1/12/16

Welcome back!

Last semester in MTH 761 (Grad Algebra I) we discussed

- The category Set
- The category Grp
- The category Set^G, for $G \in \text{Grp}$.

This had to do with the algebra, combinatorics and geometry of symmetry (i.e. groups acting on things).

Recall that a group has only one algebraic operation, which we may refer to as $+$, $\times$, or $\circ$, depending on the situation.

This semester in MTH 762 (Grad Algebra II) we will add another layer of complexity by considering structures with at least *two* algebraic operations.

Let me motivate this by considering a category that we neglected last semester: the category of *abelian* groups.

The category Ab :

This semester we will always denote the algebraic operation in an abelian group $G \in Ab$ by "$+$" and the identity element by "0".

We have already seen some hints that the theory of abelian groups is very different from the theory of general groups. In particular, finite abelian groups are much less complicated than general finite groups [although we didn't prove this yet].

Here are two key differences between the categories Grp & Ab.

(1) Coproduct

Given $A, B \in Grp$ recall that the direct product $A \times B$ with operation

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2)$$

satisfies the universal property

$$\begin{tikzcd}
& & A \\
C \arrow[r, dashed, "\exists!", "\varphi_A \times \varphi_B"'] \arrow[urr, bend left, "\varphi_A"] \arrow[drr, bend right, "\varphi_B"'] & A \times B \arrow[ur, "\pi_A"] \arrow[dr, "\pi_B"'] & \\
& & B
\end{tikzcd}$$

That is, given a group $C \in Grp$ and group homomorphisms $\varphi_A : C \to A$ & $\varphi_B : C \to B$, there exists a unique group homomorphism, say $\varphi_A \times \varphi_B : C \to A \times B$, such that the above diagram commutes.

This means that direct product is the categorical product in Grp. Now suppose that $A, B \in Ab$. Since the above property holds for all $(C, \varphi_A, \varphi_B)$ in Grp, it certainly holds for all $(C, \varphi_A, \varphi_B)$ in the (full) subcategory $Ab \subseteq Grp$.

[Remark: "Full" in this case means that

$$\mathrm{Hom}_{Ab}(A, B) = \mathrm{Hom}_{Grp}(A, B)$$

for all $A, B \in Ab$.]

So we conclude that direct product is also the categorical product in Ab. However, we will use a different notation.

Definition: Given $A, B \in Ab$ we define the direct sum by

$$A \oplus B := \{(a,b) : a \in A, b \in B\}$$

with operation $(a_1, b_1) + (a_2, b_2) := (a_1 + a_2, b_1 + b_2)$.

Recall the following characterization of direct sums: Given $A \in Ab$ and subgroups $B_1, B_2 \subseteq A$ we have

$$A \approx B_1 \oplus B_2$$

if and only if $B_1 + B_2 = A$ & $B_1 \cap B_2 = 0$.

///

Now recall that the categorical coproduct in Grp is given by the "free product" $*$, which is big and complicated.

The situation is much nicer in Ab.

Theorem : The product and coproduct coincide in the category Ab.

Proof : Given $A, B \in Ab$ we must show that the direct sum $A \oplus B \in Ab$ satisfies the universal property of coproducts :

$$\begin{tikzcd}
A \arrow[dr, "i_A"] \arrow[drr, bend left, "\varphi_A"] & & \\
& A \oplus B \arrow[r, dashed, "\exists!", "f"'] & C \\
B \arrow[ur, "i_B"'] \arrow[urr, bend right, "\varphi_B"'] & &
\end{tikzcd}$$

Suppose $f : A \oplus B \to C$ is some homomorphism making the diagram commute. Then for all $a \in A$ & $b \in B$ it must satisfy

$$\begin{aligned}
f(a,b) &= f\left[(a,0_B) + (0_A, b)\right] \\
&= f(a,0_B) + f(0_A, b) \\
&= f(i_A(a)) + f(i_B(b)) \\
&= \varphi_A(a) + \varphi_B(b) .
\end{aligned}$$

///

$\wr$

The only question is whether this function $f(a,b) = \varphi_A(a) + \varphi_B(b)$ is actually a homomorphism. Here is where we need the commutativity of addition: for all (a_1, b_1) & $(a_2, b_2) \in A \oplus B$ we have

$$f(a_1 + a_2, b_1 + b_2) = \varphi_A(a_1 + a_2) + \varphi_B(b_1 + b_2)$$

$$= \varphi_A(a_1) + \varphi_A(a_2) + \varphi_B(b_1) + \varphi_B(b_2)$$

$$= \varphi_A(a_1) + \varphi_B(b_1) + \varphi_A(a_2) + \varphi_B(b_2)$$

$$= f(a_1, b_1) + f(a_2, b_2).$$

This completes the proof. ///

We have shown that (finite) products and coproducts coincide in Ab.

That's nice. ☺

② "Enriched" Structure.

Let $A, B \in Ab$ and consider two homomorphisms $\varphi_1, \varphi_2 : A \to B$

We have seen above that commutativity (in B) implies that the function

$$a \longmapsto \varphi_1(a) + \varphi_2(a)$$

is actually a group homomorphism $A \to B$. Let's give it a name.

Definition: Given abelian groups A, B and homomorphisms $\varphi_1, \varphi_2 \in \mathrm{Hom}_{Ab}(A, B)$ we will define the homomorphism

$$\varphi_1 + \varphi_2 \in \mathrm{Hom}_{Ab}(A, B)$$

by $(\varphi_1 + \varphi_2)(a) := \varphi_1(a) + \varphi_2(a)$.

So what? Well, this tells us that the "hom set" $\mathrm{Hom}_{Ab}(A, B)$ is actually more than a set; it's an abelian group.

[The identity element is the "zero morphism" $0 : A \to B$ from Grp.]

Jargon: If the hom sets in a (locally small) category $\mathcal{C}$ are objects in a category $\mathcal{D}$, we say that

"$\mathcal{C}$ is enriched over $\mathcal{D}$".

Thus we have shown that

"Ab is enriched over Ab". ///

There is a very interesting special case of this. Recall that for any object X in a (locally small) category $\mathcal{C}$, the set of endomorphisms

$$\mathrm{End}_{\mathcal{C}}(X) := \mathrm{Hom}_{\mathcal{C}}(X,X)$$

is a monoid (group without inverses) under composition of arrows. Thus, if A is an abelian group then the set

$$\mathrm{End}_{Ab}(A)$$

actually has two algebraic operations: addition & composition.

You might wonder how these two operations interact.

Theorem: For all $F_1, F_2, F_3 \in \mathrm{End}_{Ab}(A)$,

- $F_1 \circ (F_2 + F_3) = (F_1 \circ F_2) + (F_1 \circ F_3)$
- $(F_1 + F_2) \circ F_3 = (F_1 \circ F_3) + (F_2 \circ F_3)$.

Proof: The proofs are similar so we'll just show the first. For all $a \in A$ we have

$$\begin{aligned} [F_1 \circ (F_2 + F_3)](a) &= F_1\big((F_2 + F_3)(a)\big) \\ &= F_1(F_2(a) + F_3(a)) \\ &= F_1(F_2(a)) + F_1(F_3(a)) \\ &= (F_1 \circ F_2)(a) + (F_1 \circ F_3)(a) \\ &= [(F_1 \circ F_2) + (F_1 \circ F_3)](a). \end{aligned}$$

///

In other words, we conclude that $\mathrm{End}_{Ab}(A)$ is a RING.

Just as $\mathrm{Aut}_{\mathcal{E}}(X)$ is the prototypical example of a "group", $\mathrm{End}_{Ab}(A)$ is the prototypical example of a "ring".

We will think of $\mathrm{End}_{Ab}(A)$ as a "concrete ring" and we will define "abstract rings" by capturing the relevont abstract properties.

☆ Definition : A *ring* is a structure

$$(R, +, \circ, 0, 1)$$

where R is a set, $+$ & $\circ$ are functions $R \times R \longrightarrow R$, and $0, 1 \in R$ are special elements satisfying three axioms:

- $(R, +, 0)$ is an abelian group.
- $(R, \circ, 1)$ is a monoid.
- For all $a, b, c \in R$ we have
  - $a \circ (b + c) = (a \circ b) + (a \circ c)$
  - $(a + b) \circ c = (a \circ c) + (b \circ c)$.

///

Stay tuned for why I believe this is the correct way to think about rings.

1/14/16

Business:

There will be one midterm and a final exam, same as last semester. The homework situation will also be the same and I'll post HW1 next week.

Last time I tried to make the case that the "ring" concept emerges naturally from the "abelian group" concept. In particular, let $A \in Ab$ be an abelian group. Then the set of endomorphisms

$$\mathrm{End}_{Ab}(A),$$

which is always a monoid under composition, <u>also</u> has the structure of an abelian group.

Proof: Given $\varphi_1, \varphi_2 \in \mathrm{End}_{Ab}(A)$ and $a, b \in A$, the commutativity of A tells us that

↓

$$\begin{aligned}&\varphi_1(a+b)+\varphi_2(a+b)\\ &\quad=\left[\varphi_1(a)+\varphi_1(b)\right]+\left[\varphi_2(a)+\varphi_2(b)\right]\\ &\quad=\left[\varphi_1(a)+\varphi_2(a)\right]+\left[\varphi_1(b)+\varphi_2(b)\right].\end{aligned}$$

This says that the function $\varphi_1+\varphi_2 : A \to A$ defined by

$$(\varphi_1+\varphi_2)(a) := \varphi_1(a)+\varphi_2(a)$$

is also an endomorphism. ///

Moreover, we showed that the operation of $\circ$ distributes over $+$, so $\mathrm{End}_{Ab}(A)$ becomes a RING with compositional identity $id_A : A \to A$ and additive identity given by the zero morphism $0 : A \to A$.

