CLASS 8, FEBRUARY 22TH: GENERATION & CAYLEY-HAMILTON

As with groups, we have a notion of generators and relations upon which we can devise the structure of any given module. We can show this directly using some of the isomorphism theorems for modules:

Proposition 8.1. *Every module M can be described by a set of generators m_α and some corresponding relations:*

$$M = \langle m_\alpha \rangle = \left\{ \sum_\alpha r_\alpha m_\alpha \mid r_\alpha \in R, \text{ all but finitely many } = 0 \right\} / \{\textit{Relations in } M\}$$

Proof. Consider the free module $R^{\oplus M}$, which has as elements

$$\{(r_m)_{m \in M} \mid r_m \in R, \text{ all but finitely many } = 0\}$$

Then there exists a natural surjection

$$\varphi : R^{\oplus M} \to M : (r_m) \to r_m \cdot m$$

It is surjective because $\varphi(1_m) = m$. In fact, by the first isomorphism theorem, we have

$$R^{\oplus M} / \ker(\varphi) \cong \mathrm{im}(\varphi) = M.$$

So $\ker(\varphi)$ is exactly the set of relations in the module M. This completes the proof. □

In practice, this is very overkill for describing the module M. Usually the number of generators is much smaller than the size of M itself :)

Example 8.2. $\mathbb{Q}$ has the natural structure of a $\mathbb{Z}$-module. It has generators $\frac{1}{n}$ for $n \in \mathbb{N}$. However, there are relationships, like

$$5 \cdot \frac{1}{10} = \frac{1}{2}$$

So again, some (most?) of the generators are superfluous.

Definition 8.3. Let Λ be a set. R is **$|\Lambda|$-generated** if there exists a surjection $R^\Lambda \to M$. If Λ can be made finite, we say M is **finitely-generated**.

Most modules of interest are finitely generated. This is because, much like in the case of linear algebra, finitely generated modules (finite dimensional vector spaces) behave much more reasonably than infinitely generated ones (infinite dimensional VSs).

Example 8.4. We can consider the ring $R = \mathbb{F}_p[x]$, and consider the Frobenius map $F : R \to R : f \mapsto f^p$. This is a ring homomorphism, which makes R into an R module with the funny structure $x \cdot y = F(x)y = x^p y$. To avoid confusion, call this module $F_* R$.

It is a simple check that $F_* R$ is a finitely-generated free module, with exactly p-generators: $1, x, \ldots, x^{p-1}$. This can be seen as follows: if $f = \sum_{i=0}^n c_i x^i$, then we can rewrite this as

$$f = \sum_{m=0}^{\lfloor n/p \rfloor} \sum_{l=0}^{p-1} c_{mp+l} x^{mp+l} = \sum_{l=0}^{p-1} \left(\sum_{m=0}^{\lfloor n/p \rfloor} c_{mp+l} x^m \right) \cdot x^l =$$

This phenomenon is the basis of a great deal of (my own) research.

Now, for the rest of class I would like to build up a beautiful result, known as the determinant trick, which will provide the building blocks to prove Nakayama's Lemma next class.

Theorem 8.5 (The Determinant Trick)**.** *Suppose M is an n-generated R-module, and $\varphi : M \to M$ is an R-linear map. If there exists an ideal I with $\varphi(M) \subseteq IM$, then there is a (monic!) polynomial*

$$p(x) = x^n + a_1 x^{n-1} + \ldots + a_n \in R[x]$$

with $a_i \in I^i$ for each i and such that $p(\varphi) = 0$ as an operator on M.

I recommend comparing this with the Cayley-Hamilton Theorem from linear algebra:

Theorem 8.6 (Cayley-Hamilton)**.** *If M is a $n \times n$ matrix with entries in a field K, then*

$$p(x) = \det(x \cdot I_n - M)$$

is a polynomial of degree n such that $p(M) = 0$ as an operator on K^n.

The determinant trick not only upgrades this theorem to allow K an arbitrary ring, but also the free module can be ANY module! Note that if we allow $I = R$ in the Determinant Trick, then Cayley-Hamilton is returned.

Proof. Given that $M = \langle m_1, \ldots, m_n \rangle$, and $\varphi(m) \in IM$ for every $m \in M$, we have

$$\varphi(m_i) = \sum_{j=1}^{n} r_{ij} m_j$$

where $r_{ij} \in I$. Therefore, we can write $\sum_{j=1}^{n} \varphi \circ \delta_{i,j} - r_{ij}$ applied to m_i is 0, where $\delta_{i,j}$ is the Dirac delta function: $\delta_{i,j} = 1$ if $i = j$ and is 0 otherwise.

Therefore, we can form an $n \times n$ matrix Λ where the (i,j)-entry is exactly $\varphi \circ \delta_{i,j} - r_{ij}$. This matrix multiplies the vector $m = (m_1, \ldots, m_n)^T$ to zero by design.

Definition 8.7. The **adjugate** of an $n \times n$ matrix M has its (i,j)-entry as $(-1)^{i+j}$ times the determinant of the matrix M with the j^{th} row and i^{th} column omitted.

If we multiply $Adj(\Lambda) \cdot \Lambda$, we get $\det(\Lambda) Id$. Therefore, this has a wonderful property that the inverse of a matrix Λ is given by $\frac{1}{\det(\Lambda)} Adj(\Lambda)$ (if it exists). However, in our case this shows that

$$\det(\Lambda) Id \cdot m = Adj(\Lambda) \cdot \Lambda \cdot m = Adj(\Lambda) \cdot 0 = 0$$

Therefore, since m_i are generators, either $M = 0$ (and we are done) or $m_i \neq 0$ and we get $\det(M) = 0$. But $\det(M)$ is a degree n polynomial in φ. This proves the claim. $\square$