B$$

of the maps f and g so that $(c, d) \mapsto (f(g), g(d))$.

The diagonal map

$$\Delta \colon C \to C \times C$$

is defined so that $c \mapsto (c, c)$.

We may thus embed the set C into the Cartesian product in a natural way.

We define $\phi = (f \times g) \circ \Delta \colon C \to P = A \times B$ so that $c \mapsto (f(c), g(c))$.

To prove the unicity of ϕ, observe that $\pi_A \circ \phi(c)$ has to be $f(c)$, and $\pi_B \circ \phi(c)$ has to be $g(c)$.

The product of infinitely many elements in $\mathrm{ob}(\mathbf{Set})$ is in $\mathrm{ob}(\mathbf{Set})$. But it is not true in general that the product of infinitely many elements in $\mathrm{ob}(\mathscr{C})$ is in $\mathrm{ob}(\mathscr{C})$ for a category $\mathscr{C}$.

2.4.2 Direct products

Example 2.1. In the category **Grp**, $G_1 \times G_2$ with pairwise operations is the direct product of G_1 and G_2. In this case, define the projection morphisms π_{G_1} and π_{G_2} as in **Set**.

Example 2.2. In the category **Ring** of rings, products are given by direct products of the form $R \times S$, with π_S and π_R defined as in **Set**.

Remark 2.3. Recall that a direct sum of rings may not be the same as the direct product of the same rings.

2.4.3 The greatest common divisor as a product

Consider the category given by the poset $(\mathbb{N}, |)$, which was discussed in the previous lecture. Recall that the morphisms in this category may be defined in the following manner.

$$\mathrm{Hom}_{\mathbb{N}}(n, m) = \begin{cases} \{(n, m)\} & \text{if } n \mid m \\ \varnothing & \text{if } n \nmid m \end{cases}.$$

If we regard the natural numbers $\mathbb{N}$ as a category, with a morphism of the form $a \longrightarrow b$ if and only if $a \mid b$, then the product of two objects in this category is the greatest common divisor of these two elements in $\mathbb{N}$.

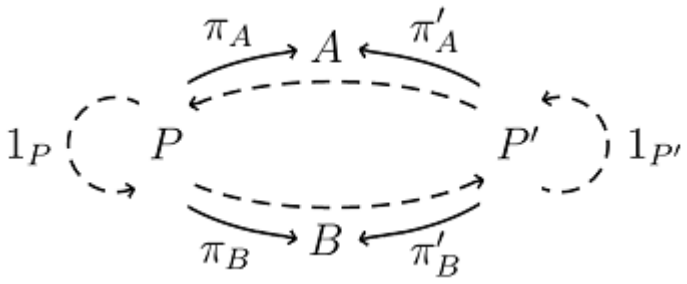
Remark 2.4. We remark that as a category, the poset $(\mathbb{N}, |)$ is sometimes denoted as $\mathbf{N}$.

2.5 Unicity of the product

How unique are products given by the construction described above?

Theorem 2.5. *For a category $\mathscr{C}$, if the product of $A, B \in \mathrm{ob}(\mathscr{C})$ exists, then the product is unique, up to isomorphism.*

Proof without words:



■

To construct the commutative diagram illustrated in the above proof, use the category-theoretic definition of product in four different ways.

In other words, apply the category-theoretic definition of product with respect to the following pairs: P and P, P and P', P' and P, and P' and P'.

All the dotted lines obtained in the above diagram are unique.

The **categorical product**[1] described above is representative of the concept of a **universal property**[2].

The word "universal" has a specific meaning in the field of category theory.

2.6 Coproducts and opposite categories

Given a category

$$(\mathscr{C}, \mathrm{Hom}_{\mathscr{C}}(\cdot,\cdot), \circ),$$

we may construct a new category $\mathscr{C}^{\mathrm{op}}$, which is referred to as the **opposite category**[3] or **dual category** of $\mathscr{C}$.

In spirit: just "reverse all the arrows". The opposite category $\mathscr{C}^{\mathrm{op}}$ is given by the tuple

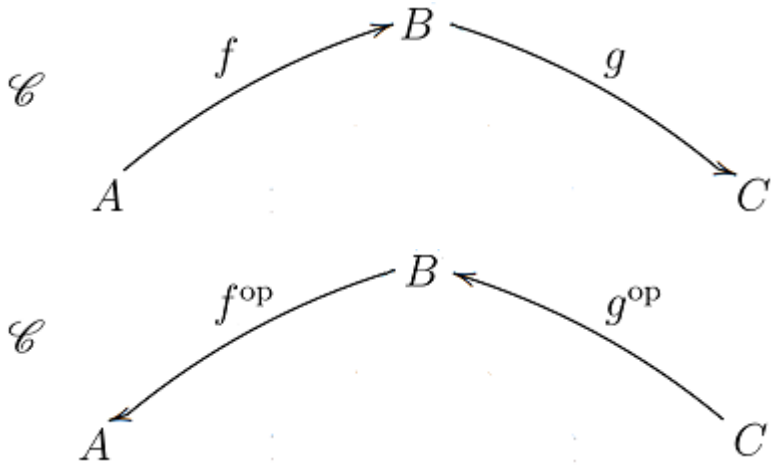
$$(\mathscr{C}, \mathrm{Hom}^{\mathrm{op}}_{\mathscr{C}}(\cdot,\cdot), \circ),$$

where

$$\mathrm{Hom}^{\mathrm{op}}_{\mathscr{C}}(A,B) := \mathrm{Hom}_{\mathscr{C}}(B,A),$$

[1] See https://en.wikipedia.org/wiki/Product_(category_theory).
[2] See https://en.wikipedia.org/wiki/Universal_property.
[3] See https://en.wikipedia.org/wiki/Opposite_category.

with $g \circ_{\text{op}} f = f \circ g$.



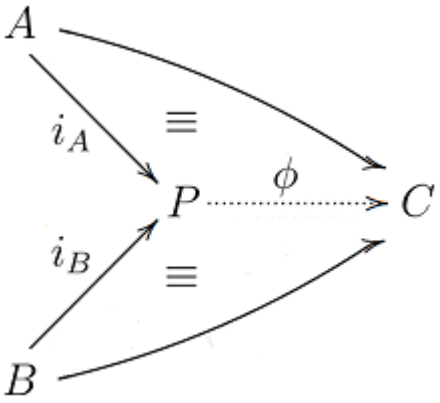
We define $\text{Hom}^{\text{op}}_{\mathscr{C}}(A, B)$ so that

$$\text{Hom}^{\text{op}}_{\mathscr{C}}(A, B) := \text{Hom}_{\mathscr{C}}(B, A),$$

and we define $g \circ_{\text{op}} f$ so that $g \circ_{\text{op}} f = f \circ g$.

To define the coproduct in $\mathscr{C}$, we make use of the product in $\mathscr{C}^{\text{op}}$.

In practice: for $A, B \in \mathscr{C}$, the ordered tuple (P, i_A, i_B) is a coproduct of A and B if the universal property indicated below is satisfied.



Theorem 2.6. *Coproducts (if they exist) are unique up to isomorphism.*

Proof. Exercise. □

Question 2.7. What is the coproduct in **Set**? What is the coproduct of two sets?

In response to the above question, it is natural to consider basic set-theoretic operations.

The coproduct of two sets A and B is the disjoint union of A and B.

With respect to the above commutative diagram for coproducts, the mapping i_A is the canonical embedding of A into the disjoint union of A and B, and similarly for i_B.

Similarly, the morphism ϕ in this case is equal to the disjoint union of f and g, which is denoted as

$$f + g \colon A + B \to C,$$

and is defined so that:

$$(f+g)(x) = \begin{cases} f(x) & x \in A \\ g(x) & x \in B. \end{cases}$$

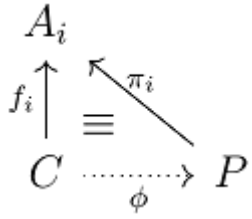
As we study category theory, we begin to see the utter importance of the maps involved.

Interestingly, in **Grp**, the coproduct is the same as the direct product in **Grp**.

