4/29/16

HW 4 due now.
Final Exam next Wed May 4,
11:00-1:30 in this room (Ungar 411).

Today: Review for Final.

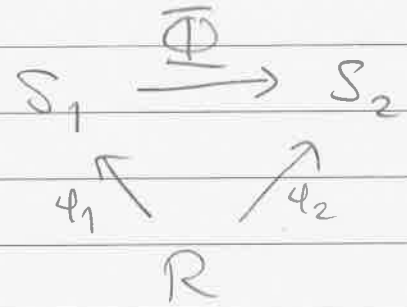
The Final Exam will cover the material discussed in lecture since the Midterm, as well as the material from HW 3 & HW 4. Here are the main topics.

(1) The Category R-Alg.

Let R be a commutative ring. We define an R-algebra as a pair (S, φ) where

- S is a (possibly noncommutative) ring.
- $\varphi : R \to S$ is a ring homomorphism
- im $\varphi \subseteq Z(S) = \{ s \in S : st = ts \ \forall t \in S \}$

We define a morphism of R-algebras $\underline{\Phi} : (S_1, \varphi_1) \to (S_2, \varphi_2)$ as a ring homomorphism $\underline{\Phi} : S_1 \to S_2$ such that the following triangle commutes:



One can check that this defines a category, which we call R-Alg. Note that we have a forgetful functor

$$U : R\text{-Alg} \longrightarrow R\text{-Mod}$$

defined by "forgetting the monoid structure". Specifically, if $\varphi : R \to S$ is an R-algebra then we obtain a ring homomorphism

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

by sending $r \in R$ to the "multiplication map" $\lambda_r(s) := \varphi(r)s = s\varphi(r)$. One can check that this defines an R-module structure on the abelian group $|S|$. [In fact, you did check this on HW 2.5(b).] With respect to this structure we can define a subring

$$\mathrm{End}_R(|S|) \subseteq \mathrm{End}_{Ab}(|S|),$$

and then observe ("trivially" but not necessarily "easily") that the ring homomorphism λ sends R into the center of this subring:

$$\lambda : R \twoheadrightarrow \operatorname{im}\lambda \subseteq Z(\operatorname{End}_R(|S|)).$$

[We did this in class on 4/7/16].

Thus we obtain an R-algebra structure on the ring $\operatorname{End}_R(|S|)$ that is compatible with the R-algebra structure on the ring S in the sense that for all $s_1, s_2, s_3 \in S$ and $r \in R$ we have

- $s_1(s_2 + \lambda_r(s_3)) = s_1 s_2 + \lambda_r(s_1 s_3)$
- $(s_1 + \lambda_r(s_2))\, s_3 = s_1 s_3 + \lambda_r(s_2 s_3)$.

[We say that the monoid structure on S is "R-bilinear".].

[Remark: The forgetful functor $U: R\text{-Alg} \to R\text{-Mod}$ has a left-adjoint free functor $T: R\text{-Mod} \to R\text{-Alg}$ called the "tensor algebra" $M \mapsto T(M)$.

↓

Unfortunately, we didn't have time to get into this.]

///

More generally, if M is any R-module defined by a ring homomorphism

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

then since R is commutative we automatically ("tautologically") obtain an R-algebra of R-linear endomorphisms

$$\lambda : R \twoheadrightarrow \mathrm{im}\,\lambda \subseteq Z(\mathrm{End}_R(M)).$$

In this sense, endomorphisms of R-modules are the "concrete" prototype for R-algebras, and thus tell us how we should define "representations" of algebras.

This also motivates the following, more "concrete", definition of R-algebras.

☆ Concrete Definition:

Let R be a commutative ring. An R-algebra is a structure $(M, \lambda, \circ, id)$ where

- (M, λ) is an R-module
- $(M, \circ, id)$ is a monoid structure making M into a ring (i.e. $\circ$ distributes over addition in M)
- The operation $\circ : M \times M \to M$ is compatible with λ (i.e. it is R-bilinear).

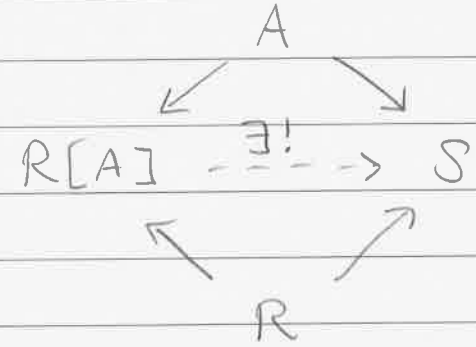
[Any book on representation theory expects you to know this, but no algebra text that I know of actually teaches this.]

---

② The category R-CAlg.

