

Week 7

???

7.1 Zorn's Lemma and Intro to Modules Over PIDs

2/13:

- Picking up from last time with Zorn's lemma.
- **Partially ordered set:** A set together with a binary relation indicating that, for certain pairs of elements in the set, one of the elements precedes the other in the ordering. *Also known as poset. Denoted by P .*
 - The domain of the **partial order** may be a proper subset of $P \times P$.
- **Partial order:** The binary relation on a poset.
- **Maximal** ($f \in P$): An element $f \in P$ such that for all $q \in P$, the statement $q > f$ is false.
- Example.
 - Let X be a set with $|X| \geq 2$ ^[1].
 - Define a poset $P = \{A \subsetneq X\}$ with corresponding partial order defined by taking subsets. In particular, if $A \subset B$, write $A \leq B$.
 - For any $x \in X$, $X - \{x\}$ is a maximal element of P .
- **Chain:** A subset of a poset P such that if c_1, c_2 are in said subset, then implies $c_1 \leq c_2$ or $c_2 \leq c_1$. *Denoted by C .*
 - In other words, a chain is a subset of a poset that is a **totally ordered set**.
- **Totally ordered set:** A set together with a binary relation indicating that, for any pair of elements in the set, one of the elements precedes the other in the ordering.
- Observation: If F is a subset of a nonempty finite chain C , then there exists $c \in F$ such that $c \geq q$ for all $q \in F$.
- **Upper bound** (of C): An element $p \in P$ such that $p \geq c$ for all $c \in C$.
- **Zorn's lemma:** Let P be a poset that satisfies
 - (i) $P \neq \emptyset$;
 - (ii) Every chain $C \subset P$ has an upper bound.

Then P has a maximal element.

¹Nori denotes cardinality by $\#X$.

- We will not prove Zorn's lemma. It rarely if ever gets proven in an undergraduate course, maybe in a logic course.
 - And by “prove” we mean “deduce Zorn's lemma from the Axiom of Choice.”
- We now investigate a situation in which Zorn's lemma gets applied.
- Let M be a finitely generated A -module.
 - Let $v_1, \dots, v_r \in M$ be elements such that $M = Av_1 + \dots + Av_r$.
 - Before we prove the proposition that requires Zorn's lemma, we will need one more definition: that of a **maximal submodule**.
- **Maximal submodule** (of M): A submodule of M that is a maximal element of the poset

$$P = \{N \subsetneq M : N \text{ is an } A\text{-submodule}\}$$

- Proposition: Every nonzero finitely generated A -module M has a maximal submodule.

Proof. To prove that M has a maximal submodule, it will suffice show that there exists a maximal element of the poset

$$P = \{N \subsetneq M : N \text{ is an } A\text{-submodule}\}$$

To do this, Zorn's lemma tells us that it will suffice to confirm that $P \neq \emptyset$ and that every chain $C \subset P$ has an upper bound. Let's begin.

We first confirm that $P \neq \emptyset$. By hypothesis, M is nonzero. Thus, the zero A -submodule is a proper subset of M , so $0 \in P$ and hence P is nonempty.

We now confirm that every chain $C \subset P$ has an upper bound. Let $C \subset P$ be an arbitrary chain. Define

$$\mathcal{N}_C = \bigcup \{N : N \in C\}$$

We will first verify that $\mathcal{N}_C \in P$, and then we will show that \mathcal{N}_C is an upper bound of C . Let's begin. To verify that $\mathcal{N}_C \in P$, it will suffice to demonstrate that \mathcal{N}_C is an A -submodule of M and that $\mathcal{N}_C \subsetneq M$.

To demonstrate that \mathcal{N}_C is an A -submodule, Proposition 10.1 tells us that it will suffice to show that $\mathcal{N}_C \neq \emptyset$ and $n_1 + an_2 \in \mathcal{N}_C$ for all $a \in A$ and $n_1, n_2 \in \mathcal{N}_C$. Since P is nonempty, \mathcal{N}_C is nonempty by definition, as desired. Additionally, let $n_1, n_2 \in \mathcal{N}_C$ be arbitrary. It follows by the definition of \mathcal{N}_C that there exist $N_1, N_2 \in C$ such that $n_i \in N_i$ ($i = 1, 2$). WLOG, assume $N_1 \subset N_2$. Then $n_1, n_2 \in N_2$. It follows since N_2 is an A -submodule that $n_1 + an_2 \in N_2 \subset \mathcal{N}_C$ for all $a \in A$, as desired.

