Week 6

Modules Intro

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 $v, v_1, v_2 \in M \dots$

  (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 $\rho(a) : M \to M$ 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) $\rho(1_A) = 1_{\mathrm{End}(M)}$
- Conditions 2-4 imply that $\rho : A \to \mathrm{End}(M)$ is a ring homomorphism.
  - Recall HW1 Q1.14, which led up to the result that
    $$\mathrm{End}(M) = \{f : M \to M \mid f \text{ is a group homomorphism}\}$$
    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 $a(b_1, \dots, b_n) = (ab_1, \dots, ab_n)$.
- ***A*-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 $\mathrm{im}(\phi)$ is a submodule of N.

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

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 $M \cong M' \oplus R$.

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 $F_2[X] \times \mathbb{Z} \to \mathbb{F}_2 \times \mathbb{F}_2$ 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 $a = u\pi^{m_0}\pi_1^{m_1}\cdots\pi_h^{m_h}$ and $b = v\pi^{n_0}\pi_1^{n_1}\cdots\pi_h^{n_h}$. 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.

6.3 Office Hours (Ray)

- Q5.2(i).
  - Do it by hand; $X^4 - 1$ and $X^2 - 1$ is an instructive example.
  - We have that $X^4 - 1 = (X^2 - 1)(X^2 + 1)$.
- Do we need proofs for Q5.4?
  - No.
- What additionally does Q5.1(iii) want us to do?
  - You can include a pointer to the previous part and reiterate your proof.
- Q5.6.
  - Commutative rings of characteristic p: The "raise to the power p" function is a ring homomorphism. This is the **Frobenius map**.

6.4 Midterm Review Sheet

2/8:

- Definitions and alternate definitions.
- **Ring**: Abelian group, associative multiplication, distributive laws.
- **Subring**: Closed under addition, multiplication, inverses; contains 1_R.
- **Ring homomorphism**: Respects addition, multiplication, identites.
- **Field**: Commutative, multiplicative inverses for every element save 0_R.
  - A commutative division ring.
  - Commutative, $0_F \neq 1_R$, multiplicative inverses.
- **Polynomial ring**: Union of all formal sums of finite length.
- **Power series ring**: $R^{\mathbb{Z}_{\geq 0}}$ under

$$\left(\sum_{n=0}^{\infty} a_n X^n\right) + \left(\sum_{n=0}^{\infty} b_n X^n\right) = \sum_{n=0}^{\infty} (a_n + b_n) X^n$$

$$\left(\sum_{p=0}^{\infty} a_p X^p\right)\left(\sum_{q=0}^{\infty} b_q X^q\right) = \sum_{\substack{p\geq 0,\\ q\geq 0}} a_p b_q X^{p+q} = \sum_{r=0}^{\infty}\left(\sum_{p=0}^{r} a_p b_{r-p}\right) X^r$$

- **Division ring**: Multiplicative inverses only.
- **Trivial ring**: Multiplication is the zero function.
- **Zero ring**: The ring $R = \{0\}$.
- **Zero divisor**: A nonzero element $a \in R$ to which there corresponds a nonzero element $b \in R$ such that either $ab = 0$ or $ba = 0$.
- **Unit**: An element $u \in R$ to which there corresponds some $v \in R$ such that $uv = 1$.
- **Integral domain**: Commutative, no zero divisors.
  - Commutative, $0_R \neq 1_R$, $a \neq 0$ and $ab = 0$ implies $b = 0$.