With respect to the commutative diagram given above, the injective mapping i_A is such that $a \mapsto (a, e_B)$, and similarly for i_B. Similarly, the morphism ϕ is equal to $m_C \circ (f \times g)$, letting m_C denote the underlying multiplicative binary operation on C, where $f \colon A \to C$ and $g \colon B \to C$.

Exercise 2.8. Define "countable product" and "countable coproduct" and construct it, if possible in the category **Ring**, letting rings be unital.

Consider using a commuting diagram of the following form for all indices i, such that the unique morphism ϕ is the same for all i.



Observe that the categorical coproduct in $\mathbf{N}$ is given by the least common multiple mapping.

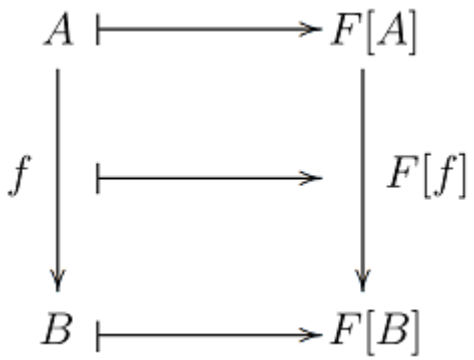
2.7 Functors

How can we compare two different categories?

Informally, a **functor** is something of a "morphism" between categories $\mathscr{C}$ and $\mathscr{D}$:

$$\begin{array}{c} F : \mathscr{C} \to \mathscr{D} \\ \cup \\ A \mapsto F[A]. \end{array}$$

Warning: This is not a function, since $\mathscr{C}$ may be not be a set.



We want the structure of the categories to be preserved, in the sense that:

- $F[1_A] = 1_{F[B]}$; and
- $F[f \circ_{\mathscr{C}} g] = F[f] \circ_{\mathscr{D}} F[g]$.

MATH 6122 lecture notes

Transcribed and formatted by John M. Campbell
jmaxwellcampbell@gmail.com

3 January 12th lecture

3.1 Basic notions in the field of category theory

- Isomorphism
- Product
- Coproduct
- Functor

Question 3.1. Can we describe the isomorphism classes in a given category?

Example 3.2. Consider the category of finite-dimensional vector spaces over a fixed field K. Given an object V in this category, we have that $V \cong K^n$ for some $n \in \mathbb{N}_0$, with K^n as a canonical representative of the isomorphism class of K^n. Furthermore, we have that

$$n \neq m \Longrightarrow V^n \ncong K^m,$$

and we thus obtain a complete classification of the isomorphism classes for the objects in the aforementioned category.

How can finite groups be classified?

Classification problems in mathematics $\longrightarrow$ a driving force behind many areas in mathematics.

Recall that there is a simple classification theorem for finitely-generated abelian groups.

Similarly, there is a complete classification theorem for R-modules for a principal ideal domain R.

3.2 Concrete categories

What is a concrete category?

Let $\mathscr{C}$ be a category, and let $\mathcal{U}\colon \mathscr{C} \to \mathbf{Set}$ be a functor.

A pair of the form $(\mathscr{C},\mathcal{U})$ is a concrete category.

Observe that $\mathcal{U}$ is an *arbitrary* functor from $\mathscr{C}$ to the category of sets.

The functor $\mathcal{U}$ is denoted in the following manner: $A \mapsto \mathcal{U}[A]$, letting A denote an object in $\mathrm{ob}(\mathscr{C})$.

Letting A be as given above, the set $\mathcal{U}[A]$ is referred to as the **underlying set** of the object A.

The functor $\mathcal{U}$ is an example of a **forgetful functor**[1].

With respect to the above definition of a concrete category, there are analogous constructions/definitions for categories containing other types of categories, given by different kinds of forgetful functors.

Question 3.3. Can we construct functors which, informally, "forget" *some* of the structure of an algebraic structure, but which do not map such algebraic objects to corresponding underlying sets?

There are many different kinds of forgetful functors of the form suggested in the above question.

For example, consider the forgetful functor from the category **Ring** of rings to the category **Ab** of abelian groups which "forgets" the multiplicative structure of the elements in $\mathrm{ob}(\mathbf{Ring})$.

This forgetful functor from **Ring** to **Ab** maps each object R in $\mathrm{ob}(\mathbf{Ring})$ to the underlying additive abelian group of R.

Recall that the category of vector spaces over a fixed field K may be denoted as $\mathbf{Vect}_K$. Then the functor which maps an object V in $\mathrm{ob}(\mathbf{Vect}_K)$ to the underlying additive abelian group of V is also a forgetful functor.

Question 3.4. Can **N** be regarded as a concrete category in a meaningful way?

[1] See https://en.wikipedia.org/wiki/Forgetful_functor.

Recall that **N** denotes the category given by the poset $(\mathbb{N}, |)$.

3.3 Free objects

Question 3.5. Given a concrete cateogry $\mathscr{C}$, what is meant by a "free" object[2] in $\mathrm{ob}(\mathscr{C})$?

Let $(\mathscr{C}, \mathcal{U})$ be a concrete category.

Suppose that there is a functor $F\colon \mathbf{Set} \to \mathscr{C}$ such that:

1. For all $X \in \mathrm{ob}(\mathbf{Set})$, there is an injective mapping of the form

$$i_X\colon X \hookrightarrow \mathcal{U}[F[X]].$$

   Observe that $\mathcal{U}[F[X]]$ is a set.

2. For each object G in $\mathscr{C}$, and each morphism $f\colon X \to \mathcal{U}[G]$, there exists a unique morphism $\phi\colon F[X] \dashrightarrow G$ such that the following diagram commutes.

$$\begin{array}{ccc} \mathcal{U}[F[X]] & \overset{\mathcal{U}[\phi]}{\cdots\!\!\rightarrow} & \mathcal{U}[G] \\ {\scriptstyle i_X}\uparrow & \nearrow_{f} & \\ X & & \end{array} \tag{3.1}$$

In a way, in certain contexts we may think about sets of the form X as being generating sets.

We may first encounter the idea of a free object in the field of linear algebra.

If we know how a linear function behaves on a basis, then we know the behaviour of this function entirely.

We thus find that *any vector space is free*.

Our definition of a free object is very category-theoretic, in the sense that there aren't really any direct references to specific elements in any sets.

[2] See https://en.wikipedia.org/wiki/Free_object.

Exercise 3.6. Show how free groups may be constructed using the above definition.

We remark that there are analogues of the above contruction of a free object based on different kinds of forgetful functors, such as the forgetful functor from **Ring** to **Ab** described above.

Consider the category of finite-dimensional vector spaces over $\mathbb{C}$.

This category may be denoted as $\mathbf{FinVect}_{\mathbb{C}}$[3]

Now, consider the forgetful functor from $\mathbf{FinVect}_{\mathbb{C}}$ to **Set**, which maps each object V in $\mathbf{FinVect}_{\mathbb{C}}$ to the underlying set $\mathcal{U}[V]$ of V.

This forgetful functor essentially "forgets" the vector space structure of an object in $\mathbf{FinVect}_{\mathbb{C}}$.

In this case, we have that

$$F\colon \mathbf{FinSet} \to \mathbf{FinVect}_{\mathbb{C}}$$

is such that

$$X \mapsto F[X] \cong \mathbb{C}^{|X|},$$

where $F[X]$ is the free vector space with basis X.

It may be useful to think of X as a generating set.

Let **ab** denote the category of finitely-generated abelian groups.

Consider the forgetful functor from **ab** to **Set** which maps each object A in **ab** to the underlying set $\mathcal{U}[A]$ of A.

Now, consider the functor

$$F\colon \mathbf{FinSet} \to \mathbf{ab}$$

whereby:

$$X \mapsto F[X] := \mathbb{Z}^{|X|},$$

and consider the injective mapping

$$i_X\colon X \to \mathbb{Z}^{|X|}$$

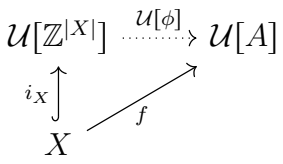
[3] See https://ncatlab.org/nlab/show/Vect.

whereby

$$x \mapsto (0, 0, \ldots, 0, 1, 0, 0, \ldots, 0),$$

endowing X with a linear order relation, letting the nonzero entry in the above binary tuple be in the position corresponding to $x \in X$.

