3/3/16

HW 2 due now.
Midterm Exam on Tues Mar 15
(after the spring break).

Today: Review for Midterm.

The theme for MTH 762 is algebraic structures with more than one binary operation.

To motivate this we looked at the category Ab of abelian groups. It differs from the category Grp of all groups in two significant ways.

1. Coproduct, cokernel, colimits in general are much nicer in Ab.

Given $A, B \in Ab$ their categorical product is <u>also</u> their coproduct and we call it the direct sum

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

Proof: Consider the injective homomorphisms

$$i_A : A \longrightarrow A \oplus B \qquad \& \qquad i_B : B \longrightarrow A \oplus B$$
$$a \longmapsto (a, 0_B) \qquad\qquad b \longmapsto (0_A, b).$$

Now let C be any <u>abelian</u> group and consider two homomorphisms

$$\varphi_A : A \longrightarrow C \qquad \& \qquad \varphi_B : B \longrightarrow C.$$

We want to show that there exists a unique homomorphism $\varphi : A \oplus B \longrightarrow C$ such that

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

<u>If</u> such φ exists then it must satisfy

$$\begin{aligned}
\varphi(a, b) &= \varphi\big((a, 0_B) + (0_A, b)\big) \\
&= \varphi(a, 0_B) + \varphi(0_A, b) \\
&= \varphi(i_A(a)) + \varphi(i_B(b)) \\
&= \varphi_A(a) + \varphi_B(b).
\end{aligned}$$

Certainly such a function exists, but is it a group homomorphism?

Yes. Since C is abelian we have

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

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

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

as desired. ///

2. Ab is enriched over Ab.

Given any group $G \in \mathrm{Grp}$ and any set $S \in \mathrm{Set}$ we can give the hom set

$$\mathrm{Hom}_{\mathrm{set}}(S, G)$$

the structure of a group by defining

$$(fg)(s) := f(s)g(s).$$

If S is also a group then the product of homomorphisms is not necessarily a homomorphism:

$$\begin{aligned}(fg)(st) &= f(st)g(st)\\ &= f(s)f(t)g(s)g(t)\\ &\neq f(s)g(s)f(t)g(t)\\ &= (fg)(s)(fg)(t).\end{aligned}$$

☹

However, if G is abelian then the above equation becomes true and we conclude that the hom set

$$\mathrm{Hom}_{Grp}(S,G)$$

is a (necessarily abelian) group. Given any other abelian group H we can also consider the composition function

$$(*) \quad \mathrm{Hom}_{Grp}(G,H)\times \mathrm{Hom}_{Grp}(S,G) \longrightarrow \mathrm{Hom}_{Grp}(S,H)$$

$$(f,g) \longmapsto f\circ g.$$

Finally, we observe that composition respects the group structures (we say that $(*)$ is "bi-additive"):

- $(f_1+f_2)\circ g = (f_1\circ g)+(f_2\circ g)$
- $f\circ(g_1+g_2) = (f\circ g_1)+(f\circ g_2)$

In summary, we say that "Ab is enriched over Ab". This means that for any abelian groups $A, B \in Ab$ the hom set $Hom_{Ab}(A,B)$ has a natural abelian group structure and composition of morphisms is biadditive with respect to this structure.

///

What is a ring?

Consider an abelian group $A \in Ab$ and its set of endomorphisms

$$End_{Ab}(A) := Hom_{Ab}(A,A).$$

By the above remarks we know that

- $(End_{Ab}(A), +, 0_{AA})$ is an abelian group
- $(End_{Ab}(A), \circ, id_A)$ is a monoid.
- Composition distributes over addition.

We will say that an abstract structure

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

is a ring if it satisfies these three properties.

"Cayley Theorem": This definition is not too general. That is, given an abstract ring R there exists an abelian group A and an injective ring homomorphism

$$R \hookrightarrow \mathrm{End}_{Ab}(A).$$

Proof: Let $R \mapsto |R|$ denote the forgetful functor $\mathrm{Rng} \to \mathrm{Ab}$. Then the function

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

$$r \longmapsto \lambda_r$$

defined by $\lambda_r(a) := r \circ a$ is an injective ring homomorphism. [Why does right multiplication by r not work?]

///

What is a module?

There are heuristic and formal ways to motivate this. Today I'll be formal.

Definition: A left R-module is a pair (A, φ) where A is an abelian group and

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

is a ring homomorphism.

[The "Cayley Theorem" says that R is a (faithful) left module over itself. Its submodules are called "left ideals".]

There are two ways to study R-modules.

1. Internal.

Let M be an R-module. An R-submodule is a subgroup $N \subseteq (M, +, 0)$ such that

$$n_1, n_2 \in N \ \& \ r \in R \implies n_1 + r n_2 \in N.$$

Let $\mathcal{L}_R(M)$ denote the collection of R-submodules of M. This is a (modular) lattice with

$$1 = M$$
$$0 = (0_M)$$
$$\wedge = \cap$$
$$\vee = +$$

In this language, the 1st, 2nd & 3rd Isomorphism Theorems and the Jordan–Hölder Theorem carry over word for word. One needs only to check that the left $(R, \circ, 1)$-action doesn't ruin things.

[Remark: The situation for rings is more awkward because there are two distinguished kinds of subobjects:

ideals = kernels
subrings = images.

For R-modules we have

submodules = kernels = images,

which is even better than in Grp!]

You should know the statements of the Isomorphism Theorems and be able to prove bits and pieces of them. [I won't ask for the hard bits like Zassenhaus or Schreier.]

We define the internal direct sum of R-modules as follows.