We know that $\mathcal{N}_C \subset M$. Thus, if $\mathcal{N}_C \subsetneq M$, then we must have $\mathcal{N}_C = M$. Suppose for the sake of contradiction that $\mathcal{N}_C = M$. Recall that $M = Av_1 + \dots + Av_r$. Since the v_i are elements of M and $\mathcal{N}_C = M$, it follows that $v_i \in \mathcal{N}_C$ ($i = 1, \dots, r$). Thus, as before, there must exist $N_1, \dots, N_r \in C$, not necessarily distinct, such that $v_i \in N_i$ ($i = 1, \dots, r$). It follows by the observation from earlier that there is an $i \in [r]$ such that for all $j \in [r]$, $N_j \subset N_i$. Consequently, $v_j \in N_j \subset N_i$ ($j = 1, \dots, r$). But N_i is an A -submodule, so $M = Av_1 + \dots + Av_r \subset N_i \subset M$. But this means that $N_i = M$, contradicting the assumption that $N_i \subsetneq P$ (since $N_i \in P$). Therefore, $\mathcal{N}_C \subsetneq M$, as desired.

It follows that $\mathcal{N}_C \in P$, as desired. Lastly, we have by its definition that $N \subset \mathcal{N}_C$ for all $N \in C$, meaning that \mathcal{N}_C is an upper bound of C by definition. Therefore, by Zorn's lemma, P has a maximal element, and hence M has a maximal submodule, as desired. \square

- Corollary: Every nonzero commutative ring R has a maximal ideal.

Proof. Consider R as an R -module. Then $R = (1)$ is finitely generated. This combined with the fact that it is nonzero by hypothesis allows us to invoke the above proposition, learning that R has a maximal submodule N . But by the observation from Lecture 6.1, N is a left ideal, which is equivalent to a two-sided ideal in a commutative ring. Maximality transfers over as well (as we can confirm), proving that N is the desired maximal ideal of R . \square

- Remark: Suppose that J is a two-sided ideal of A . Let M be an A -module such that for all $a \in J$ and $m \in M$, we have $am = 0$. Then M may be regarded as an (A/J) -module in a natural manner.
 - In particular, we may take $\rho : A \rightarrow \text{End}(M, +)$ to be a ring homomorphism.
 - We can factor $\rho = \bar{\rho} \circ \pi$, where $\pi : A \rightarrow A/J$ and $\bar{\rho} : A/J \rightarrow \text{End}(M, +)$. It follows that $\bar{\rho}$ is a ring homomorphism. Therefore, M is an A/J -module.
 - This remark will be used!
 - Review annihilators from Section 10.1!
- Remark: Given a left ideal $I \subset A$ and an A -module M , we get a whole lot of modules because each element of M generates one. In particular, we note that $Im \subset Am \subset M$, where both Im, Am are submodules for all $m \in M$.

- **Product** (of modules): The A -submodule of M defined as follows. Denoted by IM . Given by

$$IM = \sum_{m \in M} Im$$

- It follows that M/IM is an A -module, but also one with a special property: $a(M/IM) = 0$ for all $a \in I$.
 - If A is commutative, then M/IM is an A/I -module.
- Proposition: Let R be a nonzero commutative ring. If $R^m \cong R^n$ as R -modules, then $m = n$.

