2/9/16

HW 1 due now

After discussing the general theory of modules, today we move on to a new topic:

Modules over a PID.

Until further notice, all rings are assumed to be commutative. So let R be a (commutative) ring.

★ Definition: We say that R is an integral domain ("domain", for short) if for all $a, b \in R$ we have

$$ab = 0 \implies a = 0 \text{ or } b = 0.$$

Among domains we have the following chain of implications:

Field $\implies$ Euclidean $\implies$ PID $\implies$ UFD.

I assume you've seen this before, but let me quickly sketch the details.

Let $A \subseteq R$ be a subset of a (commutative) ring. We will write

$$(A) := \bigcap_{A \subseteq I} I$$

for the intersection of all ideals $I \subseteq R$ that contain A. We call this the ideal of R generated by A.

If $A = \{a_1, a_2, \cdots, a_n\}$ we will write

$$(a_1, a_2, \cdots, a_n) := (\{a_1, a_2, \cdots, a_n\}).$$

Ideals of this form are called finitely generated. Ideals of the form $(a) = (\{a\})$ are called principal.

★ Definition: An integral domain R is called a PID ("principal ideal domain") if for each ideal $I \subseteq R$ there exists an element $a \in R$ such that

$$I = (a).$$

We say that R is a field if its group of units satisfies $R^\times = R \setminus \{0\}$. Equivalently, its only ideals are the trivial ideals

$$0 = (0) \quad \& \quad R = (1).$$

Proof: Let R be a field with ideal $I \subseteq R$. If $I \neq (0)$ then $\exists\ 0 \neq a \in I$. But then $1 = aa^{-1} \in I$ and hence $I = (1)$. Conversely, suppose R has no nontrivial ideals and consider an element $a \neq 0$. Since $(a) \neq (0)$ we must have $(a) = (1)$. Now since $1 \in (a)$, $\exists\ b \in R$ such that $ab = 1$. ///

Thus a field is a PID. More generally, we make the following definition.

★ Definition: A domain R is called Euclidean if there exists a function $\delta : R \setminus \{0\} \to \mathbb{N}$ such that for all $a, b \in R$ with $b \neq 0$ there exist $q, r \in R$ with

- $a = qb + r$
- $r = 0$ or $\delta(r) < \delta(b)$.

Remark: There are really only two interesting examples of Euclidean domains

- $\mathbb{Z}$ with $\delta(a) = |a|$
- $K[x]$ with $\delta(f) = \deg(f)$.

and the definition is meant to abstract their common properties. But the Euclidean domain concept is actually not used much because of the following theorem.

★ Theorem: Euclidean $\Rightarrow$ PID.

Proof: Let (R, δ) be Euclidean and consider an ideal $I \subseteq R$. If $I = (0)$ then we're done so suppose that $I \neq (0)$. Then the set $\delta(I \setminus \{0\}) \subseteq \mathbb{N}$ is nonempty, so by well-ordering it has a smallest element $n \in \delta(I \setminus \{0\})$. Choose $a \in I \setminus \{0\}$ so that $\delta(a) = n$. Clearly we have $(a) \subseteq I$. I claim that we also have $I \subseteq (a)$. Indeed, consider any $b \in I$. Since $a \neq 0$, $\exists\, q, r \in R$ such that

- $b = qa + r$
- $r = 0$ or $\delta(r) < \delta(a)$

The first equation implies that $r = b - qa \in I$. If $r \neq 0$ then by minimality we must have $\delta(a) \leq \delta(r)$, which contradicts the second condition above. Hence $r = 0$ and we conclude that $b = qa \in (a)$. ///

Not all PIDs are Euclidean but we prefer to think of $\mathbb{Z}$ & $K[x]$ as PIDs because the language of PIDs is more natural.

Let R be a ring. Given elements $a, b \in R$ we define the notion of "divisibility in R" by

$$a \mid b \iff (b) \subseteq (a)$$

Note that $a \mid 0$ and $1 \mid a$ for all $a \in R$. We will say that a is a proper divisor of b if

$$(b) \overset{1}{\subsetneq} (a) \overset{2}{\subsetneq} (1).$$

The first inclusion means that a is not associate to b (i.e. we don't have $a = ub$ and $b = u^{-1}a$ for some unit $u \in R^\times$)

}

and the second inclusion says that a itself is not a unit. We say that an element of R is irreducible if it has no proper divisors.

★ Definition: A domain R is called a UFD if every nonzero, nonunit element can be written uniquely as a product of irreducible elements.

★ Theorem: PID $\Rightarrow$ UFD.

Proof: Let R be a PID. There are two steps in the proof.

Step 1: Every element $a \in R$ has a factorization into irreducibles.

If not, then we obtain an infinite increasing chain of ideals.

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots$$

Note that the union $I := \bigcup_{n \in \mathbb{N}} (a_n)$ is an ideal. Since R is a PID we must have $I = (b)$ for some $b \in R$.

But then since $b \in \bigcup_n (a_n)$ there exists $m \in \mathbb{N}$ such that $b \in (a_m)$. It follows that

$$(b) \subseteq (a_m) \subsetneq (a_{m+1}) \subsetneq I = (b),$$

which is a contradiction. ///

Step 2 : "Euclid's Lemma"

We say that an element $p \in R$ is prime if for all $a, b \in R$ we have

$$p \mid ab \implies p \mid a \text{ or } p \mid b$$

$$ab \in (p) \implies a \in (p) \text{ or } b \in (p).$$

[Note : R is a domain $\iff$ $0 \in R$ is prime]

Now let $p \in R$ be irreducible. We will show that p is also prime. Indeed, suppose we have $a, b \in R$ such that

$$ab \in (p) \quad \& \quad a \notin (p)$$

We will show that $b \in (p)$.

↓

Since $a \notin (p)$ we have $(p) \subsetneq (a,p)$ and since R is a PID we have

$$(p) \subsetneq (a,p) = (c)$$

for some $c \in R$. Then since p is irreducible we must have $(a,p) = (c) = (1)$. Since $1 \in (a,p)$ there exist $x, y \in R$ such that

$$ax + py = 1.$$

Multiply both sides by b to get

$$\begin{aligned} abx + pby &= b \\ pdx + pby &= b \qquad (\text{since } ab \in (p)) \\ p(dx + by) &= b. \end{aligned}$$

We conclude that $a \in (p)$. ///

Finally, consider a nonzero, nonunit $a \in R$ and suppose we have two factorizations into irreducibles

$$a = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l.$$

Since $p_1 \mid a$ we have $p_1 \mid q_1 q_2 \cdots q_\ell$. Then by Euclid's Lemma (i.e., irreducible $\Rightarrow$ prime in a PID) and induction there exists i such that $p_1 \mid q_i$. Without loss of generality suppose that $p_1 \mid q_1$. Then since q_1 is irreducible and p_1 is not a unit, there exists a unit $u_1 \in R^\times$ such that $q_1 = u_1 p_1$.

Substiting gives

$$p_1 p_2 \cdots p_k = u_1 p_1 q_2 \cdots q_\ell.$$

Then since R is a domain we can cancel p_1 to get

$$p_2 p_3 \cdots p_k = u_1 q_2 q_3 \cdots q_\ell.$$

At this point we use induction to conclude that $k = \ell$ and that we can reorder the factors such that

$$q_2 = u_2 p_2, \; q_3 = u_3 p_3, \; \cdots, \; q_k = u_k p_k$$

for some units $u_2, u_3, \cdots, u_k \in R^\times$.

QED

2/11/16

No HW2 yet.

Among integral domains we have the following chain of implications:

$$\text{Field} \overset{\times}{\Longrightarrow} \text{Euclidean} \overset{\checkmark}{\Longrightarrow} \text{PID} \overset{\times}{\Longrightarrow} \text{UFD}.$$

This sequence of ideas really goes back to Euclid and the modern form is due to DedeKind. Last time I gave a quick review of the definitions & proofs.

We saw that the definition of "Euclidean domain" is awkward but the language of PIDs is elegant and flexible.

UFDs are also kind of awkward. Last time I taught 762 (then called 662) I pursued the theory of UFDs, which leads to notions of "smoothness" in algebraic geometry. [Notes available on my webpage.]