  - Commutative, $0_R \neq 1_R$, $a, b \neq 0$ implies $ab \neq 0$.
- **Gaussian integers**: $\mathbb{Z}[i]$.
- **Ideal**: A subset I of a ring R for which $(I, +) \leq (R, +)$ and aI, Ia, or both are subsets of I.
  - Left, right, and two-sided variations.
- **Quotient ring**: The set of all additive cosets.
- **Canonical injection**: ι.
- **Canonical surjection**: i.
- **Isomorphism** (of rings): $f \circ g$ and $g \circ f$ definition formally.
  - Bijectivity isn't always enough.
- **Principal ideal**: An ideal with a single generator.
- **Sum** (of ideals): $\{a + b : a \in I,\ b \in J\}$.
- **Product** (of ideals): $\{a_1 b_1 + \cdots + a_n b_n : n \in \mathbb{N},\ a_1, \dots, a_n \in I,\ b_1, \dots, b_n \in J\}$.
- **Characteristic** (of R): The unique $d \in \mathbb{Z}_{\geq 0}$ such that $\ker(j) = \mathbb{Z}d$, where $j : \mathbb{Z} \to R$ is the homomorphism defined by $m \mapsto m_R$.
- **Generated** (ideal): The ideal consisting of all R-multiples of some set of elements in R.
- **Maximal** (ideal): $M \subsetneq R$, no ideal S satisfies $M \subsetneq S \subsetneq R$.
- **Prime** (ideal): $P \subsetneq R$ (for R commutative), $a, b \in R$ and $ab \in P$ implies $a \in P$ or $b \in P$.
- **ED**: Integral domain, has a (positive) norm [induces a division algorithm].
- **Reducible** (element): Nonzero, $a = bc$ for some $b, c \notin R^\times$.
- **Irreducible** (element): Nonzero, not a unit, not reducible.
  - Equivalently: $\pi = ab$ implies a or b is in $R^\times$.
- **Factorization**: Product of irreducibles and a unit.
- **Equivalent** (factorizations): Same length, uniqueness up to associates (don't forget the permutation thing!).
- **UFD**: Integral domain, all factorizations of a given element are equivalent.
- **Greatest common divisor**: Divides a, b; all others divide it.
- We now move on to other major/useful results and proof sketches.
- Cancellation law: a, b, c with a not a zero divisor, $ab = ac$, implies $a = 0$ or $b = c$.
- Finite integral domains are fields.
- The property "is a subring of" is transitive.
- Proof that π respects multiplication (review!).
- NIT: The natural extension of the FIT holds.
- The cancellation lemma holds in integral domains.
- Images and kernels are subrings.

- Evaluation is a ring homomorphism.
- $I = R$ iff I contains a unit.
- R is a field iff it's commutative and its only ideals are $0, R$.
- F a field implies any nonzero ring homomorphism into another ring is an injection.
- Every proper ideal is contained in a maximal ideal.
- In commutative rings: M is maximal iff R/M is a field.
- In commutative rings: P is prime iff R/P is an integral domain.
- In commutative rings: I maximal implies I prime.
- EDs, PIDs, and UFDs are all integral domains at their most basic level; then they have additional structures corresponding to their names added on top.
- $R - \{0\} = \bigsqcup\{\text{units}, \text{reducibles}, \text{irreducibles}\}$.
- TFAE (in a PID): π irreducible, (π) maximal, π prime.
- $R[X]$ a UFD implies R a UFD.
  - Consider $r \in R$. $r \in R[X]$. Therefore it has a unique factorization. Its factorization must be in terms of degree 0 elements since it's degree 0. Therefore, R is a UFD.
- $\gcd(a, b)$ is a generator of $Ra + Rb$.
  - R is a PID, so $Ra + Rb = Rd$.
  - $a, b \in (d)$ implies $d \mid a, b$.
  - $a, b \in (d')$ implies $d = \alpha a + \beta b \in (d')$, so $d' \mid d$.
- Lastly, a checklist of things from the midterm syllabus.
- All of the material in Chapter 7 excluding...
  1. The CRT in the generality stated there (a less general version may still appear).
     - Essentially, for coprime ideals, the quotient of their product equals the quotient of their intersection is congruent to the product of their quotients.
  2. Group rings.
  3. Monoid rings.
- Special focus on...
  1. Polynomial rings and power series rings.
     - Universal property: R a ring, $\alpha : R \to B$, $x \in B$, x commutes with all $\alpha(a) \Rightarrow$ there exists a unique $\beta : R[X] \to B$ such that $\beta(a) = \alpha(a)$ for all $a \in R$ and $\beta(X) = x$.
       - Like change of coordinates and evaluation.
  2. Rings of fractions *only* for when the ring is an integral domain (no need to go to the more general Chapter 15 version).
     - Characteristics of D: $1_R \in D$, $0_R \notin D$, D contains no zero divisors, D is a multiplicative subset.
     - Universal property: $\iota : R \to D^{-1}R$ is injective, $\varphi : R \to S$ satisfying $\varphi(D) \subset S^\times$ implies a unique $\tilde{\varphi} : D^{-1}R \to S$ such that $\tilde{\varphi} \circ \iota = \varphi$, and φ injective implies $\tilde{\varphi}$ injective.
       - Key step in proof: $\tilde{\varphi}(x/t) = \varphi(x)\varphi(t)^{-1}$.
     - $\operatorname{Frac} R$ is isomorphic to the subfield of F generated by R.

