6. Modules: introduction

I talked about modules from scratch beginning with a repetition of the definition.

1. definition
2. examples
3. free modules
4. cyclic modules

6.1. definition.

Definition 6.1. A *(left) R-module* is an additive group M together with a ring homomorphism

$$\alpha : R \to \operatorname{End}(M).$$

The statement that α is a ring homomorphism is three statements:

1. $\alpha(1) = 1$
2. $\alpha(r+s) = \alpha(r) + \alpha(s)$
3. $\alpha(rs) = \alpha(r)\alpha(s)$

Writing $\alpha(r)x = rx$ this list becomes:

1. $1x = x$
2. $(r+s)x = rx + sx$
3. $(rs)x = r(s(x))$

6.2. examples.

Example 6.2. A left ideal $I \subset R$ is an R-module.

Example 6.3. The ring itself is a module. I.e., R is an R-module.

Example 6.4. The polynomial ring $R[X]$ is an R-module.

Example 6.5. If R is a field, an R-module is the same as a vector space V over the field R.

Definition 6.6. A *basis* for a vector space V over a field F is a subset $\mathcal{B} = \{b_i\} \subseteq V$ so that for every $v \in V$ there are unique scalars $x_i \in F$ almost all of which are zero so that $v = \sum x_i b_i$.

Theorem 6.7. *Every vector space V over a field K has a basis.*

We will prove this later. In fact, fields are PID's. So, this will be a special case of a more general theorem.

6.3. free modules.

Definition 6.8. An R-module M is *free* if it has a basis $\mathcal{B} = \{b_\alpha\}$. I.e., for every element x of M there are unique elements $r_i \in R$ almost all of which are zero so that

$$x = \sum r_i b_i.$$

Example 6.9. The product $R \times R \times R$ is free on the generators e_1, e_2, e_3.

Theorem 6.10. *Every module is a quotient of a free module.*

Proof. Let F be the free module generated by the set X of all nonzero elements of M. Then the inclusion map $X \to M$ induces an epimorphism $f : F \twoheadrightarrow M$ by the formula:

$$f\left(\sum r_i(x_i)\right) = \sum r_i x_i.$$

Here I used the notation (x_i) to denote the element of X corresponding to the element $x_i \in M$. This implies that M is isomorphic to the quotient:

$$M \cong F/\ker f.$$

□

This proof uses definitions which I was supposed to do earlier:

Definition 6.11. A *submodule* of an R-module M is defined to be an additive subgroup $N \subseteq M$ which is closed under the action of R. Thus:

(1) $0 \in N$
(2) $N + N = N$ (N is closed under addition: $N + N \subseteq N$. But this is equivalent to $N + N = N$ since $0 \in N$.)
(3) $RN = N$ (N is closed under multiplication by elements of R: $RN \subseteq N$. This is equivalent to $RN = N$ since $1 \in R$.)

Proposition 6.12. *If N is a submodule of M then the set of additive cosets:*

$$M/N := \{x + N \mid x \in M\}$$

forms an R-module.

Theorem 6.13. *If $f : M \to L$ is a homomorphism of R-modules then*

(1) $\ker f$ *is a submodule of* M.
(2) $\operatorname{im} f$ *is a submodule of* L.
(3) $\operatorname{im} f \cong M/\ker f$.

I gave an example of a module which is not free:

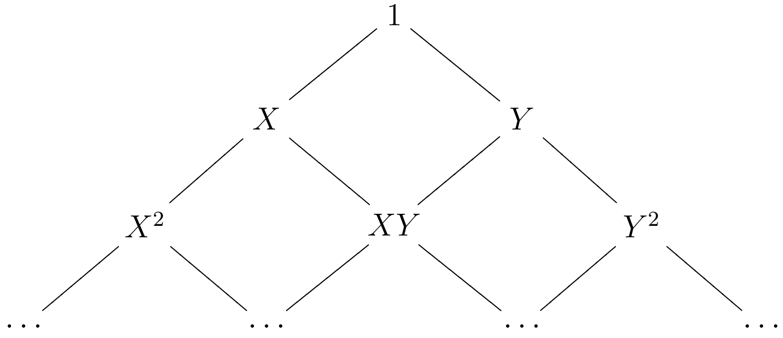
Example 6.14. Let $R = K[X,Y]$. Then the ideal (X,Y) is not a free module. It has generators X, Y but $Y(X) = X(Y)$. Another was to say this is that the epimorphism

$$R \times R \to (X,Y)$$

given by

$$(f,g) \mapsto Xf(X,Y) + Yg(X,Y)$$

is not an isomorphism since $(Y,-X)$ is in the kernel. I also drew a picture:



This is a visualization of a module because each monomial generates a submodule (ideal) and lines indicate containment, just as in a Hasse diagram.

6.4. **cyclic modules.**

Definition 6.15. A *cyclic module* is a module which is generated by one element. Thus $M = Rx$.

The question is: Can we describe all cyclic modules up to isomorphism?

If M is generated by the single element x then there is an epimorphism:

$$\phi : R \to M$$

given by $\phi(r) = rx$. This implies that $M \cong R/\ker\phi$. But what is the kernel of ϕ? It is by definition the set of all $r \in R$ so that $rx = 0$. This is called the *annihilator ideal* of x:

$$ann(x) := \{r \in R \,|\, rx = 0\}.$$

Thus,

$$M = Rx \cong R/ann(x).$$

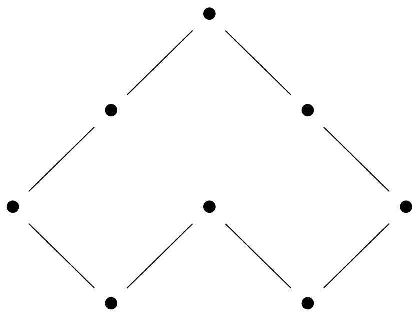
Conversely, given any left ideal $I \subseteq R$, the quotient R/I is a cyclic module. In order to give a complete classification of cyclic modules we still need to answer the following.

Question: Is it possible for two different ideals I, J to give isomorphic cyclic modules

$$R/I \cong R/J?$$

If so, we need to describe all the ideals J which give the same quotient up to isomorphism.

Cyclic modules can be visualized as a diagram with one peak:



For example, this could be $K[X,Y]/(X^3, X^2Y^2, Y^3)$. A finitely generated module could be visualized as a union of overlapping pictures of this kind.

[If someone can create the picture, I will insert it here.]