Given an abelian group $A \in Ab$ I will call $\mathrm{End}_{Ab}(A)$ a "concrete ring". The definition of "abstract rings" is meant to model this.

☆ Definition: A ring is a structure

$$(R, +, \circ, 0, 1)$$

such that

- $(R, +, 0)$ is an abelian group.
- $(R, \circ, 1)$ is a monoid
- $\circ$ distributes over $+$ (from the left and the right).

///

You might wonder how your favorite ring fits into this picture.

Example: $\mathbb{Z}$.

First let's think of $(\mathbb{Z}, +, 0)$ as an abelian group. I claim that the "multiplication" operation $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ emerges naturally from the abelian group structure. To see this let's consider the ring of endomorphisms

$$R := \mathrm{End}_{Ab}(\mathbb{Z}).$$

I claim that we have a bijection $R \leftrightarrow \mathbb{Z}$. Indeed, since $\mathbb{Z} = \langle 1 \rangle$ is a cyclic group any group homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}$ is determined by the value

$$a := \varphi(1).$$

Then since φ is a homomorphism we have

- $\varphi(0) = 0$

- For all $n > 0$,

$$\varphi(n) = \varphi(\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}})$$

$$= \underbrace{\varphi(1) + \varphi(1) + \cdots + \varphi(1)}_{n \text{ times}}$$

$$= \varphi(1) \cdot n = an.$$

- For all $n < 0$,

$$\varphi(n) = -\varphi(-n) = -a(-n) = an$$

//

We conclude that φ is just the function

$$\lambda_a(n) := an \quad .$$

Then the map $\lambda : \mathbb{Z} \to R$ defined by $a \mapsto \lambda_a$ is a bijection.

So what? Well, it's actually more than a bijection. For all $a, b, n \in \mathbb{Z}$ we have

- $$\begin{aligned} \lambda_{a+b}(n) &= (a+b)n \\ &= an + bn \\ &= \lambda_a(n) + \lambda_b(n) \\ &= (\lambda_a + \lambda_b)(n) \,. \end{aligned}$$

- $$\begin{aligned} \lambda_{ab}(n) &= (ab)n \\ &= a(bn) \\ &= \lambda_a(\lambda_b(n)) \\ &= (\lambda_a \circ \lambda_b)(n) \,. \end{aligned}$$

Furthermore we have

$$\lambda_0 = 0_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Z}$$

$$\lambda_1 = id_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Z} \,.$$

///

In summary, we have shown that the function

$$\mathbb{Z} \longrightarrow \mathrm{End}_{Ab}(\mathbb{Z})$$

$$a \longmapsto (n \longmapsto an)$$

is an *isomorphism of rings*,

$$\mathbb{Z} \approx \mathrm{End}_{Ab}(\mathbb{Z}) .$$

This suggests that the additive structure of $\mathbb{Z}$ is primary and that the multiplicative structure emerges as composition of additive homomorphisms

So there is really no such thing as

"multiplication". ///

More generally, if R is *any* abstract ring, one can show that the function

$$\lambda : R \longrightarrow \mathrm{End}_{Ab}(R)$$

defined by $\lambda_a(b) := ab$ for all $a, b \in R$ is an injective ring homomorphism.

This establishes the fact that the concept of "abstract ring" is not more general than the concept of "concrete ring".

The importance of this idea will become clear soon when we discuss "modules". But first let's discuss abstract rings for their own sake [just as we discussed abstract groups before we discussed G-sets].

The category **Rng**:

Let R & S be abstract rings.

☆ Definition: We say that $\varphi : R \to S$ is a ring homomorphism if

↓

- φ is a homomorphism of abelian groups, i.e.,
  - $\forall a,b \in R$, $\varphi(a+b) = \varphi(a)+\varphi(b)$
- φ is a homomorphism of monoids; i.e.,
  - $\forall a,b \in R$, $\varphi(a \circ b) = \varphi(a) \circ \varphi(b)$
  - $\varphi(1_R) = 1_S$.

[Note that the condition $\varphi(a \circ b) = \varphi(a) \circ \varphi(b)$ does not imply $\varphi(1_R) = 1_S$, because of the lack of inverses in a monoid.]

One can check that the collection of rings & homomorphisms form a category, which we call Rng.

The basic properties of Rng are similar to Grp, so we'll go over them fairly quickly. The analogous concept to "normal subgroup" is the concept of "ideal".

☆ Definition: Given a ring homomorphism $\varphi : R \to S$ we define the *image*

$$\operatorname{im}\varphi := \{ s \in S : \exists\, r \in R,\ \varphi(r) = s \}$$

and the *kernel*

$$\ker\varphi := \{ r \in R : \varphi(r) = 0_S \}.$$

///

Note that setwise these are just the image & kernel of φ as a homomorphism of abelian groups. The question is: how do they interact with the monoid structure?

Claim: $\operatorname{im}\varphi \subseteq S$ is a sub*ring*.

Indeed, we already know that it's a sub*group* of $(S, +, 0_S)$. To see that it's a sub*ring* we note that

- $1_S = \varphi(1_R) \in \operatorname{im}\varphi$, by definition.
- For $s_1 = \varphi(r_1)$ & $s_2 = \varphi(r_2)$ in $\operatorname{im}\varphi$ we have
$$s_1 \circ s_2 = \varphi(r_1) \circ \varphi(r_2) = \varphi(r_1 \circ r_2) \in \operatorname{im}\varphi.$$

///

Furthermore, any subring $S' \subseteq S$ is the image of the natural inclusion homomorphism $i : S' \hookrightarrow S$. We can summarize this with the following slogan:

"image $\Longleftrightarrow$ subring".

The kernel is also a subgroup of R but it is not in general a subring because it probably doesn't contain 1_R.

Instead, the kernel satisfies the following defining(?) property:

$$\forall\, a, r \in R \text{ with } a \in \ker\varphi \text{ we have}$$

$$r \circ a \in \ker\varphi \quad \& \quad a \circ r \in \ker\varphi.$$

Proof: If $\varphi(a) = 0_S$ then we have

$$\varphi(r \circ a) = \varphi(r) \circ \varphi(a) = \varphi(r) \circ 0_S = 0_S$$
$$\varphi(a \circ r) = \varphi(a) \circ \varphi(r) = 0_S \circ \varphi(r) = 0_S.$$

The fact that $s \circ 0_S = 0_S \circ s = 0_S$ for all $s \in S$ is an easy consequence of the ring axioms. ///

[Remark : Suppose that $1_R \in \ker \varphi$. Then

- for all $r \in R$ we have $r = r \circ 1_R \in \ker \varphi$ and hence $\ker \varphi = R$.

- Since $1_S = \varphi(1_R) = 0_S$ we conclude that S is the zero ring $S = \{0_S\}$.

In fact, the zero ring $0 \in \text{Rng}$ is the final object in Rng. The unique maps $R \to 0$ are the only ring maps whose kernels are subrings.]

We will try to capture the notion of kernels with the following definition.

☆ Definition : Let R be an abstract ring and let $I \subseteq R$ be a subgroup of $(R, +, 0)$.

(i) We say I is a left ideal if

$$a \in I \;\&\; r \in R \Longrightarrow r \circ a \in I$$

(ii) We say I is a right ideal if

$$a \in I \;\&\; r \in R \Longrightarrow a \circ r \in I$$

iii We say that I is a two-sided ideal (or just an ideal) if it is both left and right.

///

Now we hope that the following slogan holds:

"kernel $\Longleftrightarrow$ ideal".

Does it?

1/19/16

I'll post HW1 later this week.

Pause: I should that the definition/motivation for rings I'm giving here is far from the original version.

The notion of a ring was introduced by Richard Dedekind in 1871 in order to generalize the properties of $\mathbb{Z}$ to so-called "integral extensions" $\mathbb{Z}[\alpha]$, $\alpha \in \mathbb{C}$. Dedekind used the term "Ordnung"; our term "ring" comes from David Hilbert's "Zahlring" (1897).

Now let $\omega_n := e^{2\pi i/n}$. In 1847 Gabriel Lamé observed that if the ring

$$\mathbb{Z}[\omega_n] := \{ \alpha_0 + \alpha_1 \omega_n^1 + \cdots + \alpha_{n-1}\omega_n^{n-1} : \alpha_i \in \mathbb{Z} \}$$

has the property of unique prime factorization (UF) for all $n \in \mathbb{Z}$ then Fermat's Last Theorem is true, i.e., if $x, y, z, n \in \mathbb{Z}$ with $n \geqslant 3$ and $xyz \neq 0$ then

$$x^n + y^n \neq z^n.$$

Very soon, though, Ernst Kummer showed that $\mathbb{Z}[\omega_n]$ usually does not have UF.

To recover UF, Dedekind & Kummer both developed a theory of "ideal numbers" [Dedekind shortened the term to "ideals"].