   - $R_f \cong R[X]/(fX-1)$.

- Chapter 8/9 material.
  1. Euclidean algorithm for monic polynomials.
     - Strict less than, uniqueness proof (subtract two possibilities and get constraints), existence (induct and reduce degree).
  2. ED implies PID.
     - Take a smallest element under the norm and call it d. Divide an arbitrary $h \in I$ by d to get $qd + r$. Know that r must have smaller norm and thus be 0. Set $I = (q)$.
  3. PID implies UFD.
     - If every irreducible element of R is prime, then any two factorizations are equivalent.
       - Prove via induction.
       - Start with $r = 0$ which is trivial.
       - Show that $u'\pi_1' \cdots \pi_s' \in (\pi_1)$.
       - It's not u' that's divisible by π_1 (contradiction; proves π_1 is a unit).
       - It must be one of the others (WLOG π_1').
       - Relates $\pi_1 = u_1\pi_1'$. Apply the cancellation lemma to equal factorizations, and then the induction hypothesis. Rigorously extend $\sigma \in S_{r-1}$ in the natural way (function can stay the same).
     - Infinite chain construction.
       - Assume we can keep reducing. Generates an infinite ascending chain of ideals.
       - The infinite union is an ideal; it must have a generator. That generator must belong to an I_n; the process terminates there.
       - Uniqueness: All irreducibles are prime (π irreducible implies (π) maximal via contradiction that π is reducible, $R/(\pi)$ is a field hence integral domain hence (π) prime hence π prime), then invoke Lemma*.
  4. $\gcd(a,b)$ can be computed in a PID without factorizing the given a, b (use the Euclidean Algorithm).
     - $a = q_0b + r_0$, $b = q_1r_0 + r_1$, $r_0 = q_2r_1 + r_2$, $\dots$, $r_{n-1} = q_{n+1}r_n$.
- Wrap my head around an elementary statement of the Chinese Remainder Theorem!
- Stuff from OH on Monday.

6.5 Sub- and Quotient-Module Structure

2/10:
- On the midterm.
  - All of our midterms have been graded but 2.
  - The midterm was bad.
  - Nori is more depressed than we will be when we get ours back.
  - He wants us to understand all of the stuff that was on it.
  - The first two questions were really important.
  - The last two were on gcd's in PIDs, which is really important for Spring Quarter.
  - Nori was pretty severe on those who didn't know the definition of a ring homomorphism. You need $f(1) = 1$. You can't have $f(1) = 0$ because that takes everything to 0. You also need to know that 1_R belongs to subrings.
  - We should have it back on Monday; Wednesday latest.

- On HW5.
  - Q5.2: Proving that $(X^m - 1, X^n - 1)$ in $\mathbb{Z}[X]$ is $(X^d - 1)$ where $d = \gcd(m, n)$.
    - Nori thinks it's nice and hopes we all get it.
    - $\gcd(X - 1, X + 1) = 1$ does not imply that $\gcd(q - 1, q + 1) = 1$ for all $q \in \mathbb{Z}$.
    - Ring homomorphisms do not preserve the gcd.
  - It's all important, though.
- On HW6.
  - It is long and challenging.
  - Assuming that you've never seen modules before Monday, it will take time.
- We now begin lecture in earnest.
- A simplification of the theorem from last time that will lead into it.
- Theorem: Let R be a PID and let $M \subset R^h$ be an R-submodule. Then $M \cong R^m$ for some $0 \leq m \leq h$.