This time I'm going to look at PIDs, and in particular their module theory which is very nice. I am aiming for the "fundamental theorem of finitely generated modules over a PID", which is a simultaneous generalization of

- the classification of finite abelian groups
- the Jordan canonical form of a matrix.

The simplest kind of PIDs are fields, so we'll start with vector spaces. And since every vector space is "free" we'll start with "free modules". Here's the idea:

Consider an arbitrary ring R and an arbitrary set A. Our goal is to define the left R-module freely generated by the set A.

If it exists, let's call it $F_R(A)$. It should satisfy the following properties.

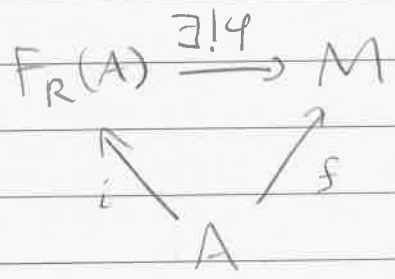
- $A \subseteq F_R(A)$

- Any R-module homomorphism $\varphi: F_R(A) \to M$ is determined by its values on the generating set A.

We can formalize this as a universal property.

☆ Universal Property of Free Modules:

We have a set function $i: A \to F_R(A)$ and for any left R-module M and any set function $f: A \to M$ there exists a unique R-module homomorphism $\varphi: F_R(A) \to M$ satisfying



We could also see this as a final object in a certain category. If $F_R(A)$ exists then by general nonsense it will be unique and the function $i: A \to F_R(A)$ will be injective.

Does it exist?

★ Theorem: Free modules exist.

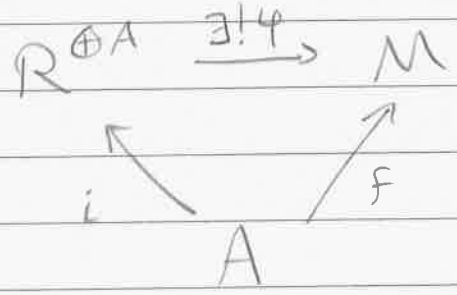
Proof: Consider a ring R and a set A. Following HW1.1(b) we define the R-module

$$R^{\oplus A} := \{ \text{Functions } A \to R \text{ with finite support} \}$$

Now consider the function $i: A \to R^{\oplus A}$ defined by sending $a \in A$ to the function $i_a: A \to R$ such that

$$i_a(b) := \begin{cases} 1 & \text{if } a = b \\ 0 & \text{if } a \neq b \end{cases}.$$

For any R-module M and any set function $f: A \to M$ we will show that there exists a unique R-module map $\varphi: R^{\oplus A} \to M$ satisfying



and hence $(R^{\oplus A}, i)$ is the free module generated by A.

To do this, note that every element $r \in R^{\oplus A}$ can be written uniquely in the form

$$r = \sum_{a \in A} r_a i_a$$

and the sum exists because we have $r_a = 0$ for all but finitely many $a \in A$.

Now the assumption $f = \varphi \circ i$ requires that

$$\begin{aligned} \varphi(r) &= \varphi\left(\sum_a r_a i_a\right) \\ &= \sum_a \varphi(r_a i_a) \quad [\varphi \text{ is additive}] \\ &= \sum_a r_a \varphi(i_a) \quad [\varphi \text{ preserves } R\text{-action}] \\ &= \sum_a r_a f(a) \quad [f = \varphi \circ i]. \end{aligned}$$

This defines a unique function $\varphi : R^{\oplus A} \to M$ and it is not difficult to check that is is an R-module homomorphism.

///

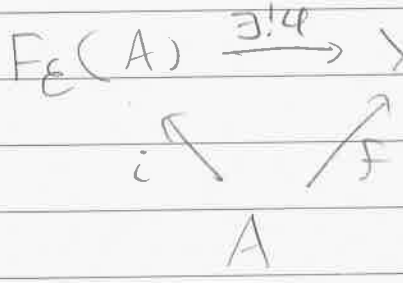
Remarks:

- Given a concrete category $\mathcal{C}$ (i.e. whose objects are sets) and a set A, the free object generated by I consists of

— an object $F_{\mathcal{C}}(A) \in \mathcal{C}$

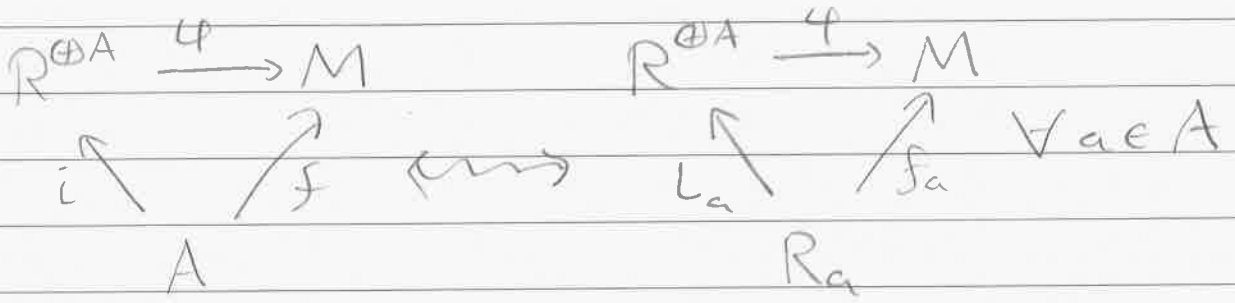
— a set function $i : A \to F_{\mathcal{C}}(A)$

such that for all objects $X \in \mathcal{C}$ and set functions $f : A \to X$ there exists a unique morphism $\varphi : F_{\mathcal{C}}(A) \to X$ in $\mathcal{C}$ such that



There is no reason in general for free objects to exist, but they do exist in most of the categories we care about.

- The proof we gave above is really just a rephrasing of the proof from HW 1.1(6) that $R^{\oplus A}$ is a coproduct in R-Mod. [Actually we only proved it in Ab but the proof extends to R-Mod.] So we could replace one of the proofs with a verification that the following two pieces of data are equivalent:



But doing so would probably make the proof less understandable!

- Given an element $r \in R^{\oplus A}$ the notation

$$r = \sum_{a \in A} r_a i_a$$

gets annoying, so we will usually abuse notation and just write

$$r = \sum_{a \in A} r_a a .$$

Here the symbol "a" really stands for the function $i_a : A \to R$. We do this all the time in linear algebra when we confuse "basis vectors" with their corresponding "coordinate functions".

- If $A = \{a_1, a_2, \cdots, a_n\}$ is finite then we will further abuse notation by writing

$$r = \sum_{i=1}^{n} r_i a_i .$$

We might even write this as a vector

$$r = (r_1, r_2, \cdots, r_n) .$$

- If $|A| = n$, we would like to write

$$R^{\oplus A} = "R^{\oplus n}" .$$

After all, isn't $R^{\oplus A}$ just the direct sum of R with itself n times?

Well, we have to be careful.

We are hoping that the following property is true.

☆ Invariant Basis Number Property (IBN):

For all sets $A, B \in \mathrm{Set}$ we have

$$R^{\oplus A} \approx R^{\oplus B} \iff A \approx B$$

in R-Mod in Set. //

It turns out that the IBN holds in great generality (e.g. it holds for all commutative rings), but not always.

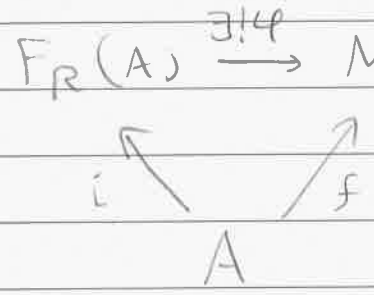
Luckily the cases where it fails are fairly pathological (e.g. the ring of endomorphisms of an infinite dimensional vector space) so they won't cause us any trouble.

2/16/16

Exam 1 is Thurs Mar 3 in class.
HW2: TBA

Let R be a ring and let A be a set. We say that $(F_R(A), i)$ is a <u>free (left) R-module generated by A</u> if

- $F_R(A)$ is a (left) R-module,
- $i : A \to F_R(A)$ is a set function,
- For all (left) R-modules M and set functions $f : A \to M$ there exists a unique R-module homomorphism $\varphi : F_R(A) \to M$ such that



In other words $(F_R(A), i)$ is an <u>initial</u> object in a certain category.

↓

If it exists, then by general nonsense it is unique and the function i is injective.