To be specific, here is Dedekind's main result

☆ Dedekind's Theorem (1871) :

Let $\mathbb{Q} \subseteq K$ be a finite degree field extension and define the corresponding "ring of integers" in K,

$$\mathcal{O}_K := \left\{ \alpha \in K : \alpha \text{ is the root of a monic polynomial in } \mathbb{Z}[x] \right\}$$

Picture :

$$\begin{tikzcd}
\mathcal{O}_K \arrow[r, hook] & K \\
\mathbb{Z} \arrow[u, hook] \arrow[r, hook] & \mathbb{Q} \arrow[u, hook]
\end{tikzcd}$$

↓

Then every ideal in $\mathcal{O}_K$ can be expressed uniquely as a "product of prime ideals" (whatever that means). ///

Example: Consider the field $\mathbb{Q} \subseteq K$, where

$$K = \mathbb{Q}(\sqrt{-5}) := \{ \alpha + \beta\sqrt{-5} : \alpha, \beta \in \mathbb{Q} \}.$$

In this case the ring of integers is

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}] = \{ \alpha + \beta\sqrt{-5} : \alpha, \beta \in \mathbb{Z} \}.$$

This ring does <u>not</u> have unique factorization of elements. Indeed, we have

$$2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$$

where $2, 3, (1+\sqrt{-5}), (1-\sqrt{-5})$ are all prime.

What's the problem? Well, recall that if $a, b \in \mathbb{Z}$ then we have

$$\begin{aligned} a\mathbb{Z} + b\mathbb{Z} &= \{ ax + by : x, y \in \mathbb{Z} \} \\ &= d\mathbb{Z}, \end{aligned}$$

where $d \in \mathbb{Z}$ is the greatest common divisor of a & b.

Unfortunately, there does not exist an element $d \in \mathbb{Z}[\sqrt{-5}]$ such that

$$\begin{aligned} & 2 \cdot \mathbb{Z}[\sqrt{-5}] + (1+\sqrt{-5}) \cdot \mathbb{Z}[\sqrt{-5}] \\ & \quad := \{ 2x + (1+\sqrt{-5})y : x, y \in \mathbb{Z}[\sqrt{-5}] \} \\ & \quad = d \cdot \mathbb{Z}[\sqrt{-5}]. \end{aligned}$$

Dedekind's solution is to regard the whole set as an "ideal number" Let's call it

$$A := (2, 1+\sqrt{-5}) := 2 \cdot \mathbb{Z}[\sqrt{-5}] + (1+\sqrt{-5}) \cdot \mathbb{Z}[\sqrt{-5}].$$

Similarly we will define the ideal numbers

$$\begin{aligned} A^* &:= (2, 1-\sqrt{-5}) \\ B &:= (3, 1+\sqrt{-5}) \\ B^* &:= (3, 1-\sqrt{-5}). \end{aligned}$$

One can check that as sets we have

↓

$$\begin{aligned} AA^* &= (2) := 2\cdot\mathbb{Z}[\sqrt{-5}]\,, \\ BB^* &= (3) \\ AB &= (1+\sqrt{-5}) \\ A^*B^* &= (1-\sqrt{-5})\,. \end{aligned}$$

One can also check that each of the ideals A, A^*, B, B^* is prime. Thus we have recovered "unique prime factorization":

$$\begin{aligned} (6) = (2)(3) &= (AA^*)(BB^*) \\ = (1+\sqrt{-5})(1-\sqrt{-5}) &= (AB)(A^*B^*)\,. \end{aligned}$$

///

In general, the ring of integers for $K := \mathbb{Q}(\sqrt{d})$ when $d \in \mathbb{Z}$ is

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d = 2 \text{ or } 3 \bmod 4 \\ \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right] & \text{if } d = 1 \bmod 4 \end{cases}$$

///

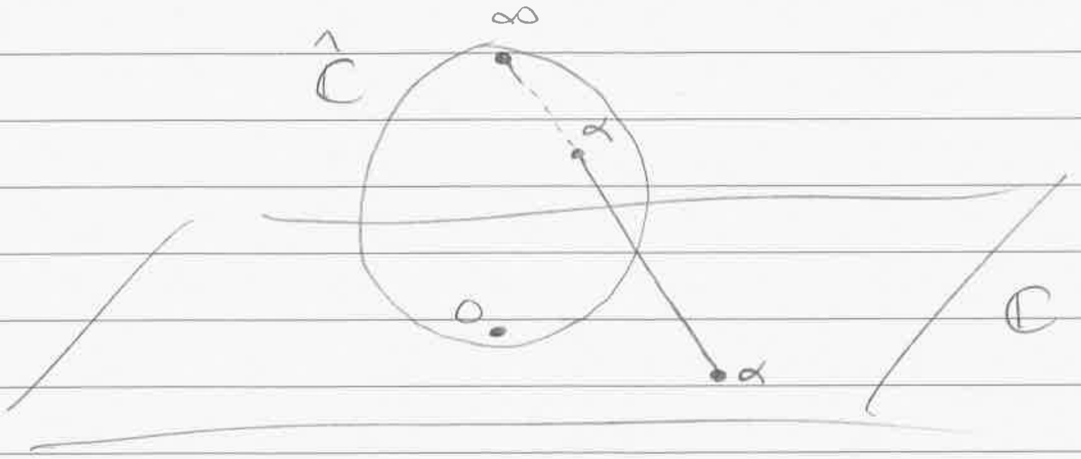
Dedekind's Theorem was the beginning of ring theory. Unfortunately, it didn't lead very quickly to a proof of Fermat's Last Theorem.

The story is not complete, however, without mentioning Dedekind's other amazing work (with Heinrich Weber) extending his technology of rings and fields to the theory of "Riemann surfaces".

Let me temporarily move to the category of "complex manifolds", without defining these. The arrows in this category are "holomorphic maps".

Let $\mathbb{C}$ be the "complex line" and let $\hat{\mathbb{C}}$ be its one point compactification, called the "Riemann sphere". The one new point in $\hat{\mathbb{C}}$ is called the "point at infinity".

Picture:



You may know the following facts from your complex analysis course:

- $\mathrm{Hom}(\mathbb{C}, \mathbb{C})$ = holomorphic functions
- $\mathrm{Hom}(\mathbb{C}, \hat{\mathbb{C}})$ = meromorphic functions
- $\mathrm{Hom}(\hat{\mathbb{C}}, \mathbb{C})$ = constant functions ("Liouville's Theorem")
- $\mathrm{Hom}(\hat{\mathbb{C}}, \hat{\mathbb{C}})$ = rational functions

Clearly the last set of functions is the nicest to work with. Let's denote this ring of functions (in fact, a field) by

$$\mathrm{End}(\hat{\mathbb{C}}) = \mathbb{C}(z) = \left\{ \frac{f(z)}{g(z)} : \begin{array}{l} f(z), g(z) \in \mathbb{C}[z] \\ g(z) \neq 0 \end{array} \right\}$$

The subring of "polynomials"

$$\mathbb{C}[z] \subseteq \mathbb{C}(z)$$

are the rational functions that have no poles except at ∞.

$\downarrow$

Now, consider any polynomial in two complex variables $f(x,y) \in \mathbb{C}[x,y]$. We say that the equation

$$f(x,y) = 0$$

implicitly defines y as an "algebraic function" of x. But we know that this is not really a function.

Example: Let $f(x,y) = y^2 - x$. Then the solution to $f(x,y) = 0$ is

$$y = \text{"}\sqrt{x}\text{"},$$

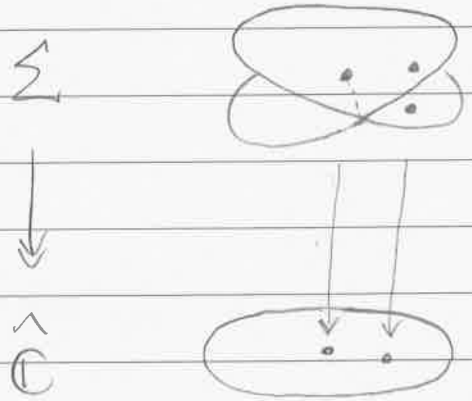
which is not a real (i.e., "single-valued") function of x. ///

Riemann's great insight in the 1850's was that the equation $f(x,y) = 0$ does define y as a single-valued function by "analytic continuation" to some new domain, called a "Riemann surface".

Topologically, a Riemann surface Σ is a finite branched covering of the Riemann sphere $\hat{\mathbb{C}}$.

Example: The Riemann surface of $f(x,y) = y^2 - x$ is generally a 2:1 covering space but it is 1:1 (branched) over the points $x = 0$ and $x = \infty$. [The numbers 0 & ∞ each have a <u>unique</u> square root but every other number has <u>two</u>.]

Near each branch the covering looks like:



Note that the self-intersection is not really there; it's an artifact of embedding the picture in $\mathbb{R}^3$.

The great insight of Dedekind and Weber (1888) was to realize that the field of meromorphic functions $K := \mathrm{Hom}(\Sigma, \hat{\mathbb{C}})$ is a finite degree extension of the field $\mathbb{C}(z) = \mathrm{Hom}(\hat{\mathbb{C}}, \hat{\mathbb{C}})$.

Picture:

$$\begin{tikzcd}
\mathcal{O}_K \arrow[r, hook] & K & \Sigma \arrow[d, two heads] \\
\mathbb{C}[z] \arrow[u, hook] \arrow[r, hook] & \mathbb{C}(z) \arrow[u, hook] & \hat{\mathbb{C}}
\end{tikzcd}$$

Now Dedekind realized that his technology of rings & ideals allowed him to provide the first rigorous proofs for some of Riemann's theorems (which Riemann had established by appeal to physical intuition from electrostatics).

It's okay if you didn't understand any of that. The point I wanted to make is that ring theory was born from a synthesis of number theory & complex analysis. From this point of view the two most important commutative rings are

$$\mathbb{Z} \quad \& \quad \mathbb{C}[z].$$

The notions of abstract rings & ideals were brought to maturity by Emmy Noether in the 1920s.

However, I always felt that the ring concept is fairly mysterious, as evidenced by the fact that there are still competing definitions of the word "ring" (i.e., with or without "1").

