Week 6

???

6.1 Module Tools

2/6:

- A fifth week summary has been posted.
  - Week 5 content is not in the midterm syllabus.
    - In particular, Gauss's Lemma is not on the midterm.
  - Lecture 5.3 won't even be on the final syllabus.
  - The techniques are applicable to a variety of problems, though, so it is good to know them.
- Today: Modules.
  - We depart from commutative rings and return to simple rings with identity to start.
- Notation: What kinds of sets different letters denote.
  - A, B: Rings.
  - R: Commutative ring.
  - F, K: Fields.
  - D: Division ring.
- Linear algebra is the study of division rings but only over fields.
- Definition of a **division ring**.
  - The only ideals of a division ring are $0, D$, just like with fields.
  - Linear independence, spanning, basis, etc. all hold in a general division ring; you only need fields for things like JCF.
- **Left *A*-module**: An abelian group $(M, +)$ equipped with a binary operation $\cdot : A \times M \to M$ defined by $(a, m) \mapsto am$ (or $a \cdot m$ in the case of potential ambiguity) satisfying the following. *Constraints*

  For all $a, b \in A$ and $v, v_1, v_2 \in M$...

  (1) $a(v_1 + v_2) = av_1 + av_2$;
  (2) $(a + b)v = av + bv$;
  (3) $a(bv) = (ab)v$;
  (4) $1_A v = v$.
- We need the last one so that multiplication is nontrivial.
- A **right *A*-module** puts the scalar on the right. Will we ever consider these??

- Notation: For all $a \in A$, define the function $\rho(a) : M \to M$ by $\rho(a)v = av$ for all $v \in M$. *Constraints*
  (1) $\rho(a)$ is a group homomorphism from $M \to M$.
  (2) $\rho(a+b) = \rho(a) + \rho(b)$.
  (3) $\rho(a)\rho(b) = \rho(ab)$.
  (4) $\rho(1_A) = 1_{\text{End}(M)}$
- Conditions 2-4 imply that $\rho : A \to \text{End}(M)$ is a ring homomorphism.
  - Recall HW1 Q1.14, which led up to the result that

    $$\text{End}(M) = \{f : M \to M \mid f \text{ is a group homomorphism}\}$$

    is a ring with identity under componentwise addition and composition (i.e., $g \cdot f = g \circ f$).
- Going forward, in-class definitions will always match those in the book.
  - It's been this way for a while??
- Examples.
  1. Let $M = A$. Then $\rho(a)b = ab$ for all $a \in A$, $b \in M = A$.
  2. If M_i ($i \in I$ an indexing set) is a (left) A-module, then the product $\prod_{i \in I} M_i$ is also an A-module.
  3. Denote an element of $\prod_{i \in I} M_i$ by $\prod_{i \in I} m_i$. An arbitrary choice of $m_i \in M_i$ for all $i \in I$ is allowed (do we need the Axiom of Choice??). We define $\cdot$ by

     $$a\left(\prod_{i \in I} m_i\right) = \prod_{i \in I}(am_i)$$

  4. The collection

     $$\oplus_{i \in I} M_i = \left\{\prod_{i \in I} m_i \mid \{i \in I : m_i \neq 0\} \text{ is a finite set}\right\}$$

     is an A-module.
     - This is a submodule of something??
     - Under the same binary operation as Example 3??
  5. In particular, A^m is an A-module with $a(b_1, \dots, b_n) = (ab_1, \dots, ab_n)$.
- **Submodule**: A subgroup $(N, +)$ of $(M, +)$ such that for all $a \in A$ and $\omega \in N$, $a\omega \in N$.
- Observation: If N_1, N_2 are submodules of M, then $N_1 + N_2$ and $N_1 \cap N_2$ are submodules.
- Question (base case): What are the submodules of A, itself?
  - Left ideals.
- **Module homomorphism**: A function $T : M \to N$ such that T is a homomorphism of abelian groups and commutes with scalar multiplication (i.e., $T(av) = aT(v)$ for all $a \in A$, $v \in M$). In full, we have

  $$T(a_1v_1 + a_2v_2) = a_1T(v_1) + a_2T(v_2)$$

  for all $a_1, a_2 \in A$ and $v_1, v_2 \in M$.
- Question: What are all of the module homomorphisms $T : A \to M$?
  - If $T(1) = v$, then $T(a \cdot 1) = aT(1) = av$ for all $a \in A$.
  - For all $v \in M$, there exists a unique $T : A \to M$ such that $T(1) = v$. This is more linear algebra.