★ Theorem: Free modules exist.

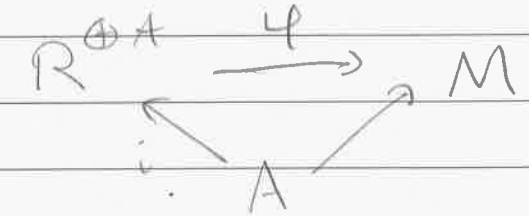
Proof: The coproduct $R^{\oplus A}$ together with the function $i : A \to R^{\oplus A}$ defined by

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

satisfies the universal property. ///.

Now we can use free modules to define the concepts of linearly independent and spanning sets in an R-module.

★ Definition: Consider a module $M \in R\text{-Mod}$ and a set $A \in \mathrm{Set}$. We will call any function $A \to M$ an indexed set of elements of M. Now consider the canonical map $\psi : R^{\oplus A} \to M$ such that



- If φ is injective we say that $A \to M$ is a linearly independent set in M.
- If φ is surjective we say that $A \to M$ is a spanning set in M.
- If φ is both injective and surjective [hence an isomorphism of R-modules] we say that $A \to M$ is a basis for M. ///

Let's unpack this a bit. If we write the function $A \to M$ as $a \mapsto m_a$ and an element $r \in R^{\oplus A}$ as $\sum_{a \in A} r_a i_a$, recall that the hom $\varphi : R^{\oplus A} \to M$ is defined by

$$\varphi(r) = \varphi\left(\sum_{a \in A} r_a i_a\right) = \sum_{a \in A} r_a m_a.$$

Now recall that φ is injective if and only if $\ker \varphi = 0$. So we can rephrase the definition of linear independence by saying that $A \to M$ is linearly independent if and only if

$$\varphi(r) = 0_M \iff r = 0_{R^{\oplus A}}$$

$$\sum_{a \in A} r_a m_a = 0 \iff r_a = 0 \quad \forall\, a \in A,$$

which agrees with the familar definition you learned in linear algebra.

Similarly the set $A \to M$ is spanning if for all $m \in M$ there exists $r \in R^{\oplus A}$ such that

$$m = \varphi(r) = \sum_{a \in A} r_a m_a .$$

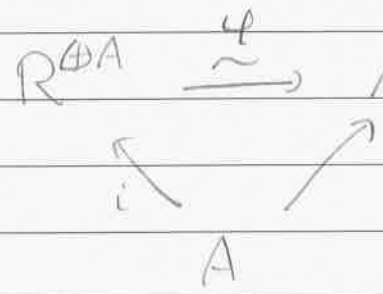
//

★ Theorem: An R-module has a basis if and only if it is free.

Proof: First note that $A \to R^{\oplus A}$ is a basis of $R^{\oplus A}$ because the induced homomorphism $\varphi: R^{\oplus A} \to R^{\oplus A}$ is the identity map (which is an iso.).

$$\begin{array}{ccc} R^{\oplus A} & \xrightarrow{\varphi}_{\cong} & R^{\oplus A} \\ & \nwarrow^{i} \quad \nearrow_{i} & \\ & A & \end{array}$$

Conversely, suppose that $A \to M$ is a basis for some R-module M. Then we obtain an isomorphism



and it follows that $(M, \varphi \circ i)$ is a free module. ///

Q: If M has a basis (i.e. if M is free) does every basis have the same cardinality?

A: Not in general. Given a ring R we say that R has the "invariant basis number" property (IBN) if

$$R^{\oplus A} \approx R^{\oplus B} \implies |A| = |B|.$$

In this case, the cardinality $|A|$ is called the rank of the module $R^{\oplus A}$.

The ring of endomorphisms over an infinite vector space does not have the IBN property, but we will see that most nice rings do have it (including all commutative rings).

To explore this, let's consider the following three concepts from linear algebra:

① basis
② maximal linearly independent set.
③ minimal spanning set.

Note that ① $\Longrightarrow$ ② & ③.

Proof: Let A be a basis for $M \in R\text{-Mod}$.

To show that M is a maximal linearly independent set, consider any $m \in M \setminus A$. Since A is spanning we can write

$$m = \sum_{a \in A} r_a m_a$$

for some $r_a \in R$. But then the set $A \cup \{m\}$ is not linearly independent.

To show that A is a minimal spanning set consider any $m_a \in A$. Now suppose for contradiction that $A \setminus \{m_a\}$ is a spanning set. It follows that we can write

$$m_a = \sum_{a \neq b} r_b m_b$$

for some $r_b \in R$, which contradicts the fact that A is independent. //

In general, though, we have

(2) $\not\Rightarrow$ (1) or (3)
(3) $\not\Rightarrow$ (1) or (2).

Proof: Consider $\mathbb{Z}$ as a $\mathbb{Z}$ module.

Note that $\mathbb{Z}$ is a free $\mathbb{Z}$-module with basis $\{1\} \subseteq \mathbb{Z}$.

To see that (2) $\not\Rightarrow$ (3), consider the set $\{n\} \subseteq \mathbb{Z}$ for any $n \in \mathbb{Z} \setminus \{0, \pm 1\}$. Note that this is an independent set because for any $a \in \mathbb{Z}$ we have $na = 0 \Rightarrow a = 0$.

And it is a maximal independent set since for any $m \in \mathbb{Z} \setminus \{n\}$ we have the nontrivial relation

$$(n)m + (-m)n = 0.$$

However, $\{n\} \subseteq \mathbb{Z}$ is not a spanning set since there exist integers not divisible by n.

To see that ② $\not\Rightarrow$ ③, consider the set $\{m, n\} \subseteq \mathbb{Z}$ for any coprime $m, n \in \mathbb{Z} \setminus \{0, \pm 1\}$ Since m, n are coprime there exist $x, y \in \mathbb{Z}$ such that

$$1 = xm + yn$$

Then for any $a \in \mathbb{Z}$ we have

$$a = (ax)m + (ay)n$$

and hence $\{m, n\}$ is a spanning set. It is minimal since neither of $\{m\}$ or $\{n\}$ is a spanning set. And it is not independent because of the relation

$$(n)m + (-m)n = 0.$$

Remark: It is not a coincidence that all maximal independent sets of $\mathbb{Z}$ have the same size. We will see that this phenomenon holds in general for modules over an integral domain, even for those that have no basis.

However, when $R = K$ is a field the three concepts ①, ②, ③ are equivalent.

Proof: Let $V \in K\text{-Mod}$ be a vector space.

To prove ② $\Rightarrow$ ① let $A \subseteq V$ be a maximal linearly independent set (which exists by Zorn's Lemma). Then for any $v \in V \setminus A$ we have a relation

$$rv + \sum_{a \in r_a} r_a v_a = 0$$

where not all coefficients are zero. Since A is independent this implies that $r \neq 0$. Then since K is a field we can divide by r to get

$$v = \sum_{a \in A} \left(\frac{-r_a}{r}\right) v_a ,$$

which proves that A is a spanning set.

To prove (3) $\Rightarrow$ (1) Let $A \subseteq V$ be a minimal spanning set and assume for contradiction that A is not linearly independent. Then there exists a relation

$$\sum_{a \in A} r_a v_a = 0$$

where not all coefficients are zero. Choose $a \in A$ such that $r_a \neq 0$. Then since K is a field we can divide by r_a to get

$$v_a = \sum_{b \neq a} \left(\frac{-r_b}{r_a} \right) v_b$$

This implies that $A \setminus \{a\}$ is still a spanning set, which contradicts the minimality of A. ///

★ Corollary (assuming Zorn's lemma):

Every vector space is a free module.

To finish, let me give you the original proof that fields have the IBN property. This argument is due to Ernst Steinitz from his paper "Algebraic Theory of Fields" (1910). It was later abstracted by Hassler Whitney and Saunders MacLane into the theory of "matroids".

★ Steinitz Exchange Lemma (1910):

Let K be a field and let $V \in K\text{-Mod}$ be a vector space. Suppose V has a finite spanning set $S \subseteq V$. Then for any independent set $I \subseteq V$ we have

$$|I| \leq |S|.$$

Proof: Let $I = \{i_1, \dots, i_m\}$ and $S = \{s_1, \dots, s_n\}$. Assume for contradiction that $m > n$.