There is also the problem of how non-commutative rings such as $\mathrm{Mat}_n(K)$ should fit into the subject. In my opinion the more recent categorical point of view significantly clarifies the situation:

- The definition of "ring" models the endomorphisms of an abelian group.

- Any ring R (whether commutative or not) should be studied through its category of modules.

=

On Thursday I'll return to the careful, systematic (and ahistorical) development of ring theory.

1/21/16

HW1 will be posted today.

Last time I discussed the origin of ring theory from Dedekind's work on unique factorization and Riemann surfaces; today, back to the dry stuff.

Recall: A ring $(R, +, \circ, 0, 1)$ is

- an abelian group $(R, +, 0)$
- a monoid $(R, \circ, 1)$
- distributive laws

$$a \circ (b + c) = (a \circ b) + (a \circ c)$$
$$(a+b) \circ c = (a \circ c) + (b \circ c)$$

///

A ring homomorphism $\varphi : R \to S$ satisfies

- $\varphi(a+b) = \varphi(a) + \varphi(b)$
- $\varphi(a \circ b) = \varphi(a) \circ \varphi(b)$
- $\varphi(1_R) = 1_S$.

We define $\ker \varphi$ & $\operatorname{im} \varphi$ as the kernel & image of φ as a homomorphism of abelian groups.

///

Then we may study how $\ker\varphi$ & $\operatorname{im}\varphi$ interact with the monoid structure. We defined the notion of sub*ring* so that

$$\text{“ image} \iff \text{subring ”}$$

but then we found that $\ker\varphi \subseteq R$ is never a subring unless $S = 0$ (the “zero ring”) & $\varphi = 0$ (the “zero morphism”).

To try to capture the “internal” properties of kernels we made the following definition.

☆ Definition: Let R be a ring and let $I \subseteq R$ be an abelian subgroup. We say that I is a (two-sided) *ideal* if for all $a, b \in R$ we have

$$a \in I \text{ or } b \in I \implies a \circ b \in I$$

[Remark: If the converse also holds then we say that I is a *prime ideal*, but this notion is usually only applied in commutative rings.]

Claim: This definition works, i.e., we have

"kernel $\Longleftrightarrow$ ideal".

Proof: We already proved $\Longrightarrow$.

So let $I \subseteq R$ be an ideal. We want to construct a ring R' and a ring homomorphism $\varphi : R \to R'$ such that $\ker \varphi = I$.

We don't need to reinvent the wheel. Since $I \subseteq R$ is a subgroup of an abelian group (hence normal) we obtain a quotient group homomorphism

$$\pi : R \to R/I$$

with $\ker \pi = I$. The problem now is to define a monoid structure on R/I so that π becomes a ring homomorphism. And we have no choice: if such a structure exists then it must satisfy

$$\pi(a) \circ \pi(b) = \pi(a \circ b)$$

$$(a+I) \circ (b+I) = (a \circ b) + I.$$

Such an operation will naturally inherit the monoid and distributive properties from R. The only thing left to check is that the proposed operation is <u>well-defined</u>.

To check this, suppose that $a+I = a'+I$ (i.e., $a-a' \in I$) and $b+I = b'+I$ (i.e., $b-b' \in I$). We want to show that

$$(a \circ b) + I = (a' \circ b') + I .$$

And, indeed, we have

$$\begin{aligned}(a\circ b)-(a'\circ b') &= (a\circ b)-(a\circ b') + (a\circ b')-(a'\circ b') \\ &= a\circ(b-b') + (a-a')\circ b .\end{aligned}$$

Since I is an ideal with $a-a' \in I$ and $b-b' \in I$, this last expression is in I, as desired.

///

We can summarize this construction with the following universal property.

↓

☆ Universal Property of Ring Quotients :

Let $\varphi : R \to S$ be a ring homomorphism and let $I \subseteq R$ be an ideal such that $I \subseteq \ker\varphi$. Then there exists a unique ring homomorphism $\overline{\varphi} : R/I \to S$ such that

$$\begin{tikzcd} & R \arrow[dl, "\pi"'] \arrow[dr, "\varphi"] & \\ R/I \arrow[rr, dashed, "\exists!\,\overline{\varphi}"'] & & S \end{tikzcd}$$
.

///

And this immediately gives us a "First Isomorphism Theorem" for rings. Let's remind ourselves how it goes.

☆ First Isomorphism Theorem for Rings :

Let $\varphi : R \to S$ be any ring homomorphism. Then the induced map $\overline{\varphi} : R/\ker\varphi \to S$ restricts to a ring iso<u>morph</u>ism

$$\overline{\varphi} : R/\ker\varphi \xrightarrow{\sim} \operatorname{im}\varphi .$$

$$a + \ker\varphi \longmapsto \varphi(a)$$

///

Proof: What needs to be checked?

The map is clearly surjective so we only need to check injectivity. Indeed, we have

$$\begin{aligned} \varphi(a) = \varphi(b) &\Longrightarrow \varphi(a) - \varphi(b) = 0 \\ &\Longrightarrow \varphi(a-b) = 0 \\ &\Longrightarrow a - b \in \ker\varphi \\ &\Longrightarrow a + \ker\varphi = b + \ker\varphi \end{aligned}$$

Alternatively, we can show that the map $\varphi : R \twoheadrightarrow \operatorname{im}\varphi$ satisfies the same universal property as the quotient $\pi : R \twoheadrightarrow R/\ker\varphi$. Indeed, given any ring hom $\mu : R \to S$ such that $\ker\varphi \subseteq \ker\mu$ we will show that $\exists!\ \bar{\mu} : \operatorname{im}\varphi \to S$ such that

$$\begin{tikzcd} & R \arrow[dl, "\varphi"'] \arrow[dr, "\mu"] & \\ \operatorname{im}\varphi \arrow[rr, "\bar{\mu}"'] & & S \end{tikzcd}$$

By commutativity, the map $\bar{\mu}$ must satisfy

$$\bar{\mu}(\varphi(a)) = \mu(a),$$

and such a map *does* exist because

$$\begin{aligned}\varphi(a)=\varphi(b) &\Longrightarrow \varphi(a)-\varphi(b)=0\\ &\Longrightarrow \varphi(a-b)=0\\ &\Longrightarrow a-b\in\ker\varphi\\ &\Longrightarrow a-b\in\ker\mu\\ &\Longrightarrow \mu(a-b)=0\\ &\Longrightarrow \mu(a)-\mu(b)=0\\ &\Longrightarrow \mu(a)=\mu(b).\end{aligned}$$

□

Are there also ring analogues of the 2nd & 3rd Isomorphism Theorems.

Well, now we have a problem. When G is a group we let $\mathcal{L}(G)$ be the lattice of subgroups and we think of normal subgroups as ("modular") elements of this lattice.

Now let R be a ring. If we let $\mathcal{L}(R)$ be the the lattice of subrings then the ideals of R will be *invisible*, and we don't want that! So the situation is necessarily more complicated.

☆ 3rd Isomorphism Theorem:

Let R be a ring with ideal I.

- If $S \leq R$ is a subring containing I then S/I is a subring of R/I and this establishes a bijection

$$\{\text{subrings of } R \text{ containing } I\} \longleftrightarrow \{\text{subrings of } R/I\}.$$

- If $J \leq R$ is an ideal containing I then J/I (defined as an abelian group) is an ideal of R/I and this establishes a bijection

$$\{\text{ideals of } R \text{ containing } I\} \longleftrightarrow \{\text{ideals of } R/I\}.$$

Furthermore, for each such J we have an isomorphism of rings

$$\frac{R/I}{J/I} \approx \frac{R}{J}.$$

Proof: "Exercise" ☺

///

☆ 2nd Isomorphism Theorem :

Let R be a ring with ideal $I \subseteq R$.

- If $S \subseteq R$ is a subring then

  - $I + S := \{a+b : a \in I, b \in S\}$ is a subring of R.

  - $I \cap S$ is an ideal of R.

  - We have an isomorphism of rings

$$\frac{I+S}{I} \approx \frac{S}{I \cap S}.$$

- If $J \subseteq R$ is an ideal then

  - $I + J := \{a+b : a \in I, b \in J\}$ is an ideal of R.

  - $I \cap J$ is an ideal of R.

Proof : "Exercise" ☺ //

So we seem to have two 2nd and two 3rd "Isomorphism Theorems for Rings", and in each case only one of them involves an actual isomorphism of rings.

Let's examine the missing isomorphisms:

- Given an ideal $I \subseteq R$ and a subring $S \subseteq R$ containg I we have a perfectly good isomorphism of abelian groups

$$\frac{R/I}{S/I} \approx \frac{R}{S},$$

but (as we know) the objects on the left and right are not rings in any reasonable way.

- Given any two ideals $I, J \subseteq R$ we have an isomorphism of abelian groups

$$\frac{I+J}{I} \approx \frac{J}{I \cap J},$$

but, again, neither of these groups has a natural ring structure. ///

Question: Do the group isomorphisms

$$\frac{R/I}{S/I} \approx \frac{R}{S} \quad \& \quad \frac{I+J}{I} \approx \frac{J}{I \cap J}$$

carry some extra structure related to the ring structure of R?

The answer is yes, and we will discuss this next time.

1/26/16

Fixed a couple small issues in Problems 1 & 2 of HW 1.

Last time we discussed the 1st, 2nd & 3rd Isomorphism Theorems for Rings.