With respect to the commutative diagram whereby



we have that:

$$x \mapsto (0, 0, \ldots, 0, 1, 0, 0, \ldots, 0) \mapsto f(x).$$

The mapping ϕ is well-defined, with

$$\phi\left((a_1, a_2, \ldots, a_{|X|})\right) = \sum_{i=1}^{|X|} a_i f(x_i).$$

This is a morphism of abelian groups.

In many ways, the above results are essentially the same as corresponding results in linear algebra, expect that we are working over the ring $\mathbb{Z}$.

Observe that the group $\mathbb{Z}/3\mathbb{Z}$ is not free, since we have that

$$\forall n \in \mathbb{N}_0 \ \mathbb{Z}/3\mathbb{Z} \ncong \mathbb{Z}^n.$$

So, we find that not all objects in the category **ab** are free.

Exercise 3.7. In **Grp**, what is $F[X]$, with respect to the commutative diagram illustrated in (3.1)? Study some different ways of defining free objects in **Grp**. How can these different definitions be reformulated in terms of a category-theoretic framework? How can these different definitions be reformulated using forgetful functors?

Question 3.8. What are some interesting examples of categories in which each object is free?

Q1: Is the above definition of a free object well-defined in the sense that functors of the form F exist?

To have "free" objects, we have to *construct*, if possible, functors of the form F, letting F be as given above.

Q2: To what extent would an object of the form $F[X]$ be unique?

Theorem: For a given X, we have that $F[X] \cong F[X']$.

Proof: This is left as an exercise. The above theorem may be proven by analogy with our proof of a unicity result concerning categorical products. ■

In a way, almost everything we do in mathematics essentially amounts to doing the same sorts of things over and over again. In a way, certain concepts in category theory formalize this intuitive notion.

Problems based on the classification of a specified kind of mathematical object occur frequently in category theory.

3.4 Module theory

How can finitely-generated R-modules be classified in the case whereby R is a PID?

We abuse notation by identifying M and $\mathcal{U}[M]$, given a module M.

What are the objects in the category of left R-modules?

Such objects are of the form $M = (M = \mathcal{U}[M], +, \cdot)$.

The category of left R-modules is a particular example of a concrete category.

The mappings $+$ and $\cdot$ are such that:

$$+ \colon M \times M \to M,$$
$$\cdot \colon R \times M \to M.$$

These mappings must be such that the following axioms hold.

1. The pair $(M, +)$ forms an abelian group.

2. The mapping $\cdot\colon R \times M \to M$ is a left action of R on M. That is,

   (a) $1 \cdot m = m$;

   (b) $(rs) \cdot m = r \cdot (s \cdot m)$. Note that this is not quite the same as the associativity axiom; and

   (c) $(r + s) \cdot m = r \cdot m + s \cdot m$.

3. *Compatibility:* What happens when we "mix" the operations given above? Think of the following axiom in terms of linearity: $r \cdot (m+n) = r \cdot m + r \cdot n$.

Observe that ring actions[4] are analogous in an obvious way to group actions.

Also observe that the above axioms imply that scalar multiplication by 0 must yield 0.

What are the morphisms in the category of left R-modules?

For a fixed ring R, given two R-modules N and M, the set

$$\mathrm{Hom}_R(N, M) = \mathrm{Hom}_{\mathbf{R\text{-}Mod}}(N, M)$$

is the set of all R-linear maps from N to M:

$$\mathrm{Hom}_R(N, M) = \big\{T\colon N \to M \text{ is a function} \;\big|\; T \text{ is } R\text{-linear, i.e.: } T(r \cdot m) = rT(m) \text{ and } T(m + n) = T(m) + T(n)\big\}.$$

If R is a field, then the category **R-Mod** is the same as the category of vector spaces over the field R.

If $R = \mathbb{Z}$, then **R-Mod** is equivalent[5] in a specific sense to the category **Ab** of abelian groups.

This is illustrated below.

[4] See https://en.wikipedia.org/wiki/Module_(mathematics).
[5] See https://en.wikipedia.org/wiki/Equivalence_of_categories.

$$(M,+,\cdot) \underset{\curvearrowleft}{\overset{\rightarrow}{\Vert}} (M,+)$$

The functors illustrated above are "equivalent" in a specific sense. These functions are said to be *naturally equivalent*.

$$n \cdot x := \underbrace{x + x + \cdots + x}_{n>0}$$
$$0 \cdot x = 0$$
$$(-n) \cdot x = -(\underbrace{x + x + \cdots + x}_{n>0}).$$

In the case whereby R is a PID, can we classify the objects in **R-Mod**?

The answer to the above question is affirmative in the finitely-generated case.

What are the free objects in **R-Mod**?

Observe that (**R-Mod**,$\mathcal{U}$) is a concrete category. Are there free objects in this category?

It is true that there are free objects with respect to (**R-Mod**,$\mathcal{U}$).

Define $F\colon$ **Set** $\rightarrow$ **R-Mod** so that

$$X \mapsto \bigoplus_{x \in X} R$$

where:

I guess the point here is that he is trying to justify that free objects exist in R-Mod.

$$\bigoplus_{x \in X} R = \{f\colon X \rightarrow R \text{ is a function } \mid f \text{ has finite support}\}.$$

Recall that $\mathrm{Supp}(f) = \{x \in X \mid f(x) \neq 0\}$.

What is the ring structure on $\bigoplus_{x \in X} R$?

Elements in the direct sum $\bigoplus_{x \in X} R$ may be added in a componentwise manner, with

$$(f+g)(x) := f(x) +_R g(x),$$

letting $+ = +_R$ denote the underlying additive binary operation on R.

Similarly, we let $(rf)(x) := r \cdot (f(x))$.

Exercise 3.9. Verify that the above operations are well-defined in the sense that in both cases, the expressions resulting from applying these operations are in $\bigoplus_{x \in X} R$.

Observe that $\mathrm{Supp}(rf)$ and $\mathrm{Supp}(f+g)$ respectively satisfy the following inclusions.

$$\mathrm{Supp}(rf) \subseteq \mathrm{Supp}(f)$$
$$\mathrm{Supp}(f+g) \subseteq \mathrm{Supp}(f) \cup \mathrm{Supp}(g).$$

Exercise 3.10. Show that $F[X]$ is free in **R-Mod**.

3.5 Isomorphism theorems for modules

The first isomorphism theorem for modules: Letting $\phi\colon N \to M$ be a module morphism, we have that $\ker\phi \subseteq N$ is a sub-R-module of N, with $\mathrm{im}\phi \subseteq M$, so that

$$N/\ker\phi \cong \mathrm{im}\phi,$$

where

$$N/\ker\phi = \{n + \ker\phi \mid n \in N\}$$

with well-defined induced addition and scalar multiplication operations.

In order for $\ker\phi$ to be a sub-r-module, it must be the case that:

1. $(\ker\phi, +) \leqslant (N, +)$; and
2. R is closed under the action given by scalar multiplication, with $R \cdot \ker\phi \subseteq \ker\phi$.

There are analogues of the standard isomorphism theorems for modules:

(2) $\frac{A+B}{B} \cong \frac{A}{A \cap B}$;

(3) $\frac{M/A}{B/A} \cong M/B$;

(4) The canonical projection morphism $\pi\colon M \to M/N$ induces a bijection of the following form:

$$\{N \subseteq A \subseteq M\} \underset{\sim}{\overset{\pi^*}{\longleftrightarrow}} \{(A+N)/N \subseteq M/N\}.$$

Why do we always list these four kinds of isomorphism theorems?

Why are we interested in these four isomorphism theorems?

Just as in the case with groups, these isomorphism theorems may be used to prove that compositions factors are unique and well-defined up to permutation.

In this case for groups this result is known as the **Jordan-Hölder theorem**.

More generally, categories which satisfy all four isomorphism theorems must satisfy analogues of the classical Jordan-Hölder theorem.

