Week 7

Modules Over PIDs

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* $\boldsymbol{P}$.
  - 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* $\boldsymbol{C}$.
  - 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.

[1] Nori 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 such that $M = Av_1 + \cdots + Av_r$.
  - 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 $\mathcal{N}_C \not\subsetneq M$, then we must have $\mathcal{N}_C = M$. Suppose for the sake of contradiction that $\mathcal{N}_C = M$. Recall that $M = Av_1 + \cdots + Av_r$. 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 $M = Av_1 + \cdots + Av_r \subset N_i \subset M$. 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 $\rho : A \to \text{End}(M, +)$ to be a ring homomorphism.
  - We can factor $\rho = \bar{\rho} \circ \pi$, where $\pi : A \to A/J$ and $\bar{\rho} : A/J \to \text{End}(M, +)$. 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* $\boldsymbol{IM}$. *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 $f : R^m \to R^n$ is an isomorphism of R-modules, then f restricts to $I(R^m) \to I(R^n)$. This gives rise to the isomorphism $\bar{f} : R^m/I(R^m) \to R^n/I(R^n)$ of R-modules, in fact of R/I modules. It follows that R/I is a field, so $m = n$. ☐

- 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 $p^kM/p^{k+1}M$.
  - 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 $\mathbb{Z}[X] \to \mathbb{R}$ 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, $\prod_{i=1}^{\infty} M_i \neq \bigoplus_{i=1}^{\infty} M_i$.

7.4 Classifying Modules Over PIDs

2/15:
- We pick up from yesterday, classifying finitely generated R-modules M up to isomorphism when R is a PID.
- In particular, we begin with a further investigation of the properties of torsion modules.
- **Lift** (of $x \in M/M'$): The choice of an element $y \in M$ such that $\pi(y) = x$.
- Lemma:

  (i) $\text{Tor}(M)$ is an R-submodule of M.

  Proof. To prove that $\text{Tor}(M)$ is an R-submodule of M, Proposition 10.1 tells us that it will suffice to show that $\text{Tor}(M) \neq \emptyset$ and that $x + ry \in \text{Tor}(M)$ for all $r \in R$, $x, y \in \text{Tor}(M)$. Consider $0 \in M$. By definition, $r \cdot 0 = 0$. Thus, $0 \in \text{Tor}(M)$ as desired. Additionally, let $r \in R$ and $x, y \in \text{Tor}(M)$ be arbitrary. Since $x, y \in \text{Tor}(M)$, there exist nonzero $a, b \in R$ such that $ax = 0$ and $by = 0$. Because R is an integral domain (as a PID), a, b nonzero implies that $ab \neq 0$. Thus, since

  $$ab(x + ry) = abx + abry = b(ax) + ar(by) = b(0) + ar(0) = 0$$

  we have that $x + ry \in \text{Tor}(M)$, as desired. □

  (ii) The quotient module $M/\text{Tor}(M)$ is torsion-free.

  Proof. To prove that $M/\text{Tor}(M)$ is torsion-free, it will suffice to show that every torsion element of $M/\text{Tor}(M)$ is 0. Let's begin. Let $v \in M/\text{Tor}(M)$ be an arbitrary torsion element. Then there exists $a \in R$ nonzero such that $av = 0$. Now lift $v \in M/\text{Tor}(M)$ to $w \in M$. The constraint $av = 0 = 0 + \text{Tor}(M)$ from the quotient module implies that $0 = a\pi(w) = \pi(aw)$, hence $aw \in \text{Tor}(M)$. Thus, there exists $b \in R$ nonzero such that $b(aw) = 0$. It follows that $(ba)w = 0$, where $ba \neq 0$ since $a, b \neq 0$ by the fact that R is an integral domain. Thus, $w \in \text{Tor}(M)$, and hence $v = \pi(w) = 0$, as desired. □

- We now give some claims that will be useful later today, but whose proofs we will delay until next lecture.
- The first one pertains to the properties of finitely generated torsion-free modules over an integral domain.