☆ 1st : Let $\varphi : R \to R'$ be any ring homomorphism. Then we obtain a canonical factorization of φ :

$$\begin{tikzcd}
R \arrow[r, two heads, "\pi"'] \arrow[rrr, bend left, "\varphi"] & R/\ker\varphi \arrow[r, "\sim", "\bar{\varphi}"'] & \operatorname{im}\varphi \arrow[r, hook, "\iota"'] & R'
\end{tikzcd}$$

In particular, we have an isomorphism of rings

$$R/\ker\varphi \approx \operatorname{im}\varphi .$$

☆ 2nd : Let R be a ring with ideal $I \subseteq R$ and subring $S \subseteq R$. Then we have an isomorphism of rings

$$\frac{I+S}{I} \approx \frac{S}{I \cap S} .$$

☆ 3rd: Let R be a ring with ideals $I, J \leq R$ such that $I \leq J$. Then we have an isomorphism of rings

$$\frac{R/I}{J/I} \approx \frac{R}{J}.$$

///

Of course, if $I, J \leq R$ are any ideals and $S \leq R$ is any subring containing I then we also have the following isomorphisms of abelion groups

$$\frac{I+J}{I} \approx \frac{J}{I \cap J} \quad \& \quad \frac{R/I}{S/I} \approx \frac{R}{S}$$

Unfortunately, these groups do not have any natural ring structure.

☆ Q: Do they have any kind of structure related to the monoid structure of R?

A: Yes.

///

Recall that for any group G we defined a *G-set* as a functor

$$F : G \longrightarrow \mathrm{Set}$$

from G (thought of as a category with one object) into the category of sets. We found that G-sets form a category with morphisms given by natural transformations.

Now observe that this construction *still works* if we replace the group G by a monoid R. [After all, a monoid is *nothing but* a category with one object.] Thus we define an *R-set* as a functor

$$F : R \longrightarrow \mathrm{Set}.$$

As before, this is equivalent to choosing a set X and a monoid homomorphism

$$\varphi : R \longrightarrow \mathrm{End}_{\mathrm{Set}}(X).$$

We can also write this concretely by using the notation

$$r(x) := \varphi_r(x) \quad \forall r \in R,\ x \in X$$

Then we have the following properties

- $1_R(x) = x \quad \forall x \in X$

- $r(s(x)) = (rs)(x) \quad \forall r,s \in R,\ x \in X$,

which we could also take as axioms for the concept of a (left) monoid action $R \circlearrowright X$.

///

The point is this:

Consider a ring $(R, +, \circ, 0_R, 1_R)$. Then

- Any ideal $I \subseteq R$ carries a natural (left or right) action of the monoid $(R, \circ, 1_R)$.

- Any subring $S \subseteq R$ carries a natural (left or right) action of the monoid $(S, \circ, 1_R)$.

Thus we might want to interpret

$$\frac{I+J}{I} \approx \frac{J}{I \cap J} \quad \& \quad \frac{R/I}{S/I} \approx \frac{R}{S}$$

as isomorphisms of R-sets & S-sets, respectively. There is only one problem.

☆ Problem: Is it possible to form a quotient of monoid-sets?

Answer: No, not in general.

However, in our case we don't just have monoid-sets; we have monoid-sets and abelian groups coexisting peacefully.

Hopefully I have motivated the following definition. [If not, then I hope to motivate it by the end of the semester.]

☆ Definition: Let R be a ring. Then a (left) R-module consists of

- An abelian group $(M, +, 0_M)$

- A (left) monoid action $R \circlearrowright M$.

- A requirement that the action "respects addition" in both R and M.

↓

That is, for all $r, s \in R$ and $m, n \in M$ we require that

— $r(m+n) = r(m) + r(n)$
— $(r+s)(m) = r(m) + s(m)$.

[Note that we abuse notation by using "+" for the abelian group operation in both R and M. This is traditional; we will try not to get confused.]

///

Is it possible to say this definition with fewer words? Certainly. Recall that we already have a natural ring structure on the endomorphisms $\text{End}_{Ab}(M)$.

☆ Shorter Definition: Let R be a ring. Then a left R-module consists of an abelian group M and a homomorphism of rings

$$\varphi : R \longrightarrow \text{End}_{Ab}(M).$$

The homomorphism φ encodes the left monoid action $R \circlearrowright M$ and the fact that it preserves addition. [Sometimes we say that the action is "linear".]

OK, but is it possible to make the definition <u>even shorter</u>?

Yes, but it will involve me using the term "abelian category" without defining it. [Basically, an abelian category has hom sets that are abelian groups and well-behaved products, coproducts, kernels, cokernels, etc. It is meant to abstract the properties of Ab (hence the name). Abelian categories are becoming a standard notion in both commutative and noncommutative algebra, so you should be aware of their existence.]

The main point for us is that an abelian category with one object is just a <u>ring</u>.

☆ Shortest Definition : Let R be a ring, thought of as an abelion category with one object. Then a left R-module is just a functor of abelion categories

$$F : R \longrightarrow Ab .$$

Oh God, what have we done ?

The concept of modules is hard to motivate but we will see in time that it solves many problems.

At the moment, it solves the problem of the isomorphisms

$$\frac{I+J}{I} \simeq \frac{J}{I \cap J} \quad \& \quad \frac{R/I}{S/I} \simeq \frac{R}{S} .$$

That is : The left is an isomorphism of R-modules and the right is an isomorphism of S-modules, each in a natural way.

To show this we need only observe that a quotient of R-modules is again an R-module.

Given a left R-module M and a submodule $N \subseteq M$ [i.e. N is simultoneously a subgroup and a sub-R-set], consider the abelian group M/N. One can check that the prescription

$$r(m+N) = r(m) + N \quad \forall\, r \in R,\ m \in M$$

defines a left R-module structure on M/N and that this structure satisfies the following universal property.

☆ Universal Property of R-module Quotients:

Let R be a ring and let $N \subseteq M$ be a left R-submodule. Then for any R-module homomorphism $\varphi : M \longrightarrow P$ satisfying $N \subseteq \ker \varphi$, there exists a unique R-module homomorphism $\overline{\varphi} : M/N \longrightarrow P$ such that

$$\begin{tikzcd} & M \arrow[dl, "\pi"'] \arrow[dr, "\varphi"] & \\ M/N \arrow[rr, "\exists ! \overline{\varphi}"'] & & P \end{tikzcd}$$

Proof : Everything already works in the category of abelian groups. Just check that the extra R-action doesn't spoil things.

///

As is usually the case with abstract algebra, the proof is an afterthought. The real work is in finding the *correct* *definition*.

1/28/16

HW1 due next Thurs Feb 4.
(Small errors corrected, so please check the latest version.)

Last time I gave the definition of an "R-module". This is a unifying algebraic concept that is above the groups-rings-fields level of generality.

Consequently, it is a difficult concept to motivate. Last time I motivated it through the search for "2nd" & "3rd" Isomorphism Theorems for Rings.

I'll try to motivate it a bit more before proceeding with the basic theory.

Recall that we had two definitions for the "group" concept.

G1. A collection of symmetries of an object.

G2. A "set with structure" satisfying certain axioms.

The axioms of G2 are intended to model the properties of G1. We then check that our abstract definition is not "too general" as follows.

"Cayley's Theorem": Given an abstract group G we have an injective group homomorphism

$$\varphi : G \hookrightarrow \mathrm{Aut}_{\mathrm{Grp}}(G)$$

defined by $\varphi_g(h) := g \circ h$.

Thus we can realize G as a concrete group of symmetries of some "thing"; namely, itself.

The study of all homomorphisms

$$\varphi : G \longrightarrow \mathrm{Aut}_{\mathcal{C}}(X)$$

is called the representation theory of G. For any category $\mathcal{C}$ we have a category

$$\mathcal{C}^G$$

of "representations of G in $\mathcal{C}$".

///

Similarly, we have two definitions for "ring":

R1. A collection of endomorphisms of an abelian group.

R2. A "set with structure" satisfying certain axioms intended to model R1.

To check that R2 is not "too general" we have another "Cayley-Type Theorem":

Given an abstract ring R, we have an injective ring homomorphism

$$\lambda : R \hookrightarrow \mathrm{End}_{Ab}(R)$$

defined by $\lambda_a(b) := a \circ b$.

Thus we can realize R as a concrete ring of endomorphisms of some abelian group; namely, itself.

The study of all homomorphisms

$$\varphi : R \longrightarrow \mathrm{End}_{Ab}(M)$$

is called the <u>module</u> theory of R. ///

Just as we had a category of <u>G-sets</u> consisting of functors

$$G \longrightarrow \text{Set},$$

we have a category of left R-modules consisting of "additive functors"

$$R \longrightarrow Ab.$$

[The presence of abelian groups on the ground floor of this theory leads to the perspective of "abelian categories", which is different from "sets with structure".]

The two perspectives are often combined by turning the group G into the group <u>ring</u> R[G] and looking at the category of

$$R[G]\text{-modules}.$$

We will do this later. ///

That was pretty pure. Is there a more applied motivation for modules?

Yes. Again this comes from an analogy between number theory and physics.

Remark: $\mathbb{Z}$-modules = Abelian groups.

Indeed, if R is any ring then there exists a unique ring homomorphism

$$\varphi : \mathbb{Z} \longrightarrow R$$

defined by $\varphi(1_{\mathbb{Z}}) = 1_R$. [That is, $\mathbb{Z}$ is the initial object in the category Rng.]

Thus if M is an abelian group then there is a unique $\mathbb{Z}$-module structure

$$\varphi : \mathbb{Z} \longrightarrow \mathrm{End}_{Ab}(M) ;$$

namely, the obvious one given by "repeated addition" in M. This gives us an isomorphism of categories

$$\mathbb{Z}\text{-Mod} = Ab .$$

[stronger than just an equivalence].