MATH 6122 lecture notes

Transcribed and formatted by John M. Campbell
jmaxwellcampbell@gmail.com

4 January 17th lecture

4.1 The category of left R-modules

Recall that **R-Mod** denotes the category of left R-modules, given a ring R.

Objects: The objects in this category are tuples of the form $(M, +, \cdot)$.

Morphisms: A morphism $\phi \colon M \to N$ in **R-Mod** is an R-linear mapping.

Free objects: The free objects in this category are objects of the form

$$F[X] = \bigoplus_{x \in X} R = \{f \colon X \to R \mid \operatorname{supp}(f) < \infty\}.$$

If $|X| < \infty$, then $F[X] \cong R^{|X|}$.

We previously stated the four isomorphism theorems for **R-Mod**.

Question 4.1. How can R-modules be classified?

Question 4.2. How can finitely-generated modules over PIDs be classified?

As with some other definitions we have discussed in class, the definition of a basis for a module consists of something of an "existence" component, together with a "unicity" component.

■ **Span** ("existence"): We let RB denote the family whereby

$$RB := \left\{ \sum_{i=1}^{n} r_i b_i \ : \ r_i \in R, b_i \in B, n \in \mathbb{N} \right\} \subseteq M.$$

If $RB = M$, we say that B **spans** M.

■ R**-linearly independent** ("unicity"): Basically, this means that a finite summation of the form $\sum_{i=1}^{n} r_i b_i$ is unique in a specific sense. This is tested by the condition whereby:

$$\sum_{i=1}^{n} r_i b_i \Longrightarrow \forall i \ r_i = 0.$$

Definition 4.3. A subset B of a module M is a basis if B spans M and is linearly independent.

Remark 4.4. Interestingly, we are not guaranteed that a given module will necessarily have a basis: in general, not all modules have bases.

Example 4.5. Let $R = \mathbb{Z}$, and consider the module consisting of elements in $\mathbb{Z}^2$, which we denote using column-vector notation, endowed with the binary operation $+$ whereby

$$\begin{bmatrix} a \\ b \end{bmatrix} + \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a+c \\ b+d \end{bmatrix}$$

for $a, b, c, d \in \mathbb{Z}$, together with the operation $\cdot$ whereby:

$$n \cdot \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} na \\ nb \end{bmatrix},$$

with $n \in \mathbb{Z}$. We thus find that

$$B = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$$

is a basis.

Example 4.6. Now let M denote the module whereby $M = (\mathbb{Z}/3\mathbb{Z}, +, \cdot)$, letting the elements in $\mathbb{Z}/3\mathbb{Z}$ be denoted as equivalence classes, writing $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$. We define the underlying additive binary operation on M so that

$$(a + 3\mathbb{Z}) + (b + 3\mathbb{Z}) = (a + b) + 3\mathbb{Z}.$$

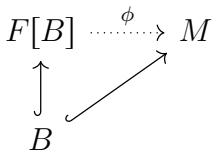
Similarly, we define the operation $\cdot$ so that

$$n \cdot (a + 3\mathbb{Z}) = na + 3\mathbb{Z}.$$

Basically, these operations turn $\mathbb{Z}/3\mathbb{Z}$ into a $\mathbb{Z}$-module, writing $\overline{1} = 1 + 3\mathbb{Z}$, and similarly for $\overline{2}$ and $\overline{3}$. We find that $\overline{0} \notin B$, since the additive identity element in the underlying additive abelian group of a module can never be in a linearly independent set. To show why $\overline{0} \notin B$ in this case, observe that if $\overline{0}$ were an element in B, then the equality $4 \cdot \overline{0} = \overline{0}$ would imply that $4 = 0$ with $4 \in \mathbb{Z}$ and $0 \in \mathbb{Z}$, which is absurd. Similarly, if $\overline{1}$ were an element in B, then the equation $3 \cdot \overline{1} = \overline{0}$ would yield that equality "$3 = 0$". Finally, if $\overline{2}$ were in B, then the equality $3 \cdot \overline{2} = \overline{0}$ would imply that $3 = 0$. This shows that no subset of $\mathbb{Z}/3\mathbb{Z}$ could be linearly independent. Informally, the **torsion elements**[1] of the group $\mathbb{Z}/3\mathbb{Z}$ are problematic in this case.

[1] See https://en.wikipedia.org/wiki/Torsion_(algebra).

If B is a basis for M, then $M \cong F[B]$.



We observe that:

1. The morphism ϕ is surjective, since B is a spanning set; and
2. The kernel of ϕ is trivial, since B is linearly independent.

We thus find that the universality of free objects show how linear independence and the spanning set condition are related in an elegant way.

Moral: If M has a basis, then M is a free object in **R-Mod**.

If $B \cong B'$ with respect to the category **Set**, i.e., if $|B| = |B'|$, then $F[B] \cong F[B']$. Basically, this follows from the functoriality of F, as the functor F will map an isomorphism to an isomorphism.

Is the converse true?

Is it true that $F[B] \cong F[B']$ implies $|B| = |B'|$?

This is not true in general. However, if the underlying ring is a field, then the implcation $F[B] \cong F[B'] \implies |B| = |B'|$ holds.

This is also true for specific types of rings.

Theorem 4.7. *If R is a commutative ring with unity, then $F[B] \cong F[B'] \implies |B| = |B'|$, given bases B and B' in an R-module M.*

We proceed to consider the following elementary result in linear algebra.

Lemma 4.8. *If $R = F$ is a field, then $F[B] \cong F[B'] \implies |B| = |B'|$, given bases B and B' in a vector space over F.*

Proving the following proposition requires the use of a form of **Zorn's lemma**[2].

Proposition 4.9. *A commutative ring with unity has a maximal ideal.*

[2]See https://en.wikipedia.org/wiki/Zorn's_lemma.

The **axiom of choice**[3] is equivalent to Zorn's lemma.

Zorn's lemma: Let S be an ordered set of infinite cardinality, endowed with an antisymmetric, transitive, reflexive order relation "$\leqslant$". A chain in S is an ordered sequence of the form $a_1 \leqslant a_2 \leqslant \cdots$. If every chain in S has an element in S that covers it, then there is a maximal element in S.

Typical application of Zorn's lemma: showing existence of maximal ideals.

Proof of Proposition 4.9: Let S denote the set

$$S = \{J \subsetneq R \ : \ J \text{ is an ideal}\}$$

ordered with the inclusion binary relation, denoted by $\subseteq$. To use the hypotheses of Zorn's lemma, we begin by considering a chain of the following form:

$$J_1 \subseteq J_2 \subseteq \cdots .$$

We need to find an ideal $I \in S$ such that $J_r \subseteq I$ for all indices r.

One candidate: take $I = \bigcup_{r \geqslant 1} J_r$. Is this in S?

Where do we use the hypothesis that R is commutative?

To show that I is an ideal, we begin by showing that I is closed under the additive operation denoted by $+$.

Let a and b be elements in I. So, we have that $a \in J_k$ and $b \in J_\ell$ for some indices k and ℓ.

If $\ell > k$, then $J_k \subseteq J_\ell$. Similarly, if $\ell \leqslant k$, then $J_\ell \subseteq J_k$.

For $\ell \leqslant k$, we have that $b \in J_\ell \subseteq J_k$, with $a \in J_k$.

So, in this case, we have that $a, b \in J_k$. But J_k is an ideal, which shows that $a + b \in J_k$. Therefore $a + b \in I$.

Now, let $r \in R$. Also, let $a \in I$.

Since a must be in an ideal J_k for some index k, we have that ra must be in J_k, thus proving that $ra \in I$, as desired.

[3] See https://en.wikipedia.org/wiki/Axiom_of_choice.

So, we have shown that $I \subseteq R$ is an ideal.

We claim that $I \neq R$. By way of contradiction, suppose that $I = R$.

We thus have that $1 \in I = R$, since R is unital. This implies that $1 \in J_k$, for some index $k \in \mathbb{N}$. This, in turn, implies that $J_k = R$.

We thus arrive at a contradiction, since J_k is not equal to R.