- Question: What are all linear transformations $T : A^n \to M$?
  - Suppose $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, 0, \ldots, 0)$, etc. Then
  $$(a_1, \ldots, a_n) = \sum_{i=1}^{n} a_i e_i$$
  - Therefore,
  $$T(a_1, \ldots, a_n) = \sum_{i=1}^{n} a_i T e_i$$
  - Take any ordered n-tuple of elements in M; then given $v_1, \ldots, v_n \in M$, there is a unique A-module homomorphism $T : A^n \to M$ such that $T(e_i) = v_i$ $(i = 1, \ldots, n)$.
- **Isomorphism** (of A-modules): A bijective module homomorphism $T : M \to N$, where M, N are A-modules.
- It follows that $T^{-1} : N \to M$ is also a homomorphism.
- Proposition: Let N be a submodule of M. Then the quotient group M/N has a unique structure of an A-module such that $\pi : M \to M/N$ (defined with groups) is an A-module homomorphism.

  Proof.

  Existence: For all $a \in A$, we have that $\rho(a) : M \to M$ take $\rho(a)N \subset N$. It induces $\overline{\rho(a)} : M/N \to M/N$. Take $\overline{\rho(a)}$, which is scalar multiplication by a on M/N. ☐

- FIT: Let $\phi : M \to N$ be a module homomorphism. Then $\ker(\phi)$ is a submodule M and $\operatorname{im}(\phi)$ is a submodule of N.

$$\begin{tikzcd}
M \arrow[r, "\phi"] \arrow[d, "\pi"'] & N \\
M/\ker(\phi) \arrow[r, "\bar{\phi}"'] & \operatorname{im}(\phi) \arrow[u, "i"']
\end{tikzcd}$$

Figure 6.1: First isomorphism theorem of modules.

- Example: $A = \mathbb{Z}$ and $M = \mathbb{Z}/(27)$.
- Theorem: Let R be a PID. Then every R-submodule of R^n is isomorphic to R^m for some $0 \leq m \leq n$.
- Think in terms of fields! If Nori had been couching all of this in terms of vector spaces, we would all get all of this immediately.
- Let $n = 1$, $(2) \subsetneq \mathbb{Z}$. Then $m = n$ does not imply $M = R^n$.
- Submodules of R are ideals. Thus, in a PID, they're principal ideals.

  Proof. Case 1 (base case): Let $n = 1$. We know that $M = (b)$ for some $b \in R$. If $b = 0$, then we're done. Thus, assume $b \neq 0$. Then $T : R \to (b)$ given by $T(a) = ab$ for all $a \in A$. It follows that T is onto. From the fact that R is an integral domain, we have that T is 1-1.

  Case 2 (general case): We induct on n. Suppose that $i : R^{n-1} \hookrightarrow R^n$ is given by
  $$i(a_1, \ldots, a_{n-1}) = (a_1, \ldots, a_{n-1}, 0)$$

Let M be a submodule of R^n. Then $R^{n-1} \times \{0\} \hookrightarrow R^n$ and $M \cap (R^{n-1} \times \{0\}) \cong R^\ell$ for $0 \leq \ell \leq n-1$. Suppose that you define the ideal $\pi(a_1, \ldots, a_n) = a_n$. Let $\pi(M) = I$. Then you have some ideal I. It follows that $\pi : M \to I \subset R$. Let $M' = \ker \phi$. $M/M' \cong I$. At this point, there are only two cases ($a = 0$ and $a = M$). $\square$

- Next time: We will wrap up this proof with the following proposition.
- Proposition: If M' is a submodule of M and $M/M' \cong R$ as an R-module, then $M \cong M' \oplus R$.