Dedekind invented the concept of "module" [his notation] at the same time he invented rings ["Ordnungen"]: in his 1871 paper on unique factorization.

To discuss the physics angle, let X be a real manifold. An n-dimensional *vector field* is a (probably smooth) function

$$\varphi : X \longrightarrow \mathbb{R}^n .$$

Vector fields form an *abelian group* called, say, $\mathrm{Vec}_n(X)$ under pointwise addition:

$$(\varphi_1 + \varphi_2)(x) := \varphi_1(x) + \varphi_2(x) .$$

They do *not* form a ring, but they do have an important additional structure coming from scalar multiplication in $\mathbb{R}^n$.

Let $\mathbb{R}[X]$ be the ring of (probably smooth) functions $X \longrightarrow \mathbb{R}$. We can think of $f \in \mathbb{R}[X]$ as a "scalar" that varies from point to point.

↓

Finally, we are allowed to "scale" vector fields. Given a field $\varphi : X \to \mathbb{R}^n$ and a "scalar" $f : X \to \mathbb{R}$ we define the new vector field $f\varphi : X \to \mathbb{R}^n$ by

$$(f\varphi)(x) := f(x)\varphi(x).$$

Thus $\mathrm{Vec}_n(X)$ is a module over $\mathbb{R}[X]$.

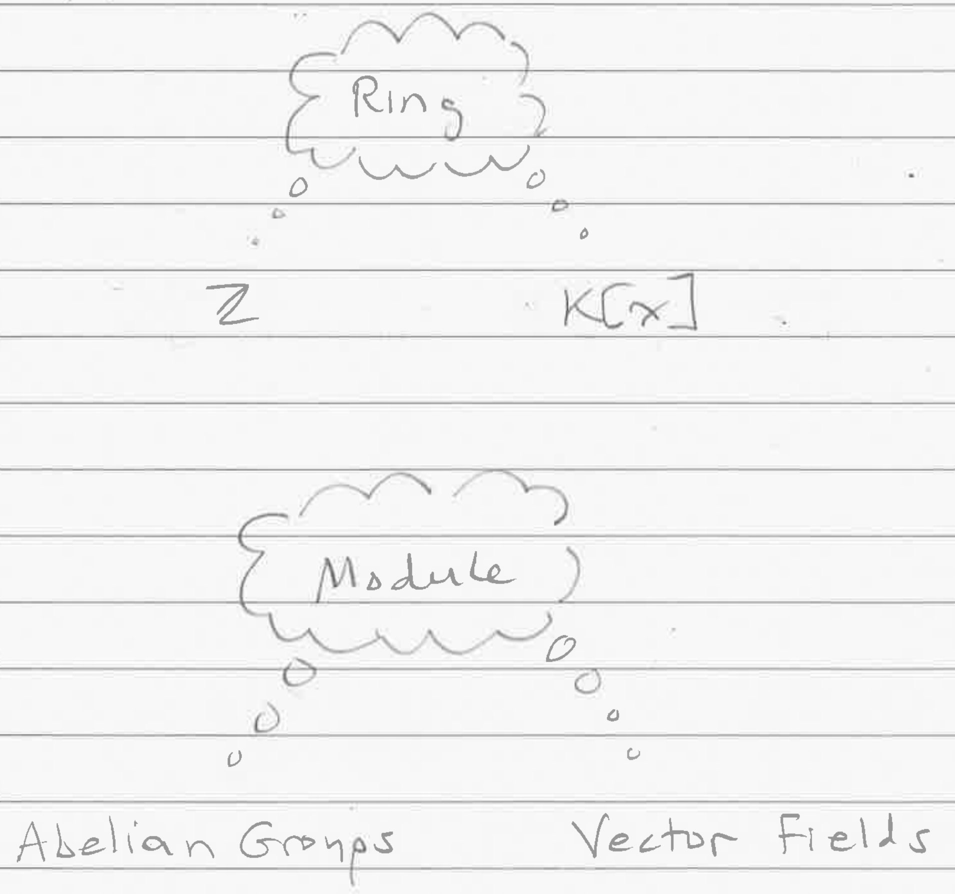
So if you are physically inclined, you can think of the "module" concept as a generalization of "vector field".

[Remark: A "vector field" is a "global section of a vector bundle". But some interesting vector bundles may not have any global sections (e.g. the Möbius band). In this case "modules" must be replaced by "sheaves of modules".

We will not pursue sheaves in this class but you should be aware of their existence.]

In summary, the "module" concept is a simultaneous generalization of "abelian group" and "vector field", just as the "ring" concept is a generalization of "integers" and "polynomials over a field".

Picture:



///

Maybe that's enough motivation for today?

Having decided that the definition of module is correct and interesting we will proceed to develop the basic theory.

☆ Definition: Let R be a ring. The collection of left R-modules forms a category which we call R-$\underline{\text{Mod}}$.

The morphisms in the category are sometimes called "R-linear maps". We can guess the definition pretty easily. If left R-modules are "additive functors"

$$R \to Ab$$

then morphisms should be "additive natural transformations".

To be concrete, let M & N be abelian groups with linear R-actions defined by

$$\alpha : R \to End(M) \quad \& \quad \beta : R \to End(N)$$

Then a group homomorphism $\varphi : M \to N$ is called R-linear if for all $r \in R$ the following diagram commutes:

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\alpha_r"'] & N \arrow[d, "\beta_r"] \\ M \arrow[r, "\varphi"] & N \end{tikzcd}$$

In symbols, we have

$$\varphi(\alpha_r(m)) = \beta_r(\varphi(m)) \quad \forall\, m \in M,\ r \in R.$$

And if you're willing to leave the R-actions implicit we can just write

$$\varphi(r(m)) = r(\varphi(m)) \quad \forall\, m \in M,\ r \in R.$$

or even

$$\boxed{\varphi r = r \varphi \quad \forall\, r \in R}$$

///

2/2/16

HW1 due Thursday.

Today: The category R-Mod.

Let R be a ring. Recall that a left R-module is an additive functor $R \to Ab$. These naturally form a category with morphisms given by natural transformations.

Concretely: A left R-module consists of an abelian group M and a ring hom $\alpha: R \to End_{Ab}(M)$. If $\beta: R \to End_{Ab}(N)$ is another module then a function $\varphi: M \to N$ is called an R-module hom (or an R-linear map) if $\forall r \in R, m, n \in M$,

$$\varphi(m + \alpha_r(n)) = \varphi(m) + \beta_r(\varphi(n)).$$

Examples:

- We saw last time that $\mathbb{Z}$-modules are just abelian groups:

$$\mathbb{Z}\text{-Mod} = Ab.$$

- If K is a field then a K-module is just a vector space over K. We will write

$$K\text{-Vec} := K\text{-Mod}$$

for the category of K-vector spaces and K-linear maps.

- More generally, one can use "sheaves of modules" to construct "vector bundles" on a manifold.

If M is an R-module (we will assume "left" unless otherwise stated) then we say that $N \subseteq M$ is an R-submodule if

$$r \in R,\ m, n \in N \implies m + rn \in N$$

(i.e., N is closed under addition and scalar multiplication).

Examples:

- subspaces of a vector space.

- Any ring R is a module over itself by left multiplication. The submodules are precisely the left ideals. ///

If $\varphi : M \to N$ is a morphism of R-modules then one can check that $\ker\varphi \subseteq M$ and $\mathrm{im}\,\varphi \subseteq N$ are both R-submodules.

Furthermore, given any submodule $P \subseteq M$ we saw that there is a natural R-module structure on the quotient:

$$r(m+P) := r(m) + P.$$

Thus in the category R-Mod the following slogan holds:

"kernel $\Longleftrightarrow$ submodule $\Longleftrightarrow$ image"

Note that this is an improvement over the categories Grp & Rng.

Given a module $M \in R$-Mod, this inspires us to consider the lattice $\mathcal{L}_R(M)$ of R-submodules.

Note that this is indeed a lattice with top element M and bottom element 0 (the "zero module"). For all $A, B \in \mathcal{L}_R(M)$ the meet and join are given by

$$A \wedge B = A \cap B \quad \& \quad A \vee B = A + B,$$

with the obvious R-module structures.

The lattice $\mathcal{L}_R(M)$ is the correct setting to think about 1st, 2nd & 3rd Isomorphism Theorems and everything works out as nicely as possible.

1st: For all $\varphi : A \to B$ we have a module isomomorphism

$$A/\ker\varphi \approx \operatorname{im}\varphi$$

and lattice isomorphisms

$$\mathcal{L}_R(A, \ker\varphi) \approx \mathcal{L}_R(\operatorname{im}\varphi) \approx \mathcal{L}_R(A/\ker\varphi).$$

where the left isomorphism comes from a Galois connection.

2nd : For all $A, B \in \mathcal{L}_R(M)$ we have

$$\frac{A+B}{A} \approx \frac{B}{A \cap B}.$$

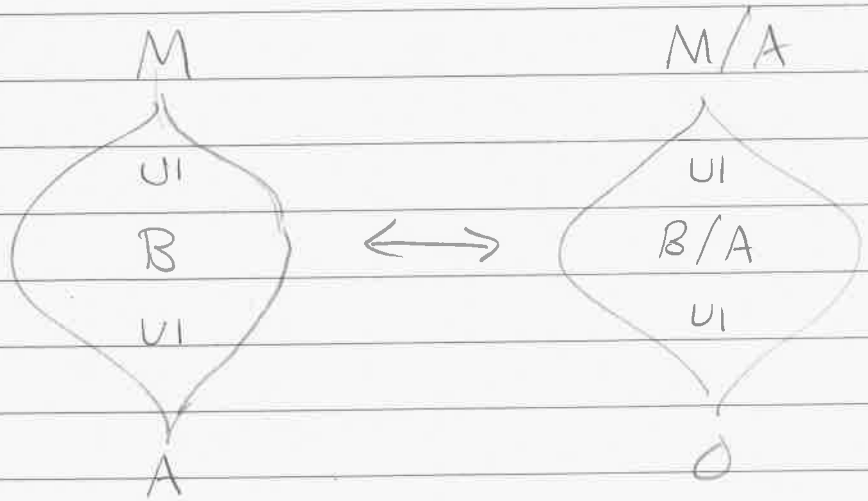
This says in particular that $\mathcal{L}_R(M)$ is a modular lattice [a concept invented by Dedekind in 1900 under the name "dual group of module type"].