So, by Zorn's lemma, there must exist a maximal ideal in R. ■

Question 4.10. What are some interesting examples of noncommutative unital rings with no maximal ideals?

Recall that $I \subseteq R$ is a maximal ideal if and only if R/I is a field.

Letting R be a commutative ring with unity, suppose that $R^n \cong R^m$.

Now, consider the quotient ring R^n/IR^n, where IR^n denotes the submodule obtained by multiplying by elements of I on the left.

We thus have that $R^n/IR^n \cong R^m/IR^m$.

If M is an R-module, we have that $IM \subseteq M$, since I is an ideal.

Using an analogue of the Chinese Remainder Theorem, it can be shown that $R^n/IR^n \cong (R/I)^n$.

We thus have that $(R/I)^n \cong (R/I)^m \implies n = m$.

A similar argument may be used with respect to infinite-dimensional vector spaces.

The Chinese Remainder Theorem may be formulated in the following manner.

Assuming R is a commutative ring with unity, letting A_1, A_2, …, A_k be ideals in R, and letting M be an R-module, we have that:

1. For each index i, $A_iM \subseteq M$;
2. The mapping $\phi\colon M \to \bigoplus_{i=1}^{k} M/(A_iM)$ whereby

$$m \mapsto (m + A_1M_1, m + A_2M, \ldots, m + A_kM)$$

is a well-defined R-linear map, with

$$\ker \phi = A_1M \cap A_2M \cap \cdots \cap A_kM; \text{ and}$$

3. If $A_i + A_j = R$ for all $i \neq j$, i.e., A_i and A_j are coprime, then ϕ is surjective, and $\ker\phi = A_1A_2 \cdots A_kM$, with:

$$\boxed{\frac{M}{A_1A_2 \cdots A_kM} \cong \bigoplus_{i=1}^{k} \frac{M}{A_iM}.}$$

Exercise 4.11. Show that $R^n/(IR^n) \cong (R/I)^n$.

Hint: Consider the second item in the above list, given within the above formulation of the Chinese Remainer Theorem.

The Chinese Remainder Theorem is often used for $\mathbb{Z}$-modules.

Observe that in $\mathbb{Z}$, relatively prime integers yield coprime ideals.

For example, letting $n = p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, with $(p_i, p_j) = 1$, using the Euclidean algorithm, we have that

$$p_i^{\alpha_i}\mathbb{Z} + p_j^{\alpha_j}\mathbb{Z} = \mathbb{Z},$$

which, in turn, implies that

$$\mathbb{Z}/n\mathbb{Z} \cong \bigoplus_{i=1}^{k} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}.$$

4.2 Noetherian modules

What does it mean for an R-module to be Noetherian?

A module M is Noetherian if: for each chain

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M$$

of submodules, there exists k such that $M_i = M_k$ for all $i \geqslant k$.

Lemma 4.12. *A module M is Noetherian iff every submodule of M is finitely-generated.*

Remark 4.13. Since we can think of a ring as being a module over itself, we may define a Noetherian ring using the above definition. By the above lemma, we thus have that a ring R is Noetherian iff every ideal of R is finitely-generated

Proof of Lemma 4.12: ($\Longrightarrow$) To prove that if a module M is Noetherian then every submodule of M is finitely-generated, we proceed to prove the contrapositive of this conditional statement. So, suppose that it is not the case that every submodule of M is finitely-generated.

So, let $N \subseteq M$ be a submodule of M which can only be generated by an infinite set, and nothing finite.

Let $n_1, n_2, \ldots \in N$ be defined inductively so that

$$n_k \in N \backslash \text{Span}\{n_1, n_2, \ldots, n_{k-1}\}$$

for all indices k. It is possible to define elements of N in this manner, since N is not finitely generated.

$$\begin{aligned} M_1 &= \text{Span}_R\{n_1\} \\ M_2 &= \text{Span}_R\{n_1, n_2\} \\ &\cdots \\ M_k &= \text{Span}_R\{n_1, n_2, \ldots, n_k\} \\ &\text{etc.} \end{aligned}$$

Since $M_i \neq M_j$ for distinct indices i and j, we thus obtain a strictly increasing chain of the form

$$M_1 \subsetneq M_2 \subsetneq \cdots .$$

We thus find that M is not Noetherian.

($\Longleftarrow$) Conversely, suppose that any submodule of M is finitely generated.

Now, let

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M$$

be an increasing chain of submodules.

Write $M_* = \bigcup_{i \geqslant 1} M_i \subseteq M$.

Observe that M_* is a submodule of M.

So, from our initial assumption, we have that M_* is finitely generated.

Let $M_* = \text{Span}_R\{a_1, a_2, \ldots, a_\ell\}$.

Let $a_j \in M_{k_j}$ for some index k_j, letting $j \in \mathbb{N}$ be such that $1 \leqslant j \leqslant \ell$.

Now, let $k = \max\{k_j \ : \ j \in \mathbb{N}, 1 \leqslant j \leqslant \ell\}$.

So, we have that $a_j \in M_{k_j} \subseteq M_k$ for $j = 1, 2, \ldots, \ell$.

So, we have that $M_k \subseteq M_* = \text{Span}_R\{a_1, a_2, \ldots, a_\ell\} \subseteq M_k$.

Therefore, $M_* = M_k$.

So, for all indices i such that $i \geqslant k$, we have that $M_i = M_k$, and hence M is Noetherian, as desired.

Claim 4.14. If R is an integral domain, then $M = F[X]$ is free of rank $|X| = n < \infty$, and $F[X] \cong F[Y] \iff |X| = |Y|$.

In this case, we have that rank $= |X|$ is well-defined.

Suppose that $A \subseteq M$, with $|A| \geqslant n + 1$.

This implies that A is linearly dependent, i.e., not linearly independent.

This is true if $R = F$ is a field.

Observe that $A \subseteq M \cong R^n \subseteq Q_{R^*}^n$. The ring Q_{R^*} of quotients is actually a field, since R is an integral domain.

So, A is Q_{R^*}-linearly dependent:

$$\sum x_i a_i = 0,$$

such that not all expressions of the form x_i are zero in Q_{R^*}.

Multiplying the finite equation given above by the least common multiple of the denominators, we have that

$$\sum r_i a_i = 0,$$

such that not all expressions of the form r_i are zero in R.

MATH 6122 lecture notes

Transcribed and formatted by John M. Campbell
jmaxwellcampbell@gmail.com

5 January 19th lecture

5.1 The category of left R-modules

Recall that we define a basis $B \subseteq M$ of an R-module M so that:

1. The set B spans M, with $RB = M$; and
2. The set B is linearly independent in the sense that $\sum r_i b_i = 0 \implies r_i = 0$ in R for all indices i.

• The $\mathbb{Z}$-module $\mathbb{Z}/3\mathbb{Z}$ has no basis.

• If $B \subseteq M$ is a basis, then $M \cong F[B]$.

• Noetherian: $M_1 \subseteq M_2 \subseteq \cdots \subseteq M$, letting M be an R-module, such that there exists an index k such that $M_i = M_k$ for all indices i such that $i \geqslant k$.

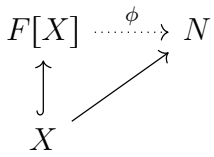
Lemma 5.1. *An R-module M is Noetherian if and only if each submodule of M is finitely-generated.*

Students in MATH 6122 need to do many exercises concerning module theory from the suggested textbooks.

One of our main goals at this point is to classify finitely-generated R-modules for a given principal ideal domain R.

Claim 5.2. If R is an integral domain, and if M is a free R-module of the form $M = F[X]$, letting $|X| = n < \infty$, with $A \subseteq M$ and $|A| \geqslant n + 1$, then A is linearly dependent.

If N is finitely-generated, there exists a set $X \subseteq N$ such that $|X| < \infty$ and $RX = N$, so that the universal property illustrated below holds.



Since N is contained in $F[X]$, we find that the morphism ϕ is surjective.

By the first isomorphism theorem, we have that $N = \mathrm{im}(\phi) = F[X]/\ker\phi$.