- Lemma: Let R be an integral domain, and let M be a finitely generated R-module. Then there exists a submodule $M' \subset M$ such that...
  (i) $M' \cong R^h$ for some $h \geq 0$;
  (ii) There exists a nonzero $a \in R$ such that $aM \subset M'$ (equivalently, $a(M/M') = 0$).
- The next two pertain to the properties of finitely generated modules over a PID.
- Corollary: Every finitely generated torsion-free module M over a PID R is isomorphic to R^h for some $h \in \mathbb{Z}_{\geq 0}$.
- Theorem: Let M be a finitely generated R-module, where R is a PID. Then...
  (i) $\operatorname{Tor}(M) \oplus R^h \cong M$ for some $h \geq 0$;
  (ii) $\operatorname{Tor}(M)$ is finitely generated.
- **Rank** (of a module): The number h pertaining to an R-module M, where $M/\operatorname{Tor}(M) \cong R^h$. *Denoted by* $\boldsymbol{\operatorname{rank}(M)}$.
  - It follows by the proposition from last lecture (Lecture 7.1) that rank is well-defined.
- Corollary: Finitely generated R-modules M_1 and M_2 are isomorphic to each other iff
  (i) M_1 and M_2 have the same rank;
  (ii) $\operatorname{Tor}(M_1)$ is isomorphic to $\operatorname{Tor}(M_2)$.

  Proof. Suppose first that $\phi : M_1 \to M_2$ is an isomorphism. Then naturally they will have the same ranks and torsion submodules.

  On the other hand, if $\operatorname{rank}(M_1) = \operatorname{rank}(M_2)$, then $M_1/\operatorname{Tor}(M_1) \cong M_2/\operatorname{Tor}(M_2)$. This combined with the hypothesis that $\operatorname{Tor}(M_1) \cong \operatorname{Tor}(M_2)$ implies that

  $$\begin{gathered}\operatorname{Tor}(M_1) \oplus M_1/\operatorname{Tor}(M_1) \cong \operatorname{Tor}(M_2) \oplus M_2/\operatorname{Tor}(M_2) \\ M_1 \cong M_2\end{gathered}$$

  where the second line follows from the preceding theorem. $\square$

- The classification of finitely generated R-modules (R a PID) is completed by the following results.
- ***p*-primary component** (of a module): The submodule of a module M consisting of those $m \in M$ such that $p^k m = 0$ for some $k \in \mathbb{Z}_{\geq 0}$. *Denoted by* $\boldsymbol{M_{(p)}}$.
  - Showing that $M_{(p)}$ is a submodule of M can be accomplished with the submodule criterion (Proposition 10.1), just like in the first lemma proven today.
- Notation and observations.
  1. Let $M_1, \dots, M_k$ be submodules of M. Then $T : \prod_{i=1}^k M_i \to M$ defined by

     $$T(m_1, \dots, m_k) = m_1 + \cdots + m_k$$

     is not injective in general.
     - For example, if $k = 2$, then $\ker(T) \cong M_1 \cap M_2$ in general.
     - Thus, some care is required in our selection of submodules if we want $\ker(T) = 0$.
  2. Obtaining a natural R-module homomorphism $T : \oplus_{i \in I} M_i \to M$ defined as above.
     - We have that $\oplus_{i \in I} M_i \subset \prod_{i \in I} M_i$ in general. Here's why:
     - Given a finite subset $F \subset I$, we may regard $\prod_{i \in F} M_i$ as a submodule of $\prod_{i \in I} M_i$ by taking the entries in the i^{th} place to be zero for all $i \notin F$.

  - The direct sum is simply the union of the submodules $\prod_{i\in F} M_i$ taken over all finite $F \subset I$.
  - We define T on the overall direct sum one submodule $\prod_{i\in F} M_i$ at a time.

- Proposition: The natural R-module homomorphism $T : \oplus_{(p)} M_{(p)} \to \operatorname{Tor}(M)$ is an isomorphism, where the direct sum is indexed by the set of nonzero prime ideals of R.