3rd : For all $A, B \in \mathcal{L}_R(M)$ with $A \subseteq B$ we have a module isomorphism

$$\frac{M/A}{B/A} \approx \frac{M}{B}$$

and an isomorphism of lattices.

$$\mathcal{L}(M, A) \approx \mathcal{L}(M/A).$$



///

Now that lattice theory is working again, maybe we can get the Jordan-Hölder Theorem working?

Definition: We say $M \in R\text{-Mod}$ is a simple module if it has no submodules apart from 0 & M.

A composition series for $M \in R\text{-Mod}$ is a chain of submodules

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_\ell = 0$$

in which each quotient M_i / M_{i+1} is simple (equivalently, each M_{i+1} is a maximal proper submodule of M_i). We call ℓ the length of the series.

☆ Jordan-Hölder Theorem:

Let $M \in R\text{-Mod}$. If M has a composition series then any two composition series are equivalent. In particular they have the same length ℓ which we call the length of the module M.

Proof: The proof for groups using the Zassenhaus (Butterfly) Lemma and the Schreier Refinement Lemma goes through with only trivial modification. ///

Remarks:

- You already know an example of this Theorem. Consider a vector space $V \in K\text{-Vec}$ of finite length. In this case the length is equal to the usual dimension of V (size of a maximal independent set).

  Thus we can view "length" as some analogue of "dimension" for more general modules.

- You might wonder if there is some "Master" Jordan-Hölder Theorem containing Grp & R-Mod as special cases.

  Yes there is. If M is a monoid then we define an M-group as a functor

$$M \to Grp.$$

This is also called a "group with operators". The category Grp^M has a Jordan-Hölder Theorem simultaneously generalizing the two cases we know.

"Groups with operators" were introduced by Emmy Noether in the 1920s but they have fallen out of style. I don't know why. ///

Example: The length of an abelian group.

One can check that an abelian group $A \in \mathbb{Z}$-Mod is simple if and only if $A \approx \mathbb{Z}/p\mathbb{Z}$ for some prime. Therefore, an abelian group has finite length if and only if it is finite. What is the length?

Consider $A = \mathbb{Z}/n\mathbb{Z}$. By the 3rd Iso. Thm. we have an isomorphism of lattices

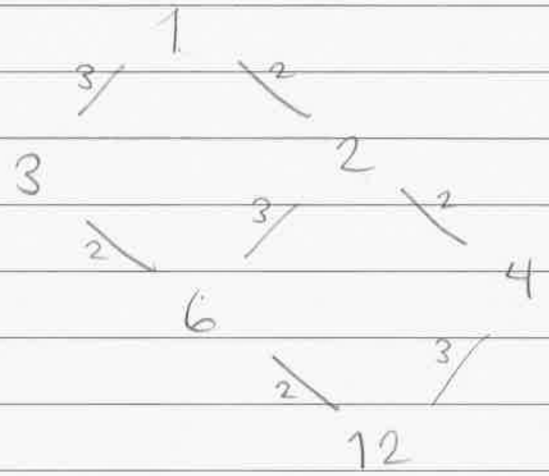
$$\mathcal{L}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}) \approx \mathcal{L}_{\mathbb{Z}}(\mathbb{Z}, n\mathbb{Z})$$

$$= \mathcal{L}_{Ab}(\mathbb{Z}, n\mathbb{Z})$$

$$\approx \mathrm{Div}(n)^{op},$$

i.e.,

the lattice of divisors of n under reverse-divisibility. The length of $\mathbb{Z}/n\mathbb{Z}$ is the length of any maximal chain in this lattice.



If $n = p_1^{n_1} p_2^{n_2} p_3^{n_3} \cdots$ for distinct primes $p_1 < p_2 < p_3 < \cdots$, one can see that the length is

$$\ell(\mathbb{Z}/n\mathbb{Z}) = n_1 + n_2 + n_3 + \cdots,$$

i.e., the length of the prime factorization of n.

Note also that $\ell(\mathbb{Z}) = \infty$, so in this case length does not agree with our intuition about "dimension".

In this case we would do better to look only at chains of prime ideals. The corresponding length is called the "Krull dimension" and we have

$$\mathrm{Kr.dim}(\mathbb{Z}) = 1,$$

which looks nicer.

You see that the word "dimension" is ambiguous. We'll be careful not to use it without qualification.

2/4/16

HW1 extended until Tuesday.

Today : The category R-mod (cont.)

Let R be a ring and consider a left module $M \in R\text{-Mod}$. We saw last time that the collection $\mathcal{L}_R(M)$ of submodules of M is a "modular lattice" with

$$A \wedge B = A \cap B \quad \& \quad A \vee B = A + B$$

for all $A, B \in \mathcal{L}_R(M)$. In the special situation that

$$A \cap B = 0 \quad \& \quad A + B = M$$

we will write $M = A \oplus B$ and say that M is the <u>internal direct sum</u> of A & B.

We can also characterize the direct sum externally.

Definition : Given $M, N \in R\text{-Mod}$ we define the direct sum as the Cartesian product set

$$M \oplus N := \{ (m,n) : m \in M, n \in N \}$$

together with the "direct product" group structure

$$(m_1, n_1) + (m_2, n_2) := (m_1 + m_2, n_1 + n_2)$$

and the left R-action

$$r(m,n) := (rm, rn) .$$

///

It is easy to check that $\oplus$ is the categorical product in R-Mod: We have projections

$$\begin{aligned} \pi_M : M \oplus N &\to M \\ (m,n) &\mapsto m \end{aligned} \quad \& \quad \begin{aligned} \pi_N : M \oplus N &\to N \\ (m,n) &\mapsto n \end{aligned}$$

such that for all $P \in$ R-Mod with maps $\varphi_M : P \to M$ & $\varphi_N : P \to N$, the map

$$\begin{aligned} \varphi_M \times \varphi_N : P &\longrightarrow M \oplus N \\ p &\longmapsto (\varphi_M(p), \varphi_N(p)) \end{aligned}$$

is the unique solution to the diagram

$$\begin{tikzcd}
 & & M \\
P \arrow[r, dashed, "\varphi_M \times \varphi_N"] \arrow[urr, bend left, "\varphi_M"] \arrow[drr, bend right, "\varphi_N"'] & M \oplus N \arrow[ur, "\pi_M"'] \arrow[dr, "\pi_N"] & \\
 & & N
\end{tikzcd}$$.

The reason we don't call it "$M \times N$" is because $\oplus$ is also the coproduct in R-Mod: We have inclusions

$$i_M : M \longrightarrow M \oplus N \quad \& \quad i_N : N \longrightarrow M \oplus N$$
$$m \longmapsto (m, 0_N) \qquad\qquad n \longmapsto (0_M, n)$$

such that for all $P \in R$-Mod with maps $\psi_M : M \to P$ & $\psi_N : N \to P$, the set function

$$\psi_M \oplus \psi_N : M \oplus N \longrightarrow P$$
$$(m, n) \longmapsto \psi_M(m) + \psi_N(n)$$

is the unique map such that

$$\begin{tikzcd}
M \arrow[dr, "i_M"'] \arrow[drr, bend left, "\psi_M"] & & \\
 & M \oplus N \arrow[r, dashed, "\psi_M \oplus \psi_N"] & P \\
N \arrow[ur, "i_N"] \arrow[urr, bend right, "\psi_N"'] & &
\end{tikzcd}$$.

The fact that the set function $\psi_M \oplus \psi_N$ is actually an R-module homomorphism depends on the commutativity of $(P, +, 0_P)$ and the additivity of the left R-actions.

Thus we will use $\oplus$ for both the product & coproduct in R-Mod.

[However, <u>infinite</u> products & coproducts do not agree; see HW 1.1.]

The category R-Mod has a zero object given by the "zero module" 0, hence between any two modules $M, N \in$ R-Mod we have a unique <u>zero map</u> $0_{MN} : M \to N$ defined by

$$\begin{tikzcd}
M \arrow[r, "\exists!"'] \arrow[rr, bend left, "0_{MN}"] & 0 \arrow[r, "\exists!"'] & N
\end{tikzcd}$$

This allows us to define kernels & cokernels as follows.

☆ Definition: Let $\varphi : M \to N$ be any homomorphism of R-modules.