Since S is spanning we can write

$$i_1 = a_1 s_1 + \cdots + a_n s_n$$

for some scalars $a_1, \dots, a_n \in K$.

By independence of I we have $i_1 \neq 0$ and hence at least one of $a_1, \cdots, a_n$ is nonzero. Without loss, say $a_1 \neq 0$. Then since K is a field we can divide by a_1 to get

$$s_1 = \frac{1}{a_1} i_1 - \frac{a_2}{a_1} s_2 - \cdots - \frac{a_n}{a_1} s_n,$$

and it follows that

$$\{i_1, s_2, \cdots, s_n\}$$

is a spanning set. Now assume for induction that the set

$$\{i_1, i_2, \cdots, i_k, s_{k+1}, \cdots, s_n\}$$

is spanning for some $1 \leq k < n$. In this case we have

$$i_{k+1} = b_1 i_1 + \cdots + b_k i_k + b_{k+1} s_{k+1} + \cdots + b_n s_n$$

for some scalars $b_1, \cdots, b_n \in K$. By independence of I we know that at least one of $b_{k+1}, \cdots, b_n$ is nonzero. Without loss, say $b_{k+1} \neq 0$.

Then since K is a field we can divide by b_{k+1} to get

$$s_{k+1} = -\frac{b_1}{b_{k+1}} i_1 - \cdots - \frac{b_k}{b_{k+1}} i_k + \frac{1}{b_{k+1}} i_{k+1} - \frac{b_{k+2}}{b_{k+1}} s_{k+2} - \cdots - \frac{b_n}{b_{k+1}} s_n .$$

and it follows that

$$\{ i_1, i_2, \cdots, i_{k+1}, s_{k+2}, \cdots, s_n \}$$

is a spanning set. By induction we conclude that

$$\{ i_1, i_2, \cdots, i_n \}$$

is a spanning set. Finally, since $m = |I| > |S| = n$ we obtain a relation

$$i_{n+1} = c_1 i_1 + c_2 i_2 + \cdots + c_n i_n ,$$

contradicting the independence of I. ///

★ Corollary: Let K be a field. Then for all finite sets B_1 & B_2 we have

$$K^{\oplus B_1} \approx K^{\oplus B_2} \implies |B_1| = |B_2|.$$

Proof: Let B_1 & B_2 be two bases of a vector space over K. Applying Steinitz one way gives

$$|B_1| \leq |B_2|$$

and applying it the other way gives

$$|B_2| \leq |B_1|.$$

///

[Remark: Maybe this holds for infinite bases too. I don't really care.]

2/18/16

HW 2 still TBA.

If $A \subseteq M$ is a subset of an R-module then there exists a unique R-linear map $\varphi_A : R^{\oplus A} \to M$ such that $\varphi_A(i_a) = a$ for all $a \in A$.

- If φ_A is injective we say that $A \subseteq M$ is linearly independent.
- If φ_A is surjective we say that $A \subseteq M$ is a spanning set.
- If φ_A is bijective (hence an isomorphism) we say that $A \subseteq M$ is a basis.

Thus M has a basis if and only if it is isomorphic to a free module.

Now consider the following three properties a subset $A \subseteq M$ could have:

(1) $A \subseteq M$ is a basis
(2) $A \subseteq M$ is a maximal independent set
(3) $A \subseteq M$ is a minimal spanning set.

↓

Last time we saw that

(1) $\Rightarrow$ (2) and (3)

for general R-modules, and if R is a field then we have

(2) or (3) $\Rightarrow$ (1).

Since every R-module has a maximal independent set (by Zorn's Lemma), this implies that every vector space has a basis, hence is free. Then the Steinitz Exchange Lemma shows that every basis has the same cardinality (i.e. fields satisfy the IBN property).

We also saw that (2) $\not\Rightarrow$ (3) and (3) $\not\Rightarrow$ (2) for abelian groups (i.e. $\mathbb{Z}$-modules)

Example: Consider $\mathbb{Z}$ as a $\mathbb{Z}$-module. It is free with basis $\{1\}$ or $\{-1\}$.

For all $0 \neq n \in \mathbb{Z}$ the set $\{n\} \subseteq \mathbb{Z}$ is maximal independent but is only spanning if $n = \pm 1$.

For all coprime $m, n \in \mathbb{Z} \setminus \{0, \pm 1\}$ the set $\{m, n\}$ is minimal spanning, but it is never linearly independent. ///

We can observe from this that the size of a minimal spanning set is not well-defined because $\{1\}$ and $\{2, 3\}$ are both minimal spanning sets of $\mathbb{Z}$. We also observe that every maximal independent set in $\mathbb{Z}$ has size $\{1\}$.

Furthermore, there exist non-free $\mathbb{Z}$-modules.

Claim: No (nontrivial) finite abelian group is free.

Proof: Let M be a (nontrivial) finite abelian group and consider a subset $A \subseteq M$. If $A \neq \{0\}$ then choose $0 \neq a \in A$. Then since M is a finite group there exists an integer $n > 0$ such that

$$na = \underbrace{a + a + \cdots + a}_{n \text{ times}} = 0$$

and it follows that the set A is not independent. Therefore the only independent subset of M is $\emptyset$, which is certainly not a spanning set. ↑ because M is nontrivial ///

Nevertheless, it will still make sense to discuss the "rank" of an abelian group. Our next goal is to prove the following theorem, which will motivate our interest in integral domains.

★ Theorem: Let R be an integral domain and consider a module $M \in R\text{-Mod}$ (possibly not free). Then every maximal independent subset of M has the same cardinality, which we will call the rank of M. ///

We already have most of the ingredients to prove this. The only missing piece is the following Lemma/construction establishing the close relationship between domains and fields.

↓

☆ Lemma: Let R be a ring. Then

R is an integral domain $\iff$ R is isomorphic to a subring of a field.

Proof: First let R be a subring of a field K and consider $a, b \in R$ such that $ab = 0$ and $a \neq 0$. Then a^{-1} exists in K so that

$$b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$$

in K, hence also in R.

Conversely, let R be an integral domain. We need to construct a field containing a subring isomorphic to R. The trick is to mimic the construction of $\mathbb{Q}$ from $\mathbb{Z}$. We define the set of fractions

$$\mathrm{Frac}(R) := \left\{ \left[\frac{a}{b}\right] : a, b \in R,\ b \neq 0 \right\}$$

together with the equivalence relation

$$\left[\frac{a}{b}\right] = \left[\frac{c}{d}\right] \iff ad = bc$$

and algebrac operations

$$\left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] = \left[\frac{ac}{bd}\right] \quad \& \quad \left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{ad+bc}{bd}\right].$$

(These exist because $b \neq 0$ & $d \neq 0 \Rightarrow bd \neq 0$.)

Now one can check that this defines a field structure on $\mathrm{Frac}(R)$ and that the function

$$R \longrightarrow \mathrm{Frac}(R)$$

$$r \longmapsto \left[\frac{r}{1}\right]$$

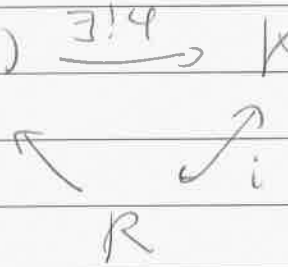
is an injective ring homomorphism. ///

The field $\mathrm{Frac}(R)$ constructed in the proof is called the field of fractions (or quotient field) of the domain R.

It satisfies the following universal property.

☆ Universal Property of Fractions:

Let R be an integral domain. Then for every field K and every injective ring homomorphism $i: R \hookrightarrow K$ there exists a unique ring homomorphism $\varphi: \mathrm{Frac}(R) \to K$ satisfying



[compare to the solution of HW 1.6(b)].

///

I'll sketch the rest of the proof next time and you will fill in the details on HW 2.

2/23/16

Exam 1 is next Thurs Mar 2 in class.
HW 2 is due on Tues Mar 15 (after Spring break). I will add one or two problems later.

Last time we discussed the field of fractions of an integral domain. More generally we have the following construction.

☆ Localization of a Module:

Let R be a commutative ring and let M be an R-module. Let $S \subseteq R$ be a subset satisfying

- $1 \in S$
- $s, t \in S \Rightarrow st \in S$
- S contains no zero divisors.