  Proof. Let F be a set of r distinct primes $p_1, \dots, p_r$ (i.e., the prime ideals $(p_1), \dots, (p_r)$ are pairwise distinct sets). Let $(m_1, \dots, m_r) \in \prod_{(p)\in F} M_{(p)}$. Then as per the notation and observations section above, T is defined such that
  $$T(m_1, \dots, m_r) = m_1 + \cdots + m_r$$
  We first prove that T is injective. Let $(m_1, \dots, m_r) \in \ker(T)$ be arbitrary. Then $T(m_1, \dots, m_r) = m_1 + \cdots + m_r = 0$. By hypothesis, there exist $k_1, \dots, k_r$ such that $p_i^{k_i} m_i = 0$ $(i = 1, \dots, r)$. Define $a = p_2^{k_2} \cdots p_r^{k_r}$. It follows that $am_2 = \cdots = am_r = 0$. Thus,
  $$\begin{aligned} a(0) &= 0 \\ a(m_1 + \cdots + m_r) &= 0 \\ am_1 + \cdots + am_r &= 0 \\ am_1 &= -(am_2 + \cdots + am_r) \\ &= -(0 + \cdots + 0) \\ &= 0 \end{aligned}$$
  Additionally, $\gcd(a, p_1^{k_1}) = 1$ by definition, so $1 \in (a, p_1^{k_1})$. It follows that there exist $b, c \in R$ such that $ba + cp_1^{k_1} = 1$. This combined with the facts that $am_1 = 0$ and $p_1^{k_1} m_1 = 0$ implies that
  $$m_1 = 1 \cdot m_1 = (ba + cp_1^{k_1})m_1 = b(am_1) + c(p_1^{k_1} m_1) = b(0) + c(0) = 0$$
  A symmetric argument shows that all $m_i = 0$, i.e., $(m_1, \dots, m_r) = (0, \dots, 0)$. Therefore, $\ker(T) = 0$, as desired.

  We now prove that T is surjective. Let $m \in \operatorname{Tor}(M)$ be arbitrary. Consider the submodule $N = Am \subset M$. To prove that m is the sum of elements, each from a p-primary component of M, it will suffice to prove that stronger condition that every element in N is the sum of elements, each from a p-primary component of M. Equivalently, it will suffice to show that N is the isomorphic to the sum of its p-primary components, since the p-primary components of N are contained in those of M. Define $I = \{a \in R : am = 0\}$. Notice that $I = \ker(l_a)$, where $l_a : R \to N$ is the left multiplication homomorphism. It follows by the FIT that there exists an isomorphism $\overline{l_a} : R/I \to N$. Thus, we need only show that R/I is isomorphic to the direct sum of its p-primary components. But the Chinese Remainder Theorem takes care of this for us since I is a nonzero ideal. ☐

- In view of the last proposition, our final task will be to classify finitely generated p-primary modules.
- We begin with some definitions.
- ***p*-primary** (module): An R-module M such that $M = M_{(p)}$ for some prime $p \in R$.
- **Annihilator** (of a module): The set of all $a \in R$ such that $am = 0$ for all $m \in M$. *Denoted by* $\mathbf{Ann}(\boldsymbol{M})$. *Given by*
  $$\operatorname{Ann}(M) = \{a \in R : am = 0 \ \forall \ m \in M\}$$
- **Annihilator** (of an element): The set of all $a \in R$ such that $am = 0$ pertaining to a specific $m \in M$. *Denoted by* $\mathbf{Ann}(\boldsymbol{m})$. *Given by*
  $$\operatorname{Ann}(m) = \{a \in R : am = 0\}$$
- Consider $l_m : R \to M$ defined by $l_m(a) = am$.
  - By the FIT, there exists a module isomorphism $\overline{l_m} : R/\operatorname{Ann}(m) \to Rm$.

  - $\ker(l_m) = \operatorname{Ann}(m)$.