  Proof. Consider the module homomorphism $\varphi : M \to R$ that selects for the last component, i.e., is defined by

  $$\varphi(a_1, \dots, a_h) = a_h$$

  for all $m = (a_1, \dots, a_h) \in M$. We now investigate the image and kernel of φ. These facts may seem disjointed now, but they will be useful later.

  Kernel: Let $M' = \ker(\varphi)$. Then $M' = M \cap (R^{h-1} \times \{0\})$.

  Image: Since M is an R-submodule, it is an additive subgroup and it is closed under multiplication by elements of R. Therefore, it is an ideal of R^h. It follows that $\operatorname{im}(\varphi)$ is an ideal of R (φ would be surjective were it extended to R^h, and then $\varphi(M)$ would be the image of an ideal under a surjective map; see Q2.3b).

  We now divide into two cases ($\operatorname{im}(\varphi) = \{0\}$ and otherwise). Suppose first that $\operatorname{im}(\varphi) = \{0\}$. Then $M' = M$. Now suppose that $\operatorname{im}(\varphi) \neq \{0\}$. By hypothesis, R is a PID. In particular, the ideal $\operatorname{im}(\varphi)$ is principal, i.e., that there exists $0 \neq b \in R$ such that $\operatorname{im}(\varphi) = Rb$. Choose $e \in M$ such that $\varphi(e) = b$ (in other words, take $e \in M$ to have b as its last entry). Define $T : M' \oplus R \to M$ by

  $$T(m', a) = m' + ae$$

  We now prove that T is a module homomorphism[1]. ...

  We now prove that T is an A-module *iso*morphism.

  We first check that T is onto. Pick an element $m \in M$ and suppose that a_h is its last element. By definition, $a_h \in \operatorname{im}(\varphi) = Rb$. Thus, there exists $d \in R$ such that $a_h = db = \varphi(de)$. Thus, $\varphi(m) = \varphi(de)$, so $\varphi(m - de) = 0$, i.e., $m' = m - de \in M'$. It follows that $m = m' + de$, so $m = T(m', d)$, as desired.

  We now check that T is injective. Since R is an integral domain, d is unique. Thus, since distinct inputs map to distinct outputs, T is 1-1. It follows that $\ker(T) = 0$.

  It follows that $M' \oplus R \cong M$.

  The rest of the proof follows by induction on $h \geq 0$. In particular, assume $h > 0$ and assume that we've proved the claim for $h - 1$. Then $M' \cong R^\ell$ for $0 \leq \ell \leq h - 1$. Case 1: $M' = M$ and Case 2: $M \cong M' \oplus R \cong R^\ell \oplus R = R^{\ell+1}$. $\square$

- On sets, $\oplus$ is the same as $\times$.

[1] Nori said A-module homomorphism. What is A??

  - By the definition of module homomorphisms, to give a module homomorphism from $N_1 \oplus N_2 \to M$ is to give one from $N_1 \to M$ and $N_2 \to M$ and add the results.
  - Related to the definition of $T(1)$ and $\varphi(e)$ from the proof.
- Why is the image an ideal?
  - $i : M \hookrightarrow R^n$ is a module homomorphism, and $\text{proj} : R^n \to R$ is a module homomorphism.
  - $I \subset R$ is a submodule, i.e., for all $m \in I$ and $\lambda \in R$, $\lambda m \in I$.
  - Then it's surjection, as discussed in the proof.
- Module homomorphisms are not ring homomorphisms. Modules don't necessarily have a ring structure.
- The collection
$$\{(a_1, \dots, a_{h-1}, 0) : a_i \in R\} \cong R^{h-1}$$
is an R-module.
- We now return to the theorem from last lecture.
- Theorem: Let A be a ring, let M be an A-module, and let $M' \subset M$ be an A-submodule (all modules are left modules). Suppose that there is an isomorphism of A-modules $\varphi : M/M' \to A^n$. Then $M' \oplus A^n \cong M$ as an A-module.