Then we will define the set of "fractions"

$$S^{-1}M := \left\{ \left[\frac{m}{s}\right] : m \in M, s \in S \right\}.$$

↓

You will prove on HW2 that the relation

$$\left[\frac{m}{s}\right] = \left[\frac{n}{t}\right] \iff tm = sn$$

is an equivalence and that the following operations are well-defined:

$$\left[\frac{m}{s}\right] + \left[\frac{n}{t}\right] = \left[\frac{tm+sn}{st}\right] \quad \& \quad r\left[\frac{m}{s}\right] = \left[\frac{rm}{s}\right].$$

Furthermore, you will show that this makes $S^{-1}M$ into an R-module with a canonical R-module homomorphism

$$\begin{aligned} M &\longrightarrow S^{-1}M \\ m &\longmapsto \left[\frac{m}{1}\right], \end{aligned}$$

We call $S^{-1}M$ a localization of M.
We can also localize the ring R by

- defining $S^{-1}R$ as an R-module
- defining multiplication by $\left[\frac{r_1}{s}\right]\left[\frac{r_2}{t}\right] = \left[\frac{r_1 r_2}{st}\right]$.

and then $S^{-1}M$ becomes an $S^{-1}R$-module.

Picture:

$$\begin{array}{ccc} S^{-1}R & \circlearrowright & S^{-1}M \\ \uparrow & & \uparrow \\ R & \circlearrowright & M \end{array}$$

(the vertical arrows are not necessarily injective)

★ Special Case: Let R be an integral domain and take $S = R \setminus \{0\}$ so that $S^{-1}R$ is the field of fractions

Now let M be an R-module with localization $S^{-1}M$ and consider a subset

$$\begin{array}{ccc} M & \longrightarrow & S^{-1}M \\ \cup & & \cup \\ A & \longrightarrow & S^{-1}A \end{array}$$

If A is a maximal R-linearly independent set in M then you will show on HW2 that $S^{-1}A$ is a maximal $S^{-1}R$-linearly independent set in $S^{-1}M$. Then since $S^{-1}R$ is a field (the field of fractions of R)

and since the function $A \to S^{-1}A$ defined by $a \mapsto [a/1]$ is injective (because A is an independent set) we can apply Steinitz Exchange over $S^{-1}R$ to get

★ **Theorem:** Let M be a module over an integral domain R. Then any two maximal R-linearly independent subsets of M have the same cardinality, which we call the rank of M.

Corollary: If R is an integral domain then for any two sets A & B we have

$$R^{\oplus A} \approx R^{\oplus B} \implies |A| = |B|.$$

[i.e. integral domains have the IBN property.]

But recall that not every module over an integral domain is free (has a basis).

Example: Every nontrivial finite abelian group has rank 0 as a $\mathbb{Z}$-module but is not free because $\emptyset$ is not a spanning set. [By convention we set $\mathbb{Z}(\emptyset) := 0$, so the trivial group is free.]

Thus we have seen two kinds of $\mathbb{Z}$-modules:

- Free abelian groups,
- Finite abelian groups.

Are there any other kinds?

In a certain sense, NO. If G is a finitely generated abelian group of rank n, then G is isomorphic to a direct sum

$$G \cong \mathbb{Z}^{\oplus n} \oplus T$$

where T is finitely generated of rank 0, and hence finite.

To make the theorem more useful we'll try to prove it over a general PID.

So let's get started. First we need a definition.

★ Definition: Let R be a commutative ring and let M be an R-module. We say that $m \in M$ is a torsion element if there exists $r \in R \setminus \{0\}$ such that $rm = 0$. We denote the set of torsion elements by

$$\mathrm{Tor}_R(M) := \{ m \in M : \exists\, r \in R \setminus \{0\},\ rm = 0 \}.$$

If R is a domain then $\mathrm{Tor}_R(M) \subseteq M$ is a submodule.

Proof: Let $m, n \in \mathrm{Tor}_R(M)$ so $\exists\, r, s \in R \setminus \{0\}$ such that $rm = sn = 0$. Since R is a domain we also have $rs \in R \setminus \{0\}$. Then for all $a \in R$ we have

$$\begin{aligned} rs(m + an) &= s(rm) + a(sn) \\ &= s \cdot 0 + a \cdot 0 \\ &= 0 \end{aligned}$$

and hence $m + an \in \mathrm{Tor}_R(M)$. ///

Furthermore, the quotient module $M/\mathrm{Tor}_R(M)$ is torsion-free (i.e. has no nonzero torsion elements).

Proof: Assume for contradiction that we have $m + \mathrm{Tor}_R(M) \neq 0 + \mathrm{Tor}_R(M)$ (i.e. $m \in M \setminus \mathrm{Tor}_R(M)$) and $r \in R \setminus \{0\}$ such that

$$0 + \mathrm{Tor}_R(M) = r(m + \mathrm{Tor}_R(M)) = rm + \mathrm{Tor}_R(M),$$

and hence $rm \in \mathrm{Tor}_R(M)$. It follows that $\exists\, s \in R \setminus \{0\}$ such that

$$0 = s(rm) = (rs)m.$$

But since R is a domain we have $rs \in R \setminus \{0\}$ and this implies that $m \in \mathrm{Tor}_R(M)$. Contradiction. ///.

Now I would like to prove the following.

- $M/\mathrm{Tor}_R(M)$ is a free R-module.
- We have a direct sum of R-modules

$$M \cong (M/\mathrm{Tor}_R(M)) \oplus \mathrm{Tor}_R(M).$$

But these results are not true unless we further assume that R is a P.I.D. And to get there we need a slightly better understanding of free modules.

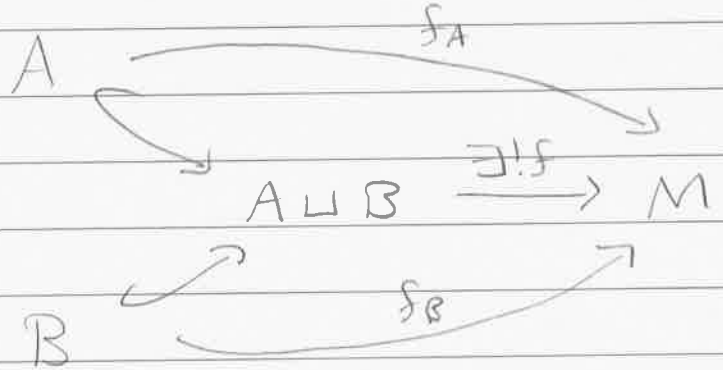
So let's go back to school.

Lemma 1: Let R be any ring and consider any two sets A, B. Then we have

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

Proof: Buckle your seatbelts; I'm going to give the correct proof of this.

First I note that the (external) disjoint union is the coproduct in the category of sets. That is, if M is any set with functions $f_A : A \to M$ & $f_B : B \to M$ then we have

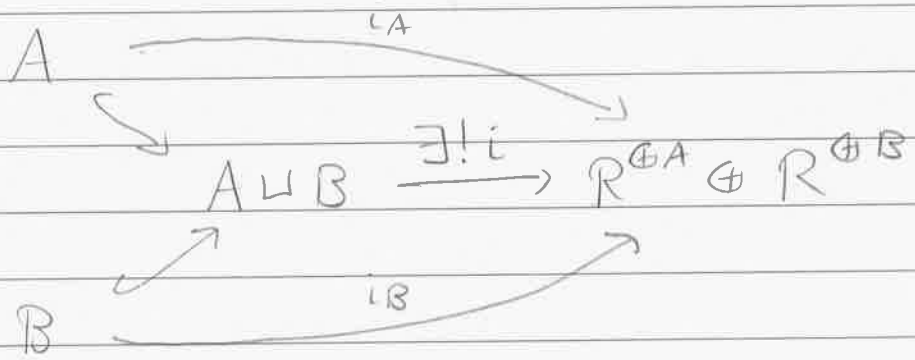


Then in retrospect we can say that $f_A = f|_A$ and $f_B = f|_B$ are the restrictions of the function f to A & B.