- The <u>kernel</u> of φ is a pair $(\ker\varphi, i)$ where $\ker\varphi \in R\text{-Mod}$ and $i : \ker\varphi \longrightarrow M$ is a map satisfying

(1)

$$\begin{tikzcd}
P \arrow[dr, "\alpha"] \arrow[drr, bend left, "\theta"] \arrow[dd, dashed, "\exists!\bar{\alpha}"'] & & \\
& M \arrow[r, "\varphi"] & N \\
\ker\varphi \arrow[ur, "i"] \arrow[urr, bend right, "0"'] & &
\end{tikzcd}$$

- The <u>cokernel</u> of φ is a pair $(\operatorname{coker}\varphi, \pi)$ where $\operatorname{coker}\varphi \in R\text{-Mod}$ and $\pi : N \longrightarrow \operatorname{coker}\varphi$ is a map satisfying

(2)

$$\begin{tikzcd}
& & P \\
M \arrow[r, "\varphi"] \arrow[urr, bend left, "0"] \arrow[drr, bend right, "0"'] & N \arrow[ur, "\beta"] \arrow[dr, "\pi"'] & \\
& & \operatorname{coker}\varphi \arrow[uu, dashed, "\exists!\bar{\beta}"']
\end{tikzcd}$$

Theorem: kernels & cokernels <u>exist</u> in R-Mod.

<u>Proof</u>: One can check that the set-theoretic kernel satisfies (1) and the quotient map $\pi : N \longrightarrow N/\operatorname{im}\varphi$ satisfies (2). ///

Furthermore, every kernel is a monomorphism ("left-concelable") in the sense that

$$\begin{tikzcd} Z \arrow[r, shift left, "\alpha"] \arrow[r, shift right, "\beta"'] & \ker\varphi \arrow[r, "i"] & M \end{tikzcd} \implies \alpha = \beta$$

$$\text{"} i\circ\alpha = i\circ\beta \text{"}$$

and every cokernel is an epimorphism ("right-concelable") in the sense that

$$\begin{tikzcd} N \arrow[r, "\pi"] & \operatorname{coker}\varphi \arrow[r, shift left, "\alpha"] \arrow[r, shift right, "\beta"'] & Z \end{tikzcd} \implies \alpha = \beta \, .$$

$$\text{"} \alpha\circ\pi = \beta\circ\pi \text{"}$$

Proof: For the first, we have a diagram

$$\begin{tikzcd} Z \arrow[dr, "i\circ\alpha = i\circ\beta"] \arrow[drr, bend left, "0"] \arrow[dd, shift right, "\alpha"'] \arrow[dd, shift left, "\beta"] & & \\ & M \arrow[r, "\varphi"] & N \\ \ker\varphi \arrow[ur, "i"'] \arrow[urr, bend right, "0"] & & \end{tikzcd}$$

By uniqueness, we have $\alpha = \beta$.

For the second, we have a diagram

$$\begin{tikzcd}
& & Z \\
M \arrow[r, "\varphi"] \arrow[urr, bend left, "0"] \arrow[drr, bend right, "0"'] & N \arrow[ur, "\alpha\circ\pi=\beta\circ\pi"] \arrow[dr, "\pi"] & \\
& & \operatorname{coker}\varphi \arrow[uu, shift left, "\alpha"] \arrow[uu, shift right, "\beta"']
\end{tikzcd}$$

By uniqueness, we have $\alpha = \beta$. ///

Note that this proof works in <u>any</u> category with a zero object. In the category R-Mod we will also find that

monomorphism $\Longrightarrow$ kernel
epimorphism $\Longrightarrow$ cokernel .

But this is a very special property [in fact, we will find that this property almost <u>characterizes</u> R-Mod]. To prove it we need to discuss the "enriched" structure of R-Mod.

Given left modules $M, N \in$ R-Mod we will use the notation

$$\operatorname{Hom}_R(M,N) := \operatorname{Hom}_{R\text{-Mod}}(M,N).$$

We already know that $\mathrm{Hom}_{Ab}(M,N)$ is an abelian group and in fact

$$\mathrm{Hom}_R(M,N) \subseteq \mathrm{Hom}_{Ab}(M,N)$$

is a subgroup.

Q: Is $\mathrm{Hom}_R(M,N)$ also an R-module?

A: No, not in general. However, if M is also an (R, S)-bimodule [meaning it carries a right S-action commuting with the left R-action] then we can define a left S-module structure on $\mathrm{Hom}_R(M,N)$ by setting

$$(s\varphi)(m) := \varphi(ms) \quad \forall\ m \in M.$$

If R happens to be commutative then every R-module is an (R, R)-bimodule and so $\mathrm{Hom}_R(M,N)$ is always an R-module.

[If R is a field and M, N are finite dimensional vector spaces then $\mathrm{Hom}_R(M,N)$ is a vector space of rectangular matrices.]

Furthermore, if $\beta_1, \beta_2 \in \mathrm{Hom}_R(M, N)$ and $\alpha_1, \alpha_2 \in \mathrm{Hom}_R(N, P)$ then we have

- $\alpha_1 \circ (\beta_1 + \beta_2) = \alpha_1 \circ \beta_1 + \alpha_1 \circ \beta_2$
- $(\alpha_1 + \alpha_2) \circ \beta_1 = \alpha_1 \circ \beta_1 + \alpha_2 \circ \beta_1$

[we say composition is "biadditive"]

and if R is commutative with $r \in R$ we have

- $\alpha_1 \circ (\beta_1 + r\beta_2) = \alpha_1 \circ \beta_1 + r(\alpha_1 \circ \beta_2)$
- $(\alpha_1 + r\alpha_2) \circ \beta_1 = \alpha_1 \circ \beta_1 + r(\alpha_2 \circ \beta_1)$

[we say composition is "R-bilinear"].

In summary we can say that

"R-Mod is enriched over Ab"

and when R is commutative,

"R-Mod is enriched over R-Mod".

Finally, we can prove the theorem.

☆ Theorem : In the category R-Mod we have

monomorphism $\Longrightarrow$ kernel
epimorphism $\Longrightarrow$ cokernel.

Proof Sketch : We'll show the first statement. The proof of the second statement is similar.

So let $\varphi : M \longrightarrow N$ be a monomorphism of left R-modules. In fact we will show that φ is the kernel of its cokernel, which is

$$\pi : N \longrightarrow N/\text{im}\,\varphi .$$

Since φ is a monomorphism we can use the "enriched" structure of R-Mod to show that $\ker\varphi = 0$ and hence φ is injective [details omitted].

Now let $\alpha : P \to N$ be any morphism satisfying $\pi \circ \alpha = 0$.

We will show that

(*)

$$\begin{tikzcd}
P \arrow[dr, "\alpha"] \arrow[drr, bend left, "0"] \arrow[dd, dashed, "\exists!\overline{\alpha}"'] & & \\
& N \arrow[r, "\pi"] & N/\mathrm{im}\varphi \\
M \arrow[ur, "\varphi"] \arrow[urr, bend right, "0"'] & &
\end{tikzcd}$$

and it will follow that φ is isomorphic the kernel of π.

To show this, note that $\ker\pi = \mathrm{im}\varphi$ is the set-theoretic kernel of π with inclusion $i : \mathrm{im}\varphi \longrightarrow N$. By the 1st Isomorphism Theorem we obtain an isomorphism $\overline{\Phi} : \mathrm{im}\varphi \longrightarrow M = M/\ker\varphi$ such that $\varphi \circ \overline{\Phi} = i$, and hence a diagram

$$\begin{tikzcd}
P \arrow[dr, "\alpha"] \arrow[drr, bend left, "0"] \arrow[d, dashed, "\exists\gamma?"] \arrow[dd, bend right=60, "\exists!\beta"'] & & \\
M \arrow[r, "\varphi"] \arrow[rr, bend right, "0"] & N \arrow[r, "\pi"] & N/\mathrm{im}\varphi \\
\mathrm{im}\varphi \arrow[u, "\overline{\Phi}"] \arrow[ur, "i"'] \arrow[urr, bend right, "0"'] & &
\end{tikzcd}$$

If γ exists then it must be defined by

$$\gamma := \Phi \circ \beta$$

and we observe that this definition commutes with the rest of the diagram because

$$\varphi \circ \gamma = \varphi \circ (\Phi \circ \beta) = (\varphi \circ \Phi) \circ \beta = i \circ \beta = \alpha$$

Finally, if $\bar{\alpha}$ is any map making $\circledast$ commute then we must have

$$\begin{aligned} i \circ (\Phi^{-1} \circ \bar{\alpha}) &= (i \circ \Phi^{-1}) \circ \bar{\alpha} \\ &= \varphi \circ \bar{\alpha} \\ &= \alpha \end{aligned}$$

and then by uniqueness of β we have

$$\begin{aligned} \Phi^{-1} \circ \bar{\alpha} &= \beta \\ \bar{\alpha} &= \Phi \circ \beta = \gamma . \end{aligned}$$

QED.

Why am I bothering telling you this?

Because it turns out that the theorem

monomorphism ⟹ kernel
epimorphism ⟹ cokernel

is the most important property of R-Mod. This is captured by the following definition and "Cayley-type" theorem.

☆ Definition: A category $\mathcal{C}$ is abelian if

- it has a zero object
- it has finite products & coproducts
- it has kernels & cokernels
- all monomorphisms are kernels & all epimorphisms are cokernels.

Amazingly, this definition implies that the category $\mathcal{C}$ is enriched over Ab. Even more amazingly, we have the following theorem that says that the definition of abelian category faithfully captures the properties of R-Mod.

☆ Freyd-Mitchell Embedding Theorem:

Let $\mathcal{C}$ be a small abelian category. Then there exists a ring R such that $\mathcal{C}$ can be embedded as a full subcategory of R-Mod.

More generally, if $\mathcal{C}$ is *any* abelian category (small or not) and if $P \in \mathcal{C}$ is a "compact, projective generator of $\mathcal{C}$" (whatever that means) then we have

$$\mathcal{C} = R\text{-Mod}$$

where $R = \mathrm{End}_{\mathcal{C}}(P)$.

///

Maybe some day (on some planet) algebra classes will begin with the definition of abelian categories...

Maybe not.