- **Cyclic** (module): An R-module M for which there exists $m \in M$ such that $M = Rm$.
  - Cyclic modules are isomorphic to $R/\operatorname{Ann}(m)$ for a similar reason to the above ($Rm = M$ here).
- With these definitions out of the way, we seek to show that every finitely generated R-module is the direct sum of cyclic modules.
- To prove this result, we will need the following lemma.
- Lemma: Let $M' = Re$ be a cyclic submodule of M, where R is a PID. We assume that...
  (i) $\operatorname{Ann}(e) = (p^n)$;
  (ii) $p^n M = 0$.

  Then every $v \in M/M'$ has a lift $w \in M$ such that $\operatorname{Ann}(w) = \operatorname{Ann}(v)$.

  Proof. Let $v \in M/M'$ be arbitrary. We first characterize the annihilator of v[2]. Since $p^n M = 0$, we know that $p^n(M/M') = 0$. Thus, we absolutely know that p^n annihilates $v \in M/M'$. However, it is possible that some power $k \leq n$ of p also annihilates the specific element v of M/M'. Let k be the smallest power of p such that $p^k v = 0$. Then $p^k \in \operatorname{Ann}(v)$. In particular, since the annihilator is an ideal (any element of the annihilator times any other element of R [multiplied left or right] is also in the annihilator by the assumed commutativity of R) and R is a PID, we know that $\operatorname{Ann}(v)$ is principal and its generator must divide p^k (i.e., be a power of p). But by the assumption that k is the smallest integer such that $p^k \in \operatorname{Ann}(v)$, we have that $\operatorname{Ann}(v) = (p^k)$.

  We now begin the bidirectional inclusion argument in earnest. Our strategy is thus: We will construct a lift w' of v, prove that $\operatorname{Ann}(v) \subset \operatorname{Ann}(w')$, and then prove that $\operatorname{Ann}(w') \subset \operatorname{Ann}(v)$. Let's begin.

  Pick any lift $w \in M$ of v. By hypothesis $p^k v = 0$, so $p^k w \in M'$. It follows since M' is cyclic that $p^k w = \alpha e$ for some $\alpha \in R$. Additionally, since $p^n M = 0$ by hypothesis, we know that $p^n w = 0$. Thus, since $n \geq k$, we have that

  $$0 = p^n w = p^{n-k} p^k w = p^{n-k} \alpha e$$

  Thus, $p^{n-k}\alpha \in \operatorname{Ann}(e)$. It follows since $\operatorname{Ann}(e) = (p^n)$ by hypothesis that

  $$\begin{aligned} p^{n-k}\alpha &= p^n \beta \\ \alpha &= p^k \beta \end{aligned}$$

  for some $\beta \in R$. Now define $w' = w - \beta e$. Note that w' is still a lift of v since we only added the element $-\beta e$ of $M' = Ae$ to it.

  In particular, we have that

  $$p^k w' = p^k w - p^k \beta e = p^k w - \alpha e = 0$$

  This proves that $p^k \in \operatorname{Ann}(w')$. Since annihilators are ideals, as discussed above, it follows that $\operatorname{Ann}(v) = (p^k) \subset \operatorname{Ann}(w')$.

  To finish the proof, it will just suffice to show that $\operatorname{Ann}(w') \subset \operatorname{Ann}(v)$. Let $a \in \operatorname{Ann}(w')$ be arbitrary. Then $aw' = 0$. It follows that $0 = \pi(aw') = a\pi(w') = av$. Therefore, $a \in Ann(v)$ as well. ☐

- Proposition: For every finitely generated p-primary module M, there exist $e_1, \dots, e_s$ such that M is the direct sum of the cyclic submodules Re_i.

[2] Steps like the following will be performed often in subsequent proofs without elaboration, so this paragraph serves to go through everything in full detail once.

Proof. Since M is finitely generated, we know that $M = Rv_1 + \cdots + Rv_r$. We induct on r.

For the base case $r = 1$, M is cyclic by definition.