Now observe that we have canonical functions

$$i_A : A \longrightarrow R^{\oplus A} \longrightarrow R^{\oplus A} \oplus R^{\oplus B}$$
$$i_B : B \longrightarrow R^{\oplus B} \longrightarrow R^{\oplus A} \oplus R^{\oplus B}$$

coming from the free module and direct sum constructions. Thus by the universal property of $A \sqcup B$ we have

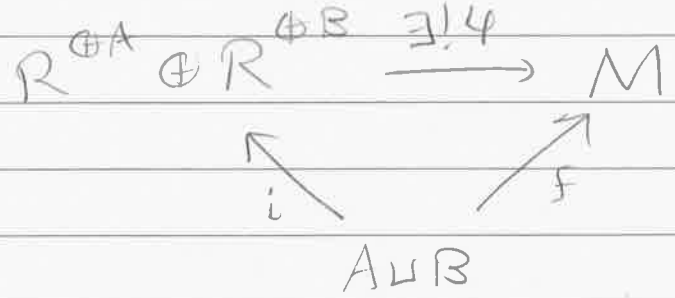


Now I claim that the function

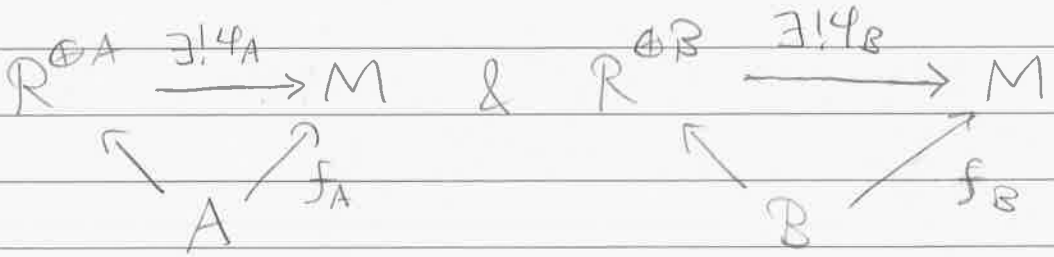
$$i : A \sqcup B \longrightarrow R^{\oplus A} \oplus R^{\oplus B}$$

satisfies the universal property of the free R-module over the set $A \sqcup B$.

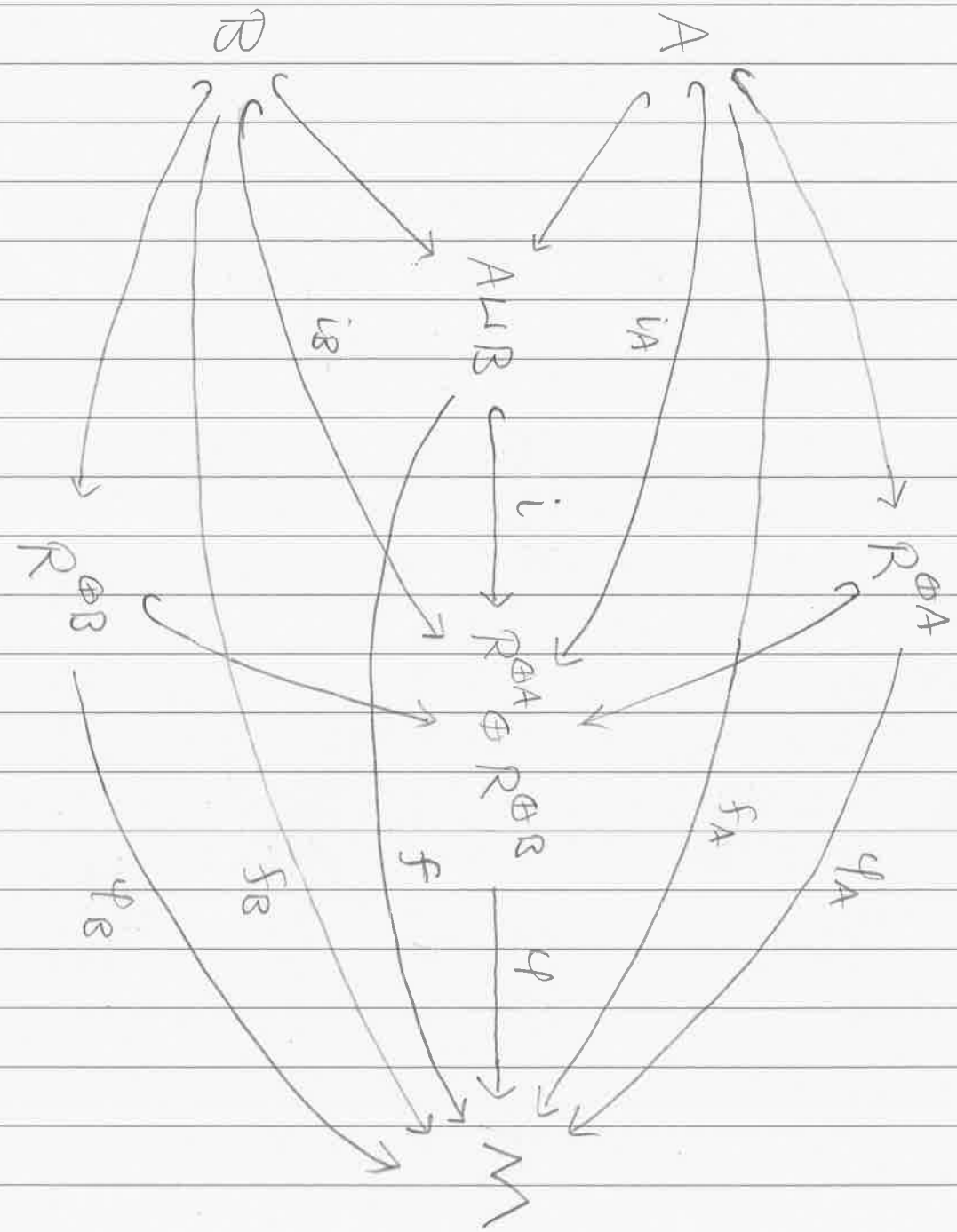
In other words, I claim the following:
Let M be any R-module. Then for any set function $f: A \sqcup B \to M$ there exists a unique R-module homomorphism φ such that



To prove this, consider the restrictions of f to A & B. Then by the universal properties of the free modules $R^{\oplus A}$ & $R^{\oplus B}$ there exist unique R-module homomorphisms φ_A & φ_B such that



Finally, the universal property of coproducts gives a unique R-module homomorphism $\varphi: R^{\oplus A} \oplus R^{\oplus B} \to M$ such that the following diagram commutes ↓



QED.

BEHOLD!

[in the spirit of Aryabhata]

Oh my God, what have we done ?!
Maybe I could have given a shorter and less correct proof but I wanted to point your attention to the following general situation.

Given an R-module M Let $|M|$ denote its underlying set. Then the universal property of free modules can be stated as

$$\mathrm{Hom}_{Set}(A, |M|) = \mathrm{Hom}_{R\text{-}Mod}(R^{\oplus A}, M)$$

[A set function $A \to |M|$ is equivalent to an R-module homomorphism $R^{\oplus A} \to M$.]

In other words the "free functor" $A \longmapsto R^{\oplus A}$ and the "forgetful functor" $M \longmapsto |M|$ form an adjoint pair

$$Set \underset{\text{forget}}{\overset{\text{free}}{\rightleftarrows}} R\text{-mod}.$$

where "free" is the "left adjoint"
"forget" is the "right adjoint".

Now we can apply a powerful meta-theorem.

☆ Meta-Theorem:

- right adjoints commute with limits
- left adjoints commute with colimits. ///

Since the free functor $A \longmapsto R^{\oplus A}$ is left adjoint and since the coproducts $\sqcup, \oplus$ are examples of colimits [see HW2.1] we automatically obtain

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

[Based on our proof of this fact, you can imagine what the proof of the meta-theorem must look like. Would it make a good homework problem? :)]

Modules over a PID to be continued...

2/25/16

SCHEDULE CHANGE:

HW2 is due next Thurs Mar 3.

Midterm Exam is on Tues Mar 15 (after the spring break).

Right now we are proving a structure theorem for modules over a domain.

Recall what we did so far:

If M is a module over an integral domain R then the set of torsion elements

$$\mathrm{Tor}_R(M) := \{ m \in M : \exists r \in R \setminus \{0\}, rm = 0 \}$$

is actually a submodule of M, and the quotient $M/\mathrm{Tor}_R(M)$ is torsion-free (i.e. has no nonzero torsion elements).