  Proof. You can either do this in one short proof with horrible notation, or you can prove it for $n = 1$ and say that induction solves the rest. We'll do the latter.

  The existence of φ says that there exists a surjection of A-modules $\psi : M \to A$ with $\ker \psi = M'$. "Take $\psi^{-1}(1)$ and set it equal to e. Then repeat the (previous??) proof." Choose $e \in M$ such that $\varphi(e) = 1$. Then $T : M' \oplus A \to M$, $T(m', a) = m' + ae$ for all $m' \in M'$ and $a \in A$. To check that T is onto will proceed symmetrically to in the previous proof. (Let $m \in M$ Put $a = \varphi(m)$. Then $a = \varphi(ae)$. Put $m' = m - ae$. Then $\varphi(m') = \varphi(m - ae) = \varphi(m) - \varphi(ae) = a - a = 0$. (This φ may be ψ!). Therefore, $m' \in M$ and $T(m', a) = m$ is onto.) How about $\ker(T)$? Let $m' \in M'$. We have $(m', a) \in \ker(T)$ implies $m' + ae = 0$. Then $\varphi(m' + ae) = 0$, $\varphi(m') + a = 0$, $m' = 0$. $\square$

- Build up to Zorn's Lemma.
  - If $\varphi : \mathbb{Z}^m \to \mathbb{Z}^n$ is an isomorphism of abelian groups, then $\bar{\varphi} : \mathbb{Z}^m/2\mathbb{Z}^m \to \mathbb{Z}^n/2\mathbb{Z}^n$ is still an isomorphism. Hence, $2^m = 2^n$ and thus $m = n$.
  - Exercise: Suppose V is an infinite dimensional vector space over a field F. Let $A = \text{End}_F(V)$. Then $A^m \cong A^n$ for all $m, n > 0$ where the isomorphism is of A-modules.
  - On the other hand, we can just resolve this issue axiomatically.
    - Let A be a ring. Consider $\text{End}_A(A^2)$. For a field, it's 2×2 matrices. Here,
$$\text{End}_A(A^2) \cong M_2(A^{\text{opp}})$$
where the opp notation denotes that multiplication has been reversed and addition is still the same, i.e.,
$$a \cdot_{\text{new}} b = b \cdot_{\text{old}} a$$
    - Assuming that A is commutative and $A \cong A^2$ as an A-module, this implies that $M_2(A) \cong A$.
    - Zorn's lemma allows us to give a proof that $A^m \cong A^n$ iff $m = n$.
    - We will delay this proof, though, until Cayley's theorem.