Now suppose that we have proven the claim for $r-1$; we now seek to prove it for r. Assume WLOG that $(p^n) = \text{Ann}(v_1) \subset \text{Ann}(v_i)$ for all $i = 1, \dots, r$. Essentially, what we are doing here is just relabeling the generators so that v_1 is the generator of M with the smallest annihilator, i.e., the one with the highest power of p as generator. In particular, since n is the largest of its kind, we know that $p^n M = 0$. Now let $e = v_1$ and $M' = Re$. Then by the properties of the canonical *surjection*, M/M' is generated by $\bar{v}_1, \dots, \bar{v}_r$. But since $\bar{v}_1 = 0$ by the definition of M', we have that M/M' is generated by $\bar{v}_2, \dots, \bar{v}_r$.

Therefore, by the induction hypothesis, there exist $e_1, \dots, e_s$ such that M is the direct sum of the cyclic submodules $\bigoplus_{i=1}^s Re_i$. Another way of phrasing this is that the natural homomorphism $T'' : Re_1 \oplus \cdots \oplus Re_s \to M/M'$ is an isomorphism. It follows by the preceding lemma that there exist lifts $w_1, \dots, w_s \in M$ of $e_1, \dots, e_s$, respectively, such that $\text{Ann}(w_i) = \text{Ann}(e_i)$ for all $i = 1, \dots, s$.

We wish to deduce that the natural homomorphism $T : Re \oplus Rw_1 \oplus \cdots \oplus Rw_s \to M$ is also an isomorphism. For surjectivity, let $N = Rw_1 + \cdots + Rw_s$. It follows logically that the image of the composite homomorphism $N \hookrightarrow M \to M/M'$ is just $Re_1 + \cdots + Re_s$. This set is, in fact, all of M/M' by the surjectivity of T''. Thus, $M' + N = M$, as desired. For injectivity, let $a, a_1, \dots, a_s$ be such that $ae + a_1 w_1 + \cdots + a_s w_s = 0$. Then we have the equation $a_1 e_1 + \cdots + a_s e_s = 0$ in M/M'. It follows by the injectivity of T'' that $a_i \in \text{Ann}(e_i)$ for all $i = 1, \dots, r$. Since $\text{Ann}(e_i) = \text{Ann}(w_i)$ by the above, it follows that $a_i w_i = 0$ ($i = 1, \dots, s$). Thus,

$$0 = ae + a_1 w_1 + \cdots + a_s w_s = ae + 0 + \cdots + 0 = ae$$

Therefore, since $ae \in Re$ is zero and is the last remaining term, $\ker(T) = 0$. $\square$

7.5 Rational Canonical Form and Proofs of Earlier Lemmas

2/17:

- Theorem: Every finitely generated R-module M (where R is a PID) is isomorphic to $\text{Tor}(M) \oplus R^h$ for some $h \in \mathbb{Z}_{\geq 0}$, where $h = \text{rank}(M)$.
- Recall the following theorem.
- Theorem: Let R be a PID. Then
  (1) Every finitely generated p-primary R-module is a finite direct sum of cyclic modules (which are isomorphic to $R/p^h R$ for some $h \in \mathbb{N}$).
  (2) Every torsion module M is the direct sum of its p-primary components.
- Corollary: Every finitely generated torsion R-module is isomorphic to the finite direct sum of cyclic p-primary modules where p is an element of a finite set of primes. *picture*
- M finitely generated implies that $M_{(p)}$ is finitely generated.
- Said aloud that only finite primes p satisfy $M_{(p)} \neq 0$.
- Theorem (Rational canonical form): Let R be a PID. Then every finitely generated R-torsion module is isomorphic to
  $$R/(a_1) \oplus \cdots \oplus R/(a_\ell)$$
  where $a_2 \mid a_1$, $a_3 \mid a_2$, $\dots$, $a_\ell \mid a_{\ell-1}$.
- Observe: The principal ideal (a_1) is exactly the annihilator of M, i.e.,
  $$(a_1) = \{\alpha \in R : \alpha m = 0 \ \forall\ m \in M\}$$
  - Later, (a_1) will play the role of a minimal polynomial, and the product will play the role of the characteristic polynomial.