In the general case we can't say much more, but in the special case that R is a PID and M is finitely generated, we will have the following extra properties:

↓

- $M/\mathrm{Tor}_R(M)$ is a free module

- The canonical surjection $M \to M/\mathrm{Tor}_R(M)$ splits so that

$$M \approx (M/\mathrm{Tor}_R(M)) \oplus \mathrm{Tor}_R(M)$$

"free part" "torsion part".

This is an important theorem so I want to give a full proof. The proof is a bit involved but it is edifying :)

Lemma 1: Let R be any ring and Let A & B be any sets. Then we have

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

I gave an explicit proof last time, but this also follows from a general principle. The free functor $A \longmapsto R^{\oplus A}$ is left adjoint (to the forgetful functor from R-Mod to Set) so it commutes with colimits. Since the coproducts $\sqcup$ in Set and $\oplus$ in R-Mod are examples of colimits, the result follows.

[Remark: Left adjoint functors do not necessarily commute with limits. For example, we will see later that

$$R^{\oplus(A\times B)} \cong R^{\oplus A} \otimes_R R^{\oplus B},$$

where $\times$ is the (Cartesian) product in Set and $\otimes_R$ is a thing that is not the product in R-Mod.]

Lemma 2: Let A be any set and let $\varphi : M \twoheadrightarrow R^{\oplus A}$ be any surjective R-module homomorphism. Then the short exact sequence

$$0 \longrightarrow \ker\varphi \hookrightarrow M \underset{\varphi}{\overset{\exists}{\rightleftarrows}} R^{\oplus A} \longrightarrow 0$$

splits and we obtain a direct sum

$$M \cong R^{\oplus A} \oplus \ker\varphi.$$

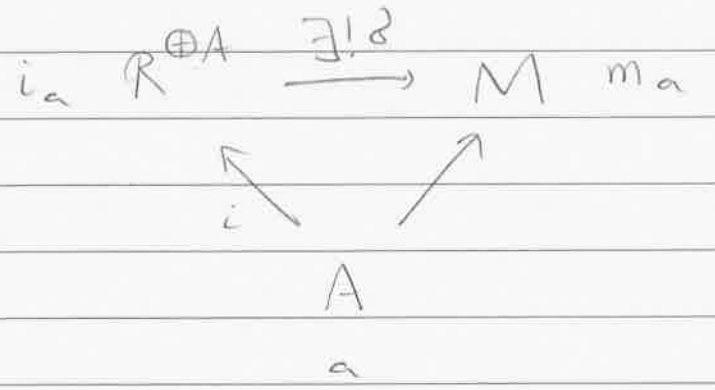
Proof: We will construct a section, i.e. an R-module homomorphism

$\delta : R^{\oplus A} \to M$ such that $\varphi \circ \delta = id_{R^{\oplus A}}$.

Since φ is surjective we can choose for each element $a \in A$ a preimage $m_a \in M$ of the basis element $i_a \in R^{\oplus A}$:

$$\varphi(m_a) = i_a.$$

[This requires the axiom of choice if A is infinite.] Now consider the set function $A \to M$ defined by $a \mapsto m_a$. Since $R^{\oplus A}$ is free there exists a unique R-module homomorphism $R^{\oplus A} \to M$ (let's call it δ) such that



Note that for all $a \in A$ we have

$$\varphi \circ \delta(i_a) = \varphi(\delta(i_a)) = \varphi(m_a) = i_a.$$

Then since $\varphi \circ \delta : R^{\oplus A} \to R^{\oplus A}$ acts like the identity on a basis, it is the identity. We conclude that δ is a section of φ.

Why does this give us a direct sum

$$M \cong R^{\oplus A} \oplus \ker \varphi \quad ?$$

Well, we already know this holds for abelian groups [MTH 761 HW 3.5] but I'll prove it again to show that it works for R-modules.

The section $\delta : R^{\oplus A} \to M$ is injective since for all $r_1, r_2 \in R^{\oplus A}$ we have

$$\delta(r_1) = \delta(r_2)$$
$$\varphi(\delta(r_1)) = \varphi(\delta(r_2))$$
$$r_1 = r_2 \quad \checkmark$$

Now we will show that M is an internal direct sum $M = \delta(R^{\oplus A}) \oplus \ker \varphi$.

- $M = \delta(R^{\oplus A}) + \ker \varphi$?

Pick any $m \in M$. We want to find $n \in \ker \varphi$ and $\delta(r) \in \delta(R^{\oplus A})$ such that

$$m = \delta(r) + n$$
$$\varphi(m) = \varphi(\delta(r) + n)$$
$$\varphi(m) = \varphi(\delta(r)) + \varphi(n)$$
$$\varphi(m) = r + 0.$$

So we will choose $r := \varphi(m)$ and $n := m - \delta(r)$. Then we check that $n \in \ker \varphi$ since

$$\begin{aligned}\varphi(n) &= \varphi(m - \delta(r)) \\ &= \varphi(m) - \varphi(\delta(r)) \\ &= r - r \\ &= 0 \end{aligned}$$ ✓

- $\delta(R^{\oplus A}) \cap \ker \varphi = 0$?

Pick any element $m \in \delta(R^{\oplus A}) \cap \ker \varphi$. Since $m \in \delta(R^{\oplus A})$ there exists

$$\sum_a r_a i_a \in R^{\oplus A} \quad \text{such that}$$

$$m = \delta\left(\sum_a r_a i_a\right) = \sum_a r_a \delta(i_a).$$

Then since $m \in \ker \varphi$ we have

$$0 = \varphi(m) = \varphi\left(\sum_a r_a \delta(i_a)\right)$$

$$= \sum_a r_a \varphi(\delta(i_a)) = \sum_a r_a i_a$$

and it follows that

$$m = \delta\left(\sum_a r_a i_a\right) = \delta(0) = 0. \quad \checkmark$$

Finally, since δ is injective we have

$$M = \delta(R^{\oplus A}) \oplus \ker \varphi \approx R^{\oplus A} \oplus \ker \varphi.$$

//

Remark: Just as with Lemma 1, this massive proof can also be shrunk into a general principle.

★ Definition: Let $\mathcal{C}$ be an abelian category. An object $P \in \mathcal{C}$ is called projective if every short exact sequence

$$0 \to A \to B \to P \to 0 \quad \text{splits}.$$

Then we can rephrase the lemma.

Lemma 2: Every free module is projective.

OK fine. Lemmas 1 & 2 are very general facts about free modules that hold over any ring. Here is the very specific fact about PIDs that makes the structure theorem work.

☆ Key Lemma About PIDs:

Let R be a PID and consider a free module $R^{\oplus A}$ of rank $|A|$. Then any submodule $M \subseteq R^{\oplus A}$ is free of rank $\leq |A|$.

Proof (induction on rank):

If $|A| = 1$ then $R^{\oplus A} = R$. Then since R is a PID, every submodule (i.e. ideal) $M \subseteq R$ is free (i.e. principal), $M = (r)$. If $r = 0$ then M has rank 0 and if $r \neq 0$ then M has rank 1.

If $|A| = n$ then $R^{\oplus A} = R^{\oplus n}$. Consider the surjective homomorphism

$$\pi : R^{\oplus n} \longrightarrow\!\!\!\!\rightarrow R^{\oplus n-1}$$

defined by $\pi(r_1, \cdots, r_n) := \pi(r_1, \cdots, r_{n-1})$. Note that $\ker \pi \approx R$. Now let $M \subseteq R^{\oplus n}$ be any submodule and consider the restricted homomorphism

$$\varphi := \pi|_M : M \longrightarrow R^{\oplus n-1}$$

By induction, the image $\varphi(M) \subseteq R^{\oplus n-1}$ is free of rank $\leq n-1$. Then by Lemma 2, the surjective homomorphism

$$\varphi : M \longrightarrow\!\!\!\!\rightarrow \underset{\text{free}}{\varphi(M)}$$

splits to give $M \approx \varphi(M) \oplus \ker \varphi$. Then since

$$\ker \varphi = \ker(\pi|_M) \subseteq \ker \pi = R$$

we see that $\ker \varphi$ is free of rank ≤ 1.

$\wr$

Putting these together gives

$$M \cong \varphi(M) \oplus \ker \varphi,$$

where $\varphi(M)$ is free of rank $\leq n-1$ and $\ker \varphi$ is free of rank ≤ 1. Finally, we use Lemma 1 [direct sum of free modules is free with basis given by the disjoint union of bases] to conclude that M is free of rank $\leq (n-1)+1 = n$.