6.6 Office Hours (Ray)

- Q5.1(ii).
  - We know that $\varphi(1,1) = (1,1)$. We know $\varphi(x,y) \neq (z,t)$. We know that $\varphi(1,0) = (1,0)$.
  - Then φ is the identity function, which is unique.
  - Necessary: If there is a unique isomorphism, then $a \neq b$.
  - Sufficient: If $a \neq b$, then you can't send identities to identities, then the isomorphism is unique.
  - You only need to *find* conditions here; prove below.
- Q5.1(iii).
  - $a \neq b$ implies that $(1,1) \mapsto (1,1)$?
  - $(1,0) \mapsto ?$. It better map to an element of order p^a. It also better be idempotent, i.e., equal to its square. $(1,0) \cdot (0,1) = 0$. If it maps to (γ, δ), then $\gamma^2 = \gamma$ and $\delta^2 = \delta$. Either $p \nmid \gamma$ or $\gamma = 0$. Same with δ. This is all if $(1,0) \mapsto (\gamma, \delta)$. We have to solve $X^2 - X = 0$ in a nonintegral domain, i.e., $X(X-1) = 0$. $\gamma(\gamma - 1) = 0$ and $\delta(\delta - 1) = 0$. At least one of these is a unit so has an inverse. Multiply through by the inverse to get $\gamma = 0$ or $\gamma - 1 = 0$. Therefore, $\gamma = 0, 1$.
  - We can prove that in any case, $(1,0) \mapsto (1,0)$ or $(0,1)$. Now we use order $a \neq b$.
  - We can just state the generalization of $a \neq b$ here; do the proof in the other one.
- Q5.2(i).
  - We have that
    $$X^m - 1 = X^{m-n}(X^n - 1) + (X^{m-n} - 1)$$
    so we can induct to some extent.
    - Induct on $n + m$??
  - The three things in the picture give us what we need.
    1. Suppose $(f,g) = (h)$. Then $h \mid f, g$, i.e., $f, g \in (h)$. This implies that there exist $\alpha, \beta \in R$ such that $f = \alpha h$ and $g = \beta h$. Furthermore, equality implies that there exist $\gamma, \delta \in R$ such that $h = \gamma f + \delta g$. With this, a supposition that $d \mid f, g$ implies that $d \mid h$.
    2. Proving that $X^d - 1 \mid X^m - 1, X^n - 1$:
       $$X^n - 1 = (X^d - 1)(1 + X^d + X^{2d} + \cdots + X^{n-d})$$
    3. Suppose $n < m$. Then
       $$X^m - 1 = X^{m-n}(X^n - 1) + (X^{m-n} - 1)$$
       It follows that $X^m - 1 \in (X^n - 1, X^{m-n} - 1)$.
- Q5.2(ii).
  - Use the evaluation homomorphism, which is surjective so it sends ideals to ideals. Thus, $(X^m - 1, X^n - 1) \mapsto (q^n - 1, q^m - 1)$ and likewise for $(X^d - 1)$.
  - We could quotient by $(X - q)$ to make that surjection an isomorphism, but we don't need to.
- Q5.4(i).
  - Example of a UFD that is not a PID. $\mathbb{Z}[\sqrt{5}]$ has $(1 + \sqrt{5})(1 - \sqrt{5}) = 2 \cdot 3$?
  - R is a UFD implies that $R[X]$ is a UFD; it follows pretty quickly to the field of fractions via Gauss's lemma?
  - $\mathbb{C}[X,Y] \in \text{UFD} - \text{PID}$. $\mathbb{C}[X]$ as well.

- Q5.4(ii).
  - Primes are irreducible. We know this. In $\mathbb{Z}_2$, the only units are the powers of 2 in both numerators and denominators. Importantly, 2 is no longer a prime. Everything else may not be either. For instance, $3 = 6 \cdot 1/2 = 3 \cdot 2 \cdot 1/2$. Now $1/2$ is a unit Take an element in $D^{-1}R$. Then the numerator is reducible to a product of primes.
  - Think about the example of rings R such that $\mathbb{Z} \subsetneq R \subsetneq \mathbb{Q}$. Such rings have a certain subset of primes in the denominators. It's true in the integers, strongly hinting that the answer is true. $3/5$ implies $1/5$ in R.
  - r, s are relatively prime, hence generate 1. Bezout's identity would be helpful.
  - Ray all but said it's true.
- Q5.4(iv).
  - Don't assume that there's a unique way to write a fraction.
- Q5.5.
  - A natural thing is contradiction.
  - Suppose for the sake of contradiction that f is reducible in $\mathbb{Z}[X]$. Let $f = qh$. We sent f to $\mathbb{Z}/p\mathbb{Z}[X]$. We reduce the coefficients by p and then our homomorphism implies that $\bar{f} = \bar{q}\bar{h}$. Let $d = \deg(f)$. We know by the irreducibility of $\bar{f}$ that either $\bar{q}$ or $\bar{h}$ is a unit. WLOG, let $\bar{h}$ be a unit. We know that $\deg(\bar{f}) = \deg(f)$. We know that $\deg(h) \geq \deg(\bar{h})$ and $\deg(g) = d \geq \deg(\bar{g})$. It follows that $\deg(\bar{h}) = 0$. Thus, $\deg(h) = 0$, so h is an integer. Finally, use that $c(f) = 1$, i.e., that gives us that $h = \pm 1$, i.e., is a unit. Proposition 9.12. Set $p = 3$?