So, we find that any finitely-generated R-module is a quotient of a free object.

So, from the above result, we are lead to consider three main objectives.

- Understand free objects in **R-Mod**;
- Understand submodules; and
- Understand quotients.

Ultimately, we want to totally understand submodules of R-modules, where R is a PID.

Firstly, our goal is to understand submodules of free objects.

Claim 5.3. If R is a PID, with M as a free module which is finitely generated with $M = F[X]$, letting $|X| = n < \infty$, and letting $N \subseteq M$ be an R-submodule, there exists a set $Y \subseteq M$ such that $|Y| \leqslant n$ and $N = F[Y]$.

Remark 5.4. Observe that Y is not necessarily contained in X.

Goal: We basically want "$Y = X$ times scalar".

As a corollary, we have that a finitely-generated free module over a PID is Noetherian.

Remark 5.5. We adopt the convention whereby PIDs are integral domains.

Lemma 5.6. *With the conditions given in Claim 5.3, the module N is finitely generated.*

Proof. Apply Claim 5.2. □

If $N = RC$, where $|C| > n$, then C is linearly dependent.

Given that $RC = RC'$ for any C' obtained from C by removing linearly dependent vectors, with $|C'| \leqslant n$.

Theorem A: Under the hypotheses of Claim 5.3, given a finitely-generated free module M, we can find an ordered basis $[x_1, x_2, \ldots, x_n]$ of M and a basis of the form

$$[y_1 = a_1 x_1, y_2 = a_2 x_2, \ldots, y_m = a_m x_m]$$

of N such that $m \leqslant n$, and

$$a_1 \mid a_2 \mid \cdots \mid a_m.$$

Recall that x divides y in a commutative ring if there is an element u such that $y = xu$.

What is special about PIDs (and UFDs) is that we can properly define (up to units) least common multiples and greatest common divisors. In the case of a PID, this is coming from the ideal property, but this is *not* coming from the divisibility property.

Question 5.7. What are some interesting examples of principal ideal domains which are not Euclidean domains?

It is clear that **Theorem A** implies that Claim 5.2 is true.

Begin by considering the hypotheses for **Theorem A**. These hypotheses give us:

• An ordered basis $[e_1, e_2, \ldots, e_n]$ of M. Observe that M has a basis, since it's a free module.

• A generating set $[f_1, f_2, \ldots, f_\ell]$ for N, with $\ell \leqslant n$, writing $f_i = \sum a_{i,j} e_j$, for $a_{i,j} \in R$.

It is convenient to denote the above ordered basis for M using column-vector notation, writing:

$$E = \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{bmatrix}.$$

Let $A = [a_{i,j}]_{\ell \times n} \in \mathrm{Mat}_{\ell \times n}(R)$.

It is also convenient to let the generating set for N be denoted using column-vector notation, with:

$$F = \begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_\ell \end{bmatrix}.$$

Technically, the expression

$$\begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_\ell \end{bmatrix}$$

is not necessarily a vector in the sense that the above entries are not necessarily in a ring.

We thus have that $F = AE$, letting the product AE be given by the usual "product" operation for matrices.

Basically, we are interested in some kind of transformation of the form suggested with respect to the following illustration, such that E' is a basis for M and F' is a generating set for N.

$$F = AE \quad \overset{\text{transformation}}{\rightsquigarrow} \quad F' = A'E'.$$

We have two main goals in terms of finding a transformation of the form indicated above:

1. Understand possible transformations allowed in terms of "manipulating" the matrix A; and
2. Create an algorithm such that given any equality of the form $F = AE$ as above, we may apply such an algorithm to produce an equality of the form

$$Y = \begin{bmatrix} a_1 & 0 & \cdots & 0 & \\ 0 & a_2 & \cdots & 0 & \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & a_m & \\ & & & & \mathbf{0} \end{bmatrix} X,$$

with $a_1|a_2|\cdots|a_m$, such that an algorithm of this form would be analogous to Gaussian elimination, although we need to "avoid" division operations which are required through the process of Gaussian elimination.

The algorithm described above is like Gaussian elimination in spirit, but the benefit is that we will be able to apply this strategy in general for PIDs, including polynomial rings.

Consider the possibility of implementing a program for this algorithm for a project for MATH 6122. There are many different kinds of algorithms for evaluating Betti numbers, and there are many applications of these algorithms in algebraic geometry.

Let R be a Euclidean domain[1]. So, there exists a Euclidean function

$$d\colon R\backslash\{0\} \to \mathbb{N}_0$$

such that: for all $a \in R$, and all $b \in R$ such that $b \neq 0$, there exist elements q and r such that $a = bq + r$, so that $r = 0$ or $d(r) < d(b)$.

With respect to the ring $\mathbb{Z}$, the corresponding Euclidean function d is the absolute value function.

For polynomial rings, the appropriate Euclidean function d is the degree function.

We proceed to define some "allowed" transformations of the equality $F = AE$.

[1] See https://en.wikipedia.org/wiki/Euclidean_domain.

C_{ij}: Nothing on F, interchanging column i and j in A, switching basis vectors e_i and e_j. This basically amounts to changing the order of the basis.

$$C_{ij} = \begin{matrix} \\ \\ \\ i \\ \\ \\ \\ j \\ \\ \\ \end{matrix} \begin{bmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & 0 & & & 1 & & \\ & & & & 1 & & & & \\ & & & & & \ddots & & & \\ & & & & & & 1 & & \\ & & & 1 & & & & 0 & \\ & & & & & & & & 1 \\ & & & & & & & & & \ddots \end{bmatrix}_{n \times n}$$

In this case, we have that $A' = AC_{ij}$ and $E' = C_{ij}E$. So, we have that

$$F = AE = A(I_n)E = A(C_{ij})(C_{ij})E,$$

thus explaining why F is unchanged.

We have that $F' = F$ still generates N.

Also, $E' = C_{ij}E$ is still a basis.

So, we have that $F' = F = A'E'$.

It may be useful to think of C_{ij} as being an operator.

Now, for a unit u, let $C_i(u)$ denote the following $n \times n$ matrix.

$$C_i(u) = \begin{matrix} \\ \\ \\ i \\ \\ \\ \\ \\ \end{matrix} \begin{bmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & u & & & & \\ & & & & 1 & & & \\ & & & & & \ddots & & \\ & & & & & & 1 & \\ & & & & & & & 1 \end{bmatrix}_{n \times n}$$

Since isomorphisms must preserve bases, we have that u needs to be invertible, since the above $n \times n$ matrix has to be invertible.

What is a unit in a ring?

A unit is basically an invertible element.

For example, the units in $\mathbb{Z}$ are -1 and 1.

The matrix operator indicated above is only defined for a unit u in R. That is, this matrix is only defined for elements u in R such that there exists an element s in R such that $us = 1$.

$A' = A \cdot C_i(u)$.

$E' = C_i(u^{-1})E$.

$F' = F$.

So, $F' = A'E'$, and $F' = F$ generates N. Also, E' is a basis since $C_i(u)$ is an isomorphism.

E' is something of a "distorted" basis, since it is not exactly the same as E.

Letting $r \in R$, define $c_{ij}(r)$ as follows.

$$c_{ij}(r) = \begin{matrix} \\ \\ \\ \\ i \\ \\ j \\ \\ \\ \end{matrix} \begin{matrix} \begin{matrix} \quad & \quad & \quad & \quad & \quad & \quad & \quad \end{matrix} \\ \begin{bmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & \ddots & & & & \\ & & & 1 & & r & \\ & & & & \ddots & & \\ & & & 0 & & 1 & \\ & & & & & & \ddots \\ & & & & & & & 1 \end{bmatrix} \end{matrix}.$$

There is no restriction on $r \in R$, with respect to the above definition.

Matrices of the form $c_{ij}(r)$ for $r \in R$ are invertible in general.

$A' = A \cdot c_{ij}(r)$.

$E' = c_{ij}(r)E$.

$F' = F$.

If we transform the matrix A in a specific way, we have to be mindful about how to transform E accordingly.