If we restrict our attention to R-algebras $\varphi : R \to S$ in which S is a commutative ring then we obtain a full subcategory $R\text{-CAlg} \subseteq R\text{-Alg}$, called the category of commutative R-algebras. This was the subject of HW3.

Recall that for any set $A \in \mathrm{Set}$ there exists a free commutative algebra $A \to R[A]$ satisfying the universal property



[There are too many maps here to give them names, so we'll have to be careful!]

If $|A| = n$ then we can identify $R[A]$ with the polynomial algebra in n commuting variables, called

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

[Formally we can view this as the "symmetric algebra" $S(R^{\oplus A})$ of the free module $R^{\oplus A}$. This $S: R\text{-Mod} \to R\text{-CAlg}$ is the left adjoint to the forgetful functor $U: R\text{-CAlg} \to R\text{-Mod}$. If $F: \mathrm{Set} \to R\text{-Mod}$ is the free module functor then we obtain

$$R[A] = S(F(A)).$$

↓

Unfortunately, we didn't have time to get into this.]

Now suppose that $A = \{s_1, s_2, \cdots, s_n\} \xrightarrow{i} S$.
Then we obtain the canonical "evaluation morphism" from the free algebra

$$\varphi_A : R[x_1, \cdots, x_n] \longrightarrow S$$
$$f(x_1, \cdots, x_n) \longmapsto f(s_1, \cdots, s_n).$$

We say that

- $A \hookrightarrow S$ is R-algebraically independent if φ_A is injective
- $A \hookrightarrow S$ is R-algebraically generating if φ_A is surjective.

We also sometimes use the notation

$$R[A] = \operatorname{im} \varphi_A \subseteq S$$

but be warned: this notation conflicts with the previous usage because $\operatorname{im} \varphi_A$ is a free algebra only when $\ker \varphi_A = 0$. We'll try not to get confused.

Furthermore, we say that

- $A \hookrightarrow S$ is R-algebraically almost-generating if S is algebraic over the subring $R[A] = \operatorname{im}\varphi_A$. [This means that for all $s \in S$ the evaluation morphism $\varphi_s : R[A][x] \to S$ is non-injective.]

- $A \hookrightarrow S$ is an R-transcendence basis if it is algebraically independent and almost-generating.

★ Steinitz Exchange for Algebras:

Let $S \in R\text{-CAlg}$ be an integral domain, let $A \subseteq S$ be algebraically independent and let $B \subseteq S$ be almost-generating. Then we can replace elements of B by elements of A while maintaining the almost-generating property. It follows that

$$|A| \leq |B|$$

and hence all R-transcendence bases have the same cardinality, called the R-transcendence degree of S. ///

No, you do not need to memorize the proof of this theorem, but you should understand the proof [in the HW3 solutions] and be able to reproduce bits and pieces of it.

Here are the Key Lemmas.

Lemma 1: If $K_1 \subseteq K_2 \subseteq K_3$ are fields then

$$[K_3 : K_1] = [K_3 : K_2][K_2 : K_1].$$

Lemma 2: Let $K \subseteq L$ be fields.

- If $[L:K] < \infty$ then $K \subseteq L$ is algebraic.
- If $K \subseteq L$ is algebraic and finitely generated as a K-algebra then $[L:K] < \infty$.

Lemma 3: Let $K \subseteq L$ be fields. Then the algebraic closure $K \subseteq Alg_K(L) \subseteq L$ is a subring of L (in fact a subfield).

Lemma 4: Let $K_1 \subseteq K_2 \subseteq K_3$ be fields. If $Alg_{K_1}(K_2) = K_2$ and $Alg_{K_2}(K_3) = K_3$, then $Alg_{K_1}(K_3) = K_3$.

Lemma 5 : Lemmas 3 & 4 also hold for integral domains by the trick of

"localization".

[This whole story generalizes to situations where R is an integral domain but S need not be (see "Noether Normalization"). However, the proofs and statements become more difficult.].

---

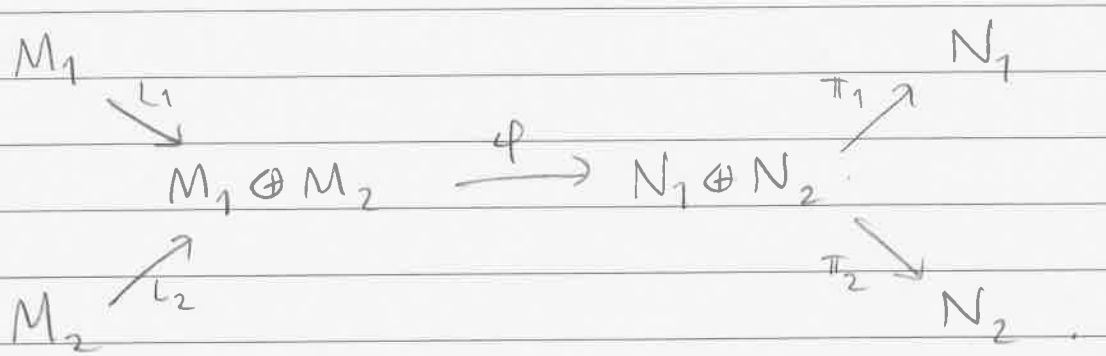
(3) Matrix Notation.

