

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 $\cdot : A \times M \rightarrow M$ 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 $v, v_1, v_2 \in M \dots$
 - (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 $\rho(a) : M \rightarrow M$ by $\rho(a)v = av$ for all $v \in M$. *Constraints*

(1) $\rho(a)$ is a group homomorphism from $M \rightarrow M$.

(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 $\rho : A \rightarrow \text{End}(M)$ is a ring homomorphism.

– Recall HW1 Q1.14, which led up to the result that

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

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 $T : M \rightarrow N$ 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 $T : A \rightarrow M$?

– 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 $T : A \rightarrow M$ such that $T(1) = v$. This is more linear algebra.

- Question: What are all linear transformations $T : A^n \rightarrow M$?

– Suppose $e_1 = (1, 0, \dots, 0)$, $e_2 = (0, 1, 0, \dots, 0)$, etc. Then

$$(a_1, \dots, a_n) = \sum_{i=1}^n a_i e_i$$

– Therefore,

$$T(a_1, \dots, a_n) = \sum_{i=1}^n a_i T e_i$$

– Take any ordered n -tuple of elements in M ; then given $v_1, \dots, v_n \in M$, there is a unique A -module homomorphism $T : A^n \rightarrow M$ such that $T(e_i) = v_i$ ($i = 1, \dots, n$).

- **Isomorphism** (of A -modules): A bijective module homomorphism $T : M \rightarrow N$, where M, N are A -modules.

- It follows that $T^{-1} : N \rightarrow M$ 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 $\pi : M \rightarrow M/N$ (defined with groups) is an A -module homomorphism.

Proof.

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

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

$$\begin{array}{ccc} M & \xrightarrow{\phi} & N \\ \pi \downarrow & & \uparrow i \\ M/\ker(\phi) & \xrightarrow{\bar{\phi}} & \text{im}(\phi) \end{array}$$

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 $T : R \rightarrow (b)$ 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

$$i(a_1, \dots, a_{n-1}) = (a_1, \dots, a_{n-1}, 0)$$

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 $\pi(a_1, \dots, a_n) = a_n$. Let $\pi(M) = I$. Then you have some ideal I . It follows that $\pi : M \rightarrow I \subset R$. 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 $M \cong M' \oplus R$.

6.2 Office Hours (Nori)

- Is the final cumulative? Will we ever be responsible for the Week 5 material?
 - Stuff from Week 5 and this lecture may show up in terms of thought processes you need to go through again, but the exact stuff won't show up. And certainly not on Wednesday's midterm.
 - The midterm will test who is thinking correctly and who can write proper proofs; there will only be one proof problem, most likely.
 - Several T/F questions.
 - If $R[X]$ is a UFD, prove that R is a UFD.
 - The two Lecture 5.2 methods are important to know (e.g., for the final).
- Review questions email?
 - Looking at the *fourth week summary* and the problems in there will help you prepare for your midterm.
 - That may be too strong a statement, but it might be nice.
 - The gcd of two elements in a PID is just found by looking for a generator. Study this!! Nori wants to put a problem on it.
- Lecture 3.1: What is \bar{X} in a quotient ring with a degree 1 or 0 polynomial divisors?
 - It is an abrupt and jumpy transition from degree 1 to 0.
 - For degree $n = 0$, we have a natural homomorphism from $\mathbb{Z}/2\mathbb{Z}[X]$ to $\mathbb{Z}[X]/(2)$.
 - For degree $n \geq 2$ in the ideal, we have a new polynomial that's solvable.
 - For degree $n = 1$, we get dyadics or something like that.
 - What about $(2X)$? It's kind of in between the $n = 1$ and $n = 0$ cases. We have an injection

$$\mathbb{Z}[X]/(2X) \hookrightarrow \mathbb{Z}[X]/(2) \times \mathbb{Z}[X]/(X) \cong \mathbb{F}_2[X] \times \mathbb{Z}$$
 - We also have a ring homomorphism from $\mathbb{F}_2[X] \times \mathbb{Z} \rightarrow \mathbb{F}_2 \times \mathbb{F}_2$ defined by evaluation in the first slot and then $f(0)$ in the next.
 - But $(\mathbb{F}_2[X] \times \mathbb{Z})/(\mathbb{Z}[X]/(2X)) \cong \mathbb{F}_2$. This conjugacy only happens as groups, though.
 - To get down to one element, you can prove that $\mathbb{Z}[X]/(2X) \cong \Delta^{-1}(\mathbb{F}_2)$ where Δ is the diagonal.
- Lecture 4.1: Showing $r \in I$ in this way would not be acceptable in the HW?
 - Probably a misstatement.
- Lecture 4.2: Incomplete statement on what's all important to prove that something is a UFD.
 - It's all important to prove that irreducibles are prime. This is equivalent to R being a UFD.
- Lecture 4.2: The whole essay thing and the greatest common divisors being well-defined.

- This is just talking about the algorithm for finding the gcd via factorization.
- Section 8.3: Using the Axiom of Choice in the construction of the infinite chain?
 - Nori never gives much thought to such matters lol.
 - You’re doing something infinitely many times, but via induction so countably so. Thus, use a countable Axiom of Choice. So it is an Axiom of Choice, but a limited one, too.
- Lecture 5.1: Conversely statement.
 - Statement (*) provides a “factorization.” But for us to know that it actually is a *factorization*, we need to know that each $\pi \in \mathcal{P}(R)$ is, in fact, irreducible. We do that as follows.
 - Suppose that $\pi = ab$ is a factorization of an irreducible element. By statement (*), write $a = u\pi_1^{m_0}\pi_1^{m_1}\cdots\pi_h^{m_h}$ and $b = v\pi_1^{n_0}\pi_1^{n_1}\cdots\pi_h^{n_h}$. It follows that

$$\pi^1\pi_1^0\cdots\pi_h^0 = \pi = ab = \pi^{m_0+n_0}\pi_1^{m_1+n_1}\cdots\pi_h^{m_h+n_h}$$

Thus, $m_i + n_i = 0$ ($i = 1, \dots, h$), so $m_i, n_i = 0$ for these i . Additionally, $m_0 + n_0 = 1$, so WLOG let $m_0 = 1$. Then $n_0 = 0$ and b is a unit. Therefore, π is irreducible.
- Lecture 5.2: Why do we assume that $a_n \neq 0$?
- Lecture 5.2: Clarification on the end of Method 1.
 - See Week 5 notes.
 - Key takeaway: You want to get a bound; it doesn’t matter if it’s the best possible bound, but a bound on the coefficients of a monic polynomial implies a bound on the roots.
- Lecture 5.2: What is going on at the end of Method 2?
- Lecture 5.2: What was the thing about reducing polynomials modulo primes?
- Lecture 6.1: Will we ever consider right A -modules?
 - No — and going forward, **A-module** means “left A -module.”
- Lecture 6.1: How long have in-class definitions matched those in the book?
 - Practically any book has a different definition of EDs. The book has the weakest definition (i.e., that with the Dedekind-Hasse norm). This definition is basically used nowhere, though.
 - The **class group** is a measure of the failure of unique factorizations. This is an example of something that’s actually useful.
 - Rings, ring homomorphisms, etc. But basically stopped in second week.
 - We need the $\phi(1) = 1$ property for instance because otherwise the image of 1 might not act like 1 in the product.
- Lecture 6.1: Axiom of Choice needed to pick an element out of each set?
- Lecture 6.1: What is the direct product a submodule of?
- Lecture 6.1: Is the submodule under the same binary operation as Example?
 - The direct sum is a submodule of the product.