Row operations: For indices i and j, we define the row operation matrix R_{ij} in the following manner:

$$R_{ij} = \begin{array}{c} \\ \\ \\ i \\ \\ j \\ \\ \\ \end{array} \begin{bmatrix} 1 & & & & & & & & \\ & 1 & & & & & & & \\ & & \ddots & & & & & & \\ & & & 0 & & 1 & & & \\ & & & & \ddots & & & & \\ & & & 1 & & 0 & & & \\ & & & & & & \ddots & & \\ & & & & & & & 1 & \end{bmatrix}_{\ell \times \ell}.$$

$F' = R_{ij}F.$

$A' = R_{ij}A.$

$E' = E.$

$F = AE \quad \rightsquigarrow \quad R_{ij}F = (R_{ij}A)E.$

Letting u be a unit, we define $R_j(u)$ by analogy with our definition of the matrix operator denoted as $C_i(u)$.

$F' = R_j(u)F.$

$A' = R_j(u)A.$

$E' = E.$

We also define $S_{ij}(r)$ by analogy with the definition of $c_{ij}(r)$ given above.

$F' = S_{ij}(r)F.$

$A' = R_{ij}(r)A.$

$E' = E.$

At each step $\longrightarrow$ what happens to E and F, while we are "transforming" A?

Algorithm: For any $F = AE$, we transform this equality as suggested below.

$$F = AE \quad \rightsquigarrow \quad Y = \overline{A}X,$$

where:

$$\overline{A} = \begin{bmatrix} a_1 & & & & \\ & a_2 & & & \\ & & \ddots & & \\ & & & a_m & \\ & & & & \mathbf{0} \end{bmatrix}.$$

Suppose that Y generates N, and that:

$$\begin{cases} y_1 = a_1 x_1 \\ y_2 = a_2 x_2 \\ \vdots \\ y_m = a_m x_m. \end{cases}$$

In this case, we have that Y is linearly independent, and that Y forms a basis.

For now, it is enough to restrict our attention to the following operators: c_{ij}, $c_i(u)$, $C_{ij}(r)$, R_{ij}, $R_i(u)$, and $S_{ij}(u)$.

Find in A the smallest expression of the form $d(a_{ij})$ for $a_{ij} \neq 0$.

Applying the operators C_{ij} and R_{ij} allows us to put this entry in the $(1,1)$-position.

① Let $A = [a_{ij}]$. Assume without loss of generality that $d(a_{11}) \leqslant d(a_{ij})$.

② Does $a_{11} | a_{ij}$ for all indices i and j?

If **Yes**, go to ③.

If **No**: If $\exists j$ such that $a_{11} \nmid a_{1j} \longrightarrow$ use division algorithm, so that $a_{1j} = a_{11}q + r$, where $d(r) < d(a_{11})$, and $r \neq 0$, with $a_{1j} - a_{11}q = r$. Since

$a_{1j} - a_{11}q = r$, we obtain a matrix of the following form.

$$AC_{j1}(-q) = \begin{bmatrix} a_{11} & \cdots & r & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{bmatrix} \rightsquigarrow \text{Go back to } ①$$

If there exists an index i such that a_{11} does not divide a_{i1}, then use the matrix operation indicated as follows.

$$R_{i1}(-q) = \begin{bmatrix} a_{11} & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ r & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{bmatrix} \rightsquigarrow \text{Go back to } ①$$

We will later discuss the case whereby the above conditions do not hold.

MATH 6122 lecture notes

Transcribed and formatted by John M. Campbell
jmaxwellcampbell@gmail.com

6 January 24th lecture

Theorem A: Given a finitely-generated free R-module M and a submodule $N \subseteq M$, we can find an ordered basis

$$[x_1, x_2, \ldots, x_n]$$

and a generating set

$$[y_1, y_2, \ldots, y_\ell]$$

for N such that:

1. $y_i = a_i x_i$;
2. $a_1 | a_2 | \cdots | a_\ell, \ \ell \leqslant n$; and
3. $[y_1, y_2, \ldots, y_\ell]$ is an ordered basis.

Start with any basis "E" of M and any finite generating set "F" of N.

$|F| \leqslant |E|$.

$\exists A \in M_{n \times \ell}(R)$.

$(*) \ \ F = AE$.

We defined 6 operations with respect to $(*)$: 3 row operations and 3 column operations.

$C_{i,j}$, $C_i(u)$ for a unit u, and $C_i(r)$ for arbitrary r.

$R_{i,j}$, $R_i(u)$ for a unit u, and $R_i(r)$ for arbitrary r.

$$A \rightsquigarrow \begin{bmatrix} a_1 & 0 & \cdots & 0 & 0 \\ 0 & a_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & a_\ell & 0 \\ 0 & 0 & \cdots & 0 & \mathbf{0} \end{bmatrix}.$$

If R is a Euclidean domain, the Euclidean function[1] $d\colon R\backslash\{0\} \to \mathbb{N}_0$ may be used to apply Euclidean-type algorithms.

① Find $d(a_{ij})$ minimal, with $a_{ij} \neq 0$. Let

$$A' = R_{1i}AC_{j1} = \begin{bmatrix} a'_{11} & \cdots \\ \vdots & \ddots \\ & \end{bmatrix},$$

with $a'_{11} \neq 0$, and $d(a'_{11}) \leqslant d(a'_{ij})$ for all entries a_{ij} such that $a_{ij} \neq 0$.

If $a'_{11} | a'_{ij}$ for all indices i and $j \longrightarrow$ ③.

If not $\longrightarrow$ ②.

② Let A be the matrix given by ①.

Find all i, j such that $a_{11} \nmid a_{ij}$.

At least one pair exists.

$(i = 1)$ $\exists$ pair (i, j) such that $a_{1,1} \nmid a_{1,j}$. Then

$$A' = AC_{i1}(-q) = \begin{pmatrix} a_{1,1} & \cdots & r & \cdots \\ \vdots & \ddots & & \\ & & & \end{pmatrix} \longrightarrow ①,$$

where $a_{1,j} = a_{1,1}q + r$, $r \neq 0$, and $d(r) < d(a_{1,1})$.

$(j = 1)$ $\exists$ $(i, 1)$ such that $a_{1,1} \nmid a_{i,1}$.

Find $a_{i,1} = a_{1,1}q + r$, where $r \neq 0$, and $d(r) < d(a_{i,1})$.

$$A' = R_{i,1}(-q)A = \begin{pmatrix} a_{1,1} & \cdots & \\ \vdots & \ddots & \\ r & & \\ \vdots & & \end{pmatrix} \longrightarrow ①.$$

Otherwise, everything in row 1 and column 1 is divisible by $a_{1,1}$.

[1] See https://en.wikipedia.org/wiki/Euclidean_domain.

(i,j) $i \neq 1$, $j \neq 1$. But $a_{1,1} \nmid a_{i,j}$.

$a_{1,1} | a_{i,1}$ and $a_{1,1} | a_{1,j}$.

$a_{i,1} = a_{1,1} q_i$.

$a_{1,j} = a_{1,1} q_j$.

$a_{i,j} = a_{1,1} q + r$, with $r \neq 0$, and $d(r) < d(a_{1,1})$.

$$R_{1,i}(1) R_{i,1}(-q_i) A C_{j,1}(-q_j) C_{j,1}(q_1 q_j - q) = \begin{pmatrix} a_{1,1} & \cdots & r & \cdots \\ \vdots & \ddots & & \\ & & & \end{pmatrix} \longrightarrow ①.$$

$$\begin{aligned} & i \begin{pmatrix} a_{1,1} & \cdots & a_{1,1} \cdot q_j \\ \vdots & \ddots & \vdots \\ a_{1,1} q_i & \cdots & a_{1,1} q + r \end{pmatrix} \overset{C_{j,1}(-q_j)}{\rightsquigarrow} \\ &= \begin{pmatrix} a_{1,1} & & 0 \\ & & \\ a_{1,1} q_i & & a_{1,1}(q - q_i q_j) + r \end{pmatrix} \overset{R_{i,1}(-q_i)}{\rightsquigarrow} \\ &= \begin{pmatrix} a_{1,1} & & 0 \\ & & \\ 0 & & a_{1,1}(q - q_i q_j) + r \end{pmatrix} \overset{R_i(1)}{\rightsquigarrow} \\ &= \begin{pmatrix} a_{1,1} & & a_{1,1}(q - q_i q_j) + r \\ & & \\ 0 & & a_{1,1}(q - q_i q_j) + r \end{pmatrix} \overset{C_{j,1}(q_i q_j - q)}{\rightsquigarrow} \\ &= \begin{pmatrix} a_{1,1} & & r \\ & & \\ 0 & & a_{1,1}(q - q_i q_j) + r \end{pmatrix}. \end{aligned}$$

Finitely many times $\longrightarrow$ r decreasing each time.