QED.

[Remark: Maybe this holds also for free modules of infinite rank and our induction can be made transfinite; I don't really care.]

3/1/16

HW 2 due Thurs
[see correction to Problem 3]
Review session Thurs.
Midterm Exam Tues Mar 15 in class.

Modules over a PID continued...

Recall what we have so far.

Lemma 1: Direct sum of free modules is free,

$$R^{\oplus A} \oplus R^{\oplus B} \cong R^{\oplus (A \amalg B)}.$$

Lemma 2: Free modules are projective. That is, every short exact sequence of the form

$$0 \to M \to N \to R^{\oplus A} \to 0 \quad \text{splits}.$$

Lemmas 1 & 2 are true over any ring.
We used them to prove the following key property for modules over a PID.

✡ Key Lemma for PIDs:

Let R be a PID. Then any submodule of the free module $R^{\oplus A}$ is free of rank $\leq |A|$

///

Also recall the following.

If R is a domain and M is an R-module then the set of torsion elements

$$\mathrm{Tor}_R(M) = \{ m \in M : \exists r \in R \setminus \{0\}, rm = 0 \}$$

is a submodule and the quotient module $M/\mathrm{Tor}_R(M)$ is torsion free. Now we can prove Part I of the Fundamental Theorem of Finitely Generated Modules over a PID.

✡ FTFGMPID, Part I:

Let R be a PID and let M be a finitely generated R-module. Then we can express M as a direct sum of a free module & a torsion module.

In particular, if $\mathrm{Tor}_R(M) \subseteq M$ is the submodule of torsion elements then we have

- $M/\mathrm{Tor}_R(M)$ is free, and
- $M \approx (M/\mathrm{Tor}_R(M)) \oplus \mathrm{Tor}_R(M)$.

Proof: To show that $M/\mathrm{Tor}_R(M)$ is free we will actually prove the more general result that any finitely generated torsion-free R-module is free.

So let F be a torsion-free R-module with finite spanning set $S \to F$. We will write $F = (S)$ to denote that S spans F. Now let $I \subseteq S$ be a maximal linearly independent subset so that $(I) \approx R^{\oplus I}$ is a free module.

For each $t \in S \setminus I$, I claim that there exists some $0 \neq r_t \in R$ such that $r_t f_t \in (I)$. Indeed, since the set $I \cup \{t\}$ is not linearly independent (by maximality of I) we must have some nontrivial linear relation

$$r_t f_t + \sum_{i \in I} r_i f_i = 0.$$

Since I is independent we must have $r_t \neq 0$. Thus we obtain $0 \neq r_t \in R$ with

$$r_t f_t = -\sum_{i \in I} r_i f_i \in (I)$$

as desired. Now consider the product

$$r := \prod_{t \in S \setminus I} r_t \in R,$$

which exists because S is finite and is nonzero because R is a domain.

Now I claim that

$$rF = r(S) \subseteq (I).$$

Indeed, given an arbitrary element

$$f = \sum_{s \in S} r_s f_s \in (S) = F$$

we have $rf_s \in (I)$ when $s \in I \subseteq S$ (obviously) and when $s = t \in S \setminus I$ we can use commutativity of R to write

$r = r' r_t$ for some $r' \in R$, so that

$$r f_s = r f_t = r' r_t f_t \in (I).$$

By linearity we obtain

$$rf = r\left(\sum_{s \in S} r_s f_s\right) = \sum_{s \in S} r_s r f_s \in (I).$$

as desired.

Now since $rF = r(S) \subseteq (I)$ and since $(I) \approx R^{\oplus I}$ is free, the Key Lemma on PIDs tells us that rF is free.

Finally, since F is torsion free and since $r \neq 0$, the R-module homomorphism

$$\begin{aligned} F &\xrightarrow{r\cdot} F \\ f &\longmapsto rf \end{aligned}$$

has trivial kernel, so the 1st Isomorphism Theorem implies that

$$F = F/\ker(r\cdot) \approx \mathrm{im}(r\cdot) = rF.$$

We conclude that F is free. ///

In summary, we have shown that if M is a f.g. module over a PID then

$M/\mathrm{Tor}_R(M)$ is a free module.

Then it follows from Lemma 2 that the short exact sequence

$$0 \longrightarrow \mathrm{Tor}_R(M) \longrightarrow M \longrightarrow M/\mathrm{Tor}_R(M) \longrightarrow 0$$

splits, so we obtain an isomorphism

$$M \cong (M/\mathrm{Tor}_R(M)) \oplus \mathrm{Tor}_R(M).$$

QED.

In what sense is the decomposition in the theorem unique?

Suppose that M has rank k and let $S = R \setminus \{0\}$. Using the fact that the "extension functor" $M \longmapsto S^{-1}M$ is left adjoint to the "restriction functor" $S^{-1}M \longmapsto M$ (details omitted)

tells us that the direct sum (a colimit) is preserved under localization:

$$S^{-1}M \cong S^{-1}(M/\mathrm{Tor}_R(M)) \oplus S^{-1}\mathrm{Tor}_R(M).$$

We can also think of this as a direct sum of $S^{-1}R$-modules. Since $S^{-1}R$ is a field (the field of fractions of R), all three modules are free so we must have

$$\mathrm{rank}(S^{-1}M) = \mathrm{rank}(S^{-1}(M/\mathrm{Tor}_R(M))) + \mathrm{rank}(S^{-1}\mathrm{Tor}_R(M))$$

by Lemma 1. Finally, we can apply HW2 Problem 4(c) to obtain

$$\begin{aligned} k &= \mathrm{rank}(M) \\ &= \mathrm{rank}(M/\mathrm{Tor}_R(M)) + \mathrm{rank}(\mathrm{Tor}_R(M)) \\ &= \mathrm{rank}(M/\mathrm{Tor}_R(M)). \end{aligned}$$

Since $M/\mathrm{Tor}_R(M)$ is free this implies

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

///

★ In summary,

Let M be a f.g. module of rank k over a PID R. Then we have

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

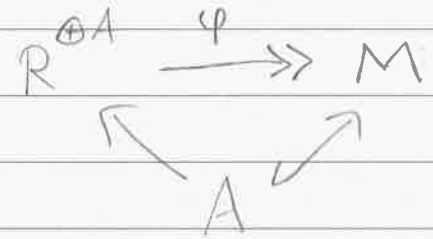
==

After the break we'll prove the FTFGMPID, Part II, which states that the torsion module $\mathrm{Tor}_R(M)$ is a direct sum of cyclic modules.

[Recall the fundamental theorem of finite abelian groups.]

To do this correctly we will first transform the problem into matrix algebra as follows.

Let M be a f.g. module over a PID R. By definition (of "finitely generated") we have a surjective homomorphism from a free module:



We can also express the surjectivity φ by saying that the following sequence is exact:

$$R^{\oplus A} \xrightarrow{\varphi} M \longrightarrow 0.$$

Now consider the kernel $\ker\varphi \subseteq R^{\oplus A}$. By the Key Lemma for PIDs we know that $\ker\varphi$ is free of rank $\leq |A|$, let's say $\ker\varphi \cong R^{\oplus B}$ for some $|B| \leq |A|$. Putting everything together gives a short exact sequence

$$0 \longrightarrow R^{\oplus B} \xrightarrow{\psi} R^{\oplus A} \xrightarrow{\varphi} M \longrightarrow 0$$

where $R^{\oplus B} \cong \operatorname{im}\psi = \ker\varphi \subseteq R^{\oplus A}$.

Note that the map φ was uniquely determined by the inclusion $A \hookrightarrow M$ so the structure of the module is really encoded by the map ψ.

Furthermore, since

$$R^{\oplus B} \xrightarrow{\psi} R^{\oplus A}$$

is a map of free modules we can encode it as an $|A| \times |B|$ matrix after choosing bases for $R^{\oplus A}$ & $R^{\oplus B}$.

The game is to choose bases so that the matrix $[\psi]$ is as nice as possible and then to read off the structure of the module from the matrix.

After the break I'll give you an algorithm to express any matrix $[\psi]$ over a PID in a standard form called the

Smith Normal Form.

The algorithm will be a generalization of the Euclidean Algorithm.