Proof. Let $I \subset R$ be a maximal ideal. (We know that one exists by the above corollary.) If $f : R^m \rightarrow R^n$ is an isomorphism of R -modules, then f restricts to $I(R^m) \rightarrow I(R^n)$. This gives rise to the isomorphism $\bar{f} : R^m/I(R^m) \rightarrow R^n/I(R^n)$ of R -modules, in fact of R/I modules. It follows that R/I is a field, so $m = n$. \square

- Classifying modules up to isomorphism under commutative rings.
 - This is a hard problem, and there are still many open problems in this field today.
 - We will not go into this, though.
- We now move on to modules over PIDs.
 - Nori will go *much* slower than the book.
 - Do you have any recommended resources??
 - Do we need to read and understand Chapters 10-11 to start on Chapter 12??
- Objective: Let R be a PID. Classify all finitely generated R -modules up to isomorphism.
 - Our first result in this field was that submodules of R^n are equal to R^m for $m \leq n$.
 - Where this is applicable: \mathbb{Z} and $F[X]$.
 - Go back and check out \mathbb{Z} -modules and $F[X]$ -modules in Section 10.1!
- **Torsion module:** An R -module M such that for all $m \in M$, there exists $0 \neq a \in R$ such that $am = 0$.
- **Torsion-free module:** An R -module M such that for all nonzero $m \in M$ and for all nonzero $a \in R$, we have $am \neq 0$.
- Theorem: If M is a finitely generated torsion-free R -module, then $M \cong R^n$ for some n .
 - With a little work, we could prove this. But Nori will postpone it.

- **p -primary** (module): An R -module M such that for all $m \in M$, there exists $k \geq 0$ for which $p^k m = 0$, where p is prime in R .
- We want to classify these up to isomorphism.
 - Nori can state these today, but will not have time to prove it until another day.
 - Something that gets annihilated by p is a $\mathbb{Z}/(p)$ -module. The moment you go from $k = 1$ to $k = 2$, things get interesting.
- Examples: $R/(p^{n_1}) \oplus \cdots \oplus R/(p^{n_k})$, where $n_1 \geq \cdots \geq n_k \geq 1$.
 - Note that $k = 0$ is allowed.
- Uniqueness will take some time, but existence can be given as an exercise now.
- M/pM is an $R/(p)$ -vector space. pM/p^2M is an $R/(p)$ -vector space as well. So is $p^k M/p^{k+1}M$.
 - Use d_0, d_1, \dots, d_k to denote the dimensions of the vector spaces.
 - d_0, \dots, d_k is a decreasing sequence of nonnegative integers.

7.2 Office Hours (Nori)

- Homework questions.
 - See pictures + unnumbered lemma.
 - Example of the kernel being bigger than (f) .
 - A ring homomorphism $\mathbb{Z}[X] \rightarrow \mathbb{R}$ must be evaluation by the universal property of polynomial rings.
 - Factoring enables a constraint on a .
- Lecture 6.1: Proposition proof?
- Lecture 6.1: $(2) \subsetneq \mathbb{Z}$ example?
- Lecture 6.1: The end of the theorem proof.
- Lecture 6.2: Does the first theorem you proved not appear in the book until Chapter 12?
- Lecture 6.2: What is A in the proof?
- Resources for the proofs in Week 6?
- Lecture 7.1: Quotient stuff.
- Recommended resources for modules over PIDs? Chapter 12?
 - We should be able to read chapter 12, since chapter 11 is just vector spaces.
 - Nori's doing Chapter 12 in the classical manner (pre-1970). Dummit and Foote (2004) just does it in the first few pages as the **elementary divisor theorem**.
- HW6: So you want us to solve 1, 10, 13 for our own edification, but we don't need to write up a solution? Will we ever be responsible for the content therein?
 - We'll need to understand them to move forward.
 - Q6.4-Q6.5 are particularly important (good for number theory).

7.3 Office Hours (Ray)

- Universal properties save you from having to do pages upon pages of ring homomorphism checks (think Q3.10).
- Algebra: Chapter 0 by Paolo Aluffi for learning quotienting by polynomials.
 - Universal properties show up on page 30.
 - Read stuff before as needed.
 - Has a chapter called universal properties of polynomial rings. Universal properties of quotients, too.
- Direct sums and direct products.
 - Let M, N be R -modules. Then $M \times N$ is an R -module defined by the Cartesian product of the sets and with **diagonal** module action $r(m, n) = (rm, rn)$ (diagonal meaning we just act on two elements).
 - $M \oplus N = M \times N$.
 - For infinite sets, we get a difference. Indeed, $\prod_{i=1}^{\infty} M_i \neq \bigoplus_{i=1}^{\infty} M_i$.