Recall that finite products and coproducts coincide in the category R-Mod (more generally, in any "additive category"). We denote this "biproduct" by $\oplus$.

Now consider any homomorphism between direct sums of modules

$$\varphi : M_1 \oplus M_2 \longrightarrow N_1 \oplus N_2 .$$

By interpreting $N_1 \oplus N_2$ as a product and $M_1 \oplus M_2$ as a coproduct we obtain a diagram:



By the universal properties of product & coproduct, the map φ is uniquely determined by its four "components"

$$\varphi_{ij} := \pi_i \circ \varphi \circ \iota_j : M_j \longrightarrow N_i .$$

Furthermore, we can express φ in terms of the following matrix notation. Given elements $m = m_1 + m_2 \in M_1 \oplus M_2$ and $n = n_1 + n_2 \in N_1 \oplus N_2$ we will write

$$m = \begin{pmatrix} m_1 \\ m_2 \end{pmatrix} \quad \& \quad n = \begin{pmatrix} n_1 \\ n_2 \end{pmatrix}$$

and then we have

$$\varphi(m) = \begin{pmatrix} \varphi_{11} & \varphi_{12} \\ \varphi_{21} & \varphi_{22} \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \end{pmatrix} = \begin{pmatrix} \varphi_{11}(m_1) + \varphi_{12}(m_2) \\ \varphi_{21}(m_2) + \varphi_{22}(m_2) \end{pmatrix}.$$

Now suppose we have a homomorphism between free modules

$$\varphi : R^{\oplus A} \longrightarrow R^{\oplus B}.$$

If the bases are $A = \{a_1, \cdots, a_m\}$ and $B = \{b_1, \cdots, b_n\}$ then we can write this as

$$\varphi : \bigoplus_{j=1}^{m} (a_j) \longrightarrow \bigoplus_{i=1}^{n} (b_i)$$

and we can define the component morphisms

$$\varphi_{ij} := \pi_i \circ \varphi \circ \iota_j : (a_j) \longrightarrow (b_i).$$

If we denote an element $r = \sum_j r_j a_j \in R^{\oplus A}$ as a column vector

$$r = \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_m \end{pmatrix}$$

then by iterating the construction above we can express φ in matrix notation as follows:

$$\varphi(r) = \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1m} \\ \vdots & & \\ \varphi_{n1} & \cdots & \varphi_{nm} \end{pmatrix} \begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} = \begin{pmatrix} \sum_j \varphi_{1j}(r_j) \\ \vdots \\ \sum_j \varphi_{nj}(r_j) \end{pmatrix}.$$

Since each component $\varphi_{ij} : (a_j) \to (b_i)$ is a homomorphism of rank 1 free modules it is uniquely determined by the ring element $s_{ij} \in R$ such that

$$\varphi_{ij}(a_j) = s_{ij} b_i .$$

Thus it is more meaningful to write

$$\varphi = \begin{pmatrix} s_{11} & \cdots & s_{1m} \\ \vdots & & \vdots \\ s_{n1} & \cdots & s_{nm} \end{pmatrix}.$$

By composing homomorphisms between free modules we recover the familiar definition of matrix multiplication. In summary, if F_1, F_2 are finitely generated free R-modules then any choice of bases

$$F_1 = R^{\oplus A} \quad \& \quad F_2 = R^{\oplus B}$$

$\{$

determines an isomorphism of abelian groups

$$\Phi_{AB} : \mathrm{Hom}_R(F_1, F_2) \xrightarrow{\sim} \mathrm{Mat}_{|B|\times|A|}(R)$$

an isomorphism of rings

$$\Phi_A : \mathrm{End}_R(F_1) \xrightarrow{\sim} \mathrm{Mat}_{|A|}(R)$$

and an isomorphism of groups

$$\Phi_A : \mathrm{Aut}_R(F_1) \xrightarrow{\sim} GL_{|A|}(R).$$

[If, moreover, R is commutative then the first is an isomorphism of R-modules & the second is an isomorphism of R-algebras.]

The great benefit of matrix notation is that we can use Gaussian elimination to obtain constructive proofs and a more concrete understanding of modules (at least over nice rings).