We remark that sequences of steps of the form

$$① \longrightarrow ② \longrightarrow ① \longrightarrow ② \longrightarrow \cdots$$

must be finite, since the value of $d(a_{1,1})$ decreases each time.

③ What do we do when everything is divisible by $a_{1,1}$?

$$A \overset{R_{j,1}(-q_j),\ \text{letting } a_{i,1}=a_{1,1}q_i}{\rightsquigarrow} \begin{pmatrix} a_{1,1} & a_{2,1} & \cdots & a_{1,\ell} \\ 0 & & & \\ 0 & & & \\ \vdots & & & \\ 0 & & & \end{pmatrix}$$

$$\overset{C_{1,j}(-q'_j),\ \text{letting } a_{1,j}=a_{1,1}q'_j}{\rightsquigarrow} \begin{pmatrix} a_{1,1} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix}.$$

We thus find that $A' \in \mathrm{Mat}_{(n-1)\times(\ell-1)}(R)$. All entries of A' are divisible by $a_{1,1}$ $\longrightarrow$ return to ①, with respect to A'.

We remark that for step ①, if the entries of A are all equal to 0, or if A is empty, then the above procedure should be terminated immediately.

Question 6.1. How can the algorithm described above be generalized to rings which are not Euclidean domains?

This algorithm actually can be generalized to PIDs. But how can this algorithm be generalized without using Euclidean norms?

The above algorithm will stop with an output of the form

$$\begin{pmatrix} a_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & a_\ell & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix},$$

where $a_1|a_2|\cdots|a_\ell$.

How can we modify this algorithm to deal with matrices over principal ideal domains?

We need an analogue of the Euclidean norm d.

Recall that every principal ideal domain is a unique factorization domain.

Also recall that in a PID, every prime element is an irreducible element.

Recall that an element p in a ring R is said to be irreducible in R if the equality whereby $p = ab$ implies that a is a unit or b is a unit.

Now, given that R is a PID, define

$$\ell \colon R \backslash \{0\} \to \mathbb{N}_0$$

in the following manner. Since R is a PID, we have that R must be a UFD, so that each element in $R\backslash\{0\}$ is uniquely a product of a finite number of irreducible elements. Letting r be a nonzero element in R, it is natural to define ℓ so that $\ell(r)$ is equal to the number of irreducible factors of r. As in Sivaramakrishnan's *Certain Number-Theoretic Episodes In Algebra*, we adopt the standard convention whereby $\ell(0_R) = 0$. We also let $\ell(r)$ vanish if r is a unit. We observe that although ℓ is not necessarily a Euclidean norm, it is analogous to a Euclidean norm.

We have that: for all a and b in R,

$$(a, b) = (d),$$

where d is the g.c.d. of a and b, with d well-defined up to units. Given that $(a, b) = (d)$, we have that there exist elements s and t in R such that $sa + tb = d$. When we have a Euclidean domain, we have an algorithm for finding s and t.

Given that $F = AE$, and given any invertible matrix T, we have that

$$TF = (TA)E,$$

and

$$F = (AT)(T^{-1}E).$$

These equalities give rise to valid transformations of the form

$$F = AE \rightsquigarrow F' = A'E'$$

with many useful properties.

Consider a matrix of the form

$$\begin{pmatrix} a_{1,1} & \cdots \\ \vdots & \ddots \\ a_{i,1} & \end{pmatrix}$$

with entries in a PID which is not a Euclidean domain, where $a_{1,1} \nmid a_{i,1}$. We don't have a division algorithm in this case.

$d = sa_{1,1} + ta_{i,1}$, where $d = \gcd(a_{1,1}, a_{i,1})$.

$a_{1,1} = ud$.

$a_{i,1} = vd$.

Observe that u and v are not necessarily units.

$d = sud + trd = (su + tr)d$.

Recall that an integral domain is a commutative ring with unity and no zero-divisors.

Also, recall that we adopt the standard convention whereby principal ideal domains are integral domains.

From the equality $d = (su+tr)d$, together with the fact that integral domains do not have zero-divisors, we have that $1 = su + tr$. Now observe that the determinant of the matrix

$$\begin{bmatrix} s & t \\ v & -u \end{bmatrix}$$

is -1, and that

$$\begin{bmatrix} u & t \\ v & -s \end{bmatrix}$$

is the inverse of the previous matrix.

Now, define the operator $T_{i,j}\begin{bmatrix} s & t \\ v & -u \end{bmatrix}$ so that:

$$\begin{array}{c} \\ i \\ \\ \\ \\ j \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccccc} & & i & & & j & \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & \cdots & & & 0 \\ 0 & \ddots & & & & & \\ 0 & & s & & & t & \\ \vdots & & & \ddots & & & \\ & & & & 1 & & \\ & & v & & & -u & \\ 0 & & & & & & 1 \end{bmatrix} \end{array}$$

Observe that the above matrix is invertible.

$$\left(T_{i,j}\begin{bmatrix} s & t \\ v & -u \end{bmatrix}\right)^{-1} = T_{i,j}\begin{bmatrix} u & t \\ v & -s \end{bmatrix}.$$

$$T_{i,j}\begin{bmatrix} s & t \\ v & -u \end{bmatrix}\begin{bmatrix} a_{1,1} & \cdots & \\ \vdots & \ddots & \\ a_{i,j} & & \\ \vdots & & \end{bmatrix} = \begin{bmatrix} d & \cdots & \\ \vdots & \ddots & \\ 0 & & \\ \vdots & & \end{bmatrix}.$$

Informally, we get the desired matrix with an expression of the form d in the $(1,1)$-entry in "one shot", compared to a process given by a sequence of steps of the form ① ⟶ ② ⟶ ① ⟶ ②, but we don't have an algorithm for finding s and t, in the case whereby the entries are not in a Euclidean domain.

With respect to the previous algorithm for matrices over Euclidean domains, we can basically replace "d" with "ℓ".

- When $a|b$, use the usual column and row operations.
- Then $a \nmid b$, use $\left(T_{i,j}\begin{bmatrix} s & t \\ v & -u \end{bmatrix}\right)$, as appropriate.

You can speed up your algorithm using operators of the form $T_{i,j}\begin{bmatrix} s & t \\ v & -u \end{bmatrix}$ whenever possible, even in the case of Euclidean domains.

In many cases, for rings which are not Euclidean domains, it may be very obvious as to how to find coefficients of the form s and t, e.g., through brute force algorithms.

However, what may be "obvious" to a human may be difficult to implement in terms of a program, e.g., through the use of brute-force algorithms.

Recall that in a PID, irreducible elements and prime elements are the same.

Theorem 6.2. *Let R be a PID, and let M be a finitely-generated R-module. Then*

(1) $M \cong R^\beta \oplus \bigoplus_{i=1}^{s} R/b_iR$ where $b_1|b_2|\cdots|b_s$, and b_i is not a unit for each index i.

(2) $M \cong R^\beta \oplus \bigoplus_{(i,j)=(1,1)}^{(s,r)} R/p_j^{\alpha_{i,j}}R$, where p_j is a prime for all indices j, and $\alpha_{1,j} \leqslant \alpha_{2,j} \leqslant \cdots \leqslant \alpha_{s,j}$.

This decomposition exists and is unique, up to units, and up to isomorphism.

With respect to the notation given in the above theorem, β denotes the Betti number.

The number β, as above, is unique. That is, the Betti number is well-defined and unique.