Definition: Let $A, B \in \mathcal{L}_R(M)$. If

- $A + B = M$
- $A \cap B = (0)$

then we will write $M = A \oplus B$. ///

2. External.

We can rephrase the definition by saying that an R-module is an "additive functor"

$$F : R \longrightarrow Ab$$

[We think of R as category with one object that is "enriched over Ab".]

and in this case it becomes obvious that a morphism of R-modules should be a natural transformation.

In more mundane terms we say that a group homomorphism $\varphi : M \to N$ is a morphism of R-modules if for all $r \in R$ we have:

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

$\varphi(r(m)) = r(\varphi(m))$ for all $m \in M$.

The resulting category R-Mod shares so many properties with Ab that we go so far as to call it an "abelian category".

[Remark: $\mathbb{Z}$ is the initial object in Rng and $\mathbb{Z}$-Mod = Ab. This is the sense in which Ab is the prototype for R-Mod.]

That was the general framework. Then we zoomed in to investigate particularly nice modules and modules over particularly nice rings.

1. Nice Modules.

Let R be a <u>ring</u> and consider a <u>set</u> A. The <u>free R-module generated by A</u> is a pair (i, M) where

- M is an R-module and $i : A \to M$ is a function
- If N is any R-module and $j : A \to N$ is any function then there exists a unique R-module homomorphism $\varphi : M \to N$ such that

$$\begin{tikzcd} M \arrow[rr, "\exists! \varphi"] & & N \\ & A \arrow[ul, "i"] \arrow[ur, "j"'] & \end{tikzcd}$$

If such a pair (i, M) exists then the function $i : A \to M$ is injective and the module M is unique up to isomorphism.

Alternatively, we would like to define a "free functor" $F : \text{Set} \longrightarrow R\text{-Mod}$ that is left adjoint to the "forgetful functor" $\mathcal{U} : R\text{-Mod} \longrightarrow \text{Set}$ in the sense that for all $A \in \text{Set}$ and $M \in R\text{-Mod}$ we have a "natural bijection"

$$\text{Hom}_{\text{Set}}(A, \mathcal{U}(M)) = \text{Hom}_{R\text{-Mod}}(F(A), M).$$

[A linear function is defined by its values on a basis.]

//

Theorem: Free modules exist.

Proof: The coproduct $R^{\oplus A}$ and the function $i : A \longrightarrow R^{\oplus A}$ defined by

$$i_a(b) = \begin{cases} 1_R & a = b \\ 0_R & a \neq b \end{cases}$$

satisfy the desired universal property. //

Now let M be an R-module and consider an "indexed subset" $A \longrightarrow M$ denoted by $a \longmapsto m_a$. Let $\varphi : R^{\oplus A} \longrightarrow M$ be the canonical R-module homomorphism from the free module. We say that $A \to M$ is

- linearly independent,
- spanning,
- a basis,

depending on whether $\varphi : R^{\oplus A} \to M$ is

- injective,
- surjective,
- bijective,

respectively. Thus a module has a basis if and only if it is free. It is straightforward to check the following general property:

☆ Each basis is a maximal linearly independendent set and a minimal spanning set.

But the converse is not true in general.
[Example: Look at the bases, maximal independent sets and minimal spanning sets of $\mathbb{Z}$ as a $\mathbb{Z}$-module.]

2. Modules Over Nice Rings.

If $R = K$ is a <u>field</u> then it is straightforward to check that

☆ Each maximal linearly independent set and each minimal spanning set is a basis.

Then assuming Zorn's Lemma (existence of maximal linearly independent sets) we conclude that every <u>vector space is free</u>.

Furthermore, the Steinitz Exchange Lemma tells us that for all sets A, B we have

$$K^{\oplus A} \approx K^{\oplus B} \Longrightarrow |A| = |B|,$$

hence the <u>dimension</u> of a vector space is well-defined.

Then, using the trick of "localization" we can prove that if R is an integral domain then every maximal linearly independent subset of M has the same size, which we call the rank of M.

Remarks:

- The idea is straightforward but there are many details to check [see HW 2 solutions].
- The same is not true for minimal spanning sets [for example, $\{1\}$ and $\{2,3\}$ are minimal spanning in $\mathbb{Z}$ but they don't have the same size].

///

But not every maximal linearly independent set is a basis because there max be torsion elements [$m \in M$ such that there exist $r \in R \setminus \{0\}$ with $rm = 0$]. Let $Tor_R(M)$ be the set of torsion elements. If R is a domain then $Tor_R(M) \subseteq M$ is a submodule and the quotient $M/Tor_R(M)$ is torsion free [has no nonzero torsion elements].

Similarly if M is a module of rank k over a domain R and if $F \subseteq M$ is a maximal free submodule then we have $F \approx R^{\oplus k}$ and the quotient M/F is torsion [consists of torsion elements].

For a general domain R it is difficult to compare these concepts [the torsion submodule & maximal free submodules], however if R is a PID then we obtain the following.

☆ FTFGMPID, Part I.

Let R be a PID and let M be an R-module. If M is finitely generated of rank k then we have

$$M \approx R^{\oplus k} \oplus \mathrm{Tor}_R(M).$$

///

You do not need to memorize the proof of this, but you should know that it's based on the following four lemmas.

↓

Lemma 1: The direct sum of free modules is free with basis given by the disjoint union of bases,

$$R^{\oplus A} \oplus R^{\oplus B} \approx R^{\oplus (A \sqcup B)}.$$

Lemma 2: If F is a free R-module, then every short exact sequence

$$0 \to M \to N \to F \to 0$$

of R-modules <u>splits</u>.

Lemma 3: If R is a PID then every submodule of $R^{\oplus A}$ is free of rank $\leq |A|$.

Lemma 4: If R is a PID then every finitely generated torsion free R-module is free.

[None of these Lemmas is trivial to prove from scratch, and I would never ask you to do such a thing on an exam.]