Specifically, we define the elementary matrices $E_{ij}(r), E_{ii}(r), P_{ij} \in GL_n(R)$. If R is a Euclidean domain then these generate the group $GL_n(R)$.

If R is, more generally, a PID then we also need the pseudo-elementary matrices:

$$E_{ij}\begin{pmatrix} a & b \\ c & d \end{pmatrix} := I + (a-1)e_{ii} + b\,e_{ij} + c\,e_{ji} + (d-1)e_{jj}.$$

Now we can describe the action of the group $GL_m(R) \times GL_n(R)$ on the set $Mat_{m\times n}(R)$ by left and right multiplication

$$(P, Q) \cdot A := PAQ^{-1}$$

in terms of algorithms involving elementary (and pseudo-elementary) row and column operations. This leads to the following theorem.

★ Smith Normal Form:

Let R be a PID and consider a matrix $A \in Mat_{m\times n}(R)$. Then there exist invertible matrices

$$P \in GL_m(R) \quad \& \quad Q \in GL_n(R)$$

and ideals $(r_d) \subseteq \cdots \subseteq (r_2) \subseteq (r_1) \subseteq R$ such that

$$PAQ^{-1} = \left(\begin{array}{ccc|c} r_1 & & & \\ & r_2 & & \\ & & \ddots & \\ & & & r_d \\ \hline & 0 & & 0 \end{array}\right)$$

Furthermore, the matrices P, Q and elements $r_1 | r_2 | \cdots | r_d$ are unique up to multiplication by units. We call PAQ^{-1} the Smith Normal Form of A. //

(4) FTFGMPID, Part II.

This allows us to completely determine the structure of finitely generated modules over a PID. Let R be a PID and let $M \in R\text{-Mod}$ be finitely generated. Then by results from before the Spring Break we obtain a short exact sequence

$$0 \to R^{\oplus m} \xrightarrow{\varphi} R^{\oplus n} \to M \to 0,$$

so that $M \cong R^{\oplus n} / \operatorname{im}\varphi$.

By the Smith Normal Form, we can choose bases $A \subseteq R^{\oplus m}$ & $B \subseteq R^{\oplus n}$ so that

$$[\varphi]_{AB} = \begin{pmatrix} r_1 & & & \\ & r_2 & & \\ & & \ddots & \\ & & & r_m \\ \hline & & 0 & \end{pmatrix} \Bigg\} n$$

$\underbrace{\qquad\qquad}_{m}$

and then it follows from the argument on HW4 Problem 1 that

$$M \cong \frac{R^{\oplus n}}{\text{im}\,\varphi} \cong R^{\oplus(n-m)} \oplus \bigoplus_{i=1}^{m} \frac{R}{(r_i)}.$$

In other words, M is isomorphic to a direct sum of cyclic modules. The number $n-m$ (called the <u>rank</u>) and the ideals

$$(r_m) \subseteq \cdots \subseteq (r_2) \subseteq (r_1)$$

(called the <u>invariant factors</u>) are isomorphism invariants of the module M.

//

(5) $K[x]$-modules.

The FTFGMPID has an immediate application to abelian groups ($\mathbb{Z}$-modules) but I think the more interesting applications relate to the "other" PID (namely, $K[x]$ where K is a field).

Using the fact that $K[x]$ is the free K-algebra generated by one element gives us a bijection between $K[x]$-modules and pairs (V, φ) where

- V is a K-vector space
- $\varphi \in \mathrm{End}_K(V)$ is a K-linear endomorphism

If V is finite dimensional (say $V = K^{\oplus n}$) then by choosing a basis we can think of φ as an $n \times n$ matrix $A = [\varphi] \in \mathrm{Mat}_n(K)$. Furthermore, two such modules (V_1, A_1) & (V_2, A_2) are isomorphic as $K[x]$-modules if and only if there exists an invertible matrix $P \in GL_n(K)$ such that

$$PA_1P^{-1} = A_2.$$

Finally, since $K[x]$ is a PID we obtain from the FTFGMPID an isomorphism of $K[x]$-modules

$$V \cong \bigoplus_{i=1}^{d} K[x]/(f_i(x))$$

for some unique monic nonconstant polynomials

$$f_1(x) \mid f_2(x) \mid \cdots \mid f_d(x).$$

[Recall: $f_d(x)$ is the minimal polynomial & $\prod f_i(x)$ is the characteristic polynomial of the corresponding morphism.]

By choosing the most obvious bases for the direct summands we can then obtain the Rational Canonical Form and the Jordan Canonical form (when K is algebraically closed) of the corresponding matrix. ///

There is more to say but it's been a Long semester so I think I'll stop here.