Proof of theorem. Let M be an arbitrary finitely generated R-torsion module. Since $M = \text{Tor}(M)$, a proposition from last lecture implies that

$$M = \text{Tor}(M) \cong \bigoplus_{(p)} M_{(p)}$$

Let $p_1, \dots, p_\ell$ be the set of distinct primes for which $M_{(p)} \neq 0$. Then

$$M \cong M_{(p_1)} \oplus \cdots \oplus M_{(p_\ell)}$$

Consider some $M_{(p_i)}$ in the above direct sum. Since it is finitely generated (because the isomorphism is natural) and p-primary (by definition), we have by another proposition from last time that

$$M_{(p_i)} \cong Re_1 \oplus \cdots \oplus Re_{s_i}$$

We know (again from last lecture) that each cyclic submodule Re_j is isomorphic to $R/\operatorname{Ann}(e_j)$. Since $M_{(p_i)}$ is p_i-primary and $e_j \in M_{(p_i)}$, we know that there exists (a minimal) $m_{i,j}$ such that $p_i^{m_{i,j}} e_j = 0$. Thus, since R is a PID, $\operatorname{Ann}(e_j) = (p_i^{m_{i,j}})$. Replacing every element in the above direct sum with our new form reveals that

$$M_{(p_i)} \cong R/(p_i^{m_{i,1}}) \oplus \cdots \oplus R/(p_i^{m_{i,s_i}})$$

WLOG, let $m_{i,1} \geq \cdots \geq m_{i,s_i}$. Define

$$a_r = \prod_{i=1}^{\ell} p_i^{m_{i,r}}$$

for all $r = 1, \dots, s_i$. It follows by the construction that $a_{r+1} \mid a_r$ ($r = 1, \dots, s_i - 1$). Additionally, we have by the Chinese Remainder Theorem that for each $r = 1, \dots, s_i$,

$$R/(a_r) \cong \prod_{i=1}^{\ell} R/(p_i^{m_{i,r}}) = \bigoplus_{i=1}^{\ell} R/(p_i^{m_{i,r}})$$

WLOG, let $s_\ell \geq s_i$ ($i = 1, \dots, \ell$). Therefore, putting everything together, we have that

$$\begin{aligned}
M &\cong M_{(p_1)} \oplus \cdots \oplus M_{(p_\ell)} \\
&\cong \left(\bigoplus_{j=1}^{s_1} R/(p_1^{m_{1,j}}) \right) \oplus \cdots \oplus \left(\bigoplus_{j=1}^{s_\ell} R/(p_\ell^{m_{\ell,j}}) \right) \\
&\cong \left(\bigoplus_{i=1}^{\ell} R/(p_i^{m_{i,1}}) \right) \oplus \cdots \oplus \left(\bigoplus_{i=1}^{\ell} R/(p_i^{m_{i,s_\ell}}) \right) \\
&\cong R/(a_1) \oplus \cdots \oplus R/(a_{s_\ell})
\end{aligned}$$

as desired. ∎

- The previous theorem but over all modules instead of just torsion modules.
- Proposition: Every finitely generated R-module, where R is a PID, is isomorphic to

  $$R/I_1 \oplus R/I_2 \oplus \cdots$$

  for a unique increasing sequence of ideals $I_1 \subset I_2 \subset \cdots$ which have the property that $I_n = R$ for some n.

  Proof.

  - 2.4: $M \cong R^h \oplus \text{Tor}(M)$ for some $h \geq 0$.

- RCF: $\operatorname{Tor}(M) \cong R/(a_1) \oplus \cdots \oplus R/(a_\ell)$ where $a_\ell \mid a_{\ell-1} \mid \cdots \mid a_1$.
- $R^h \cong Re_1 \oplus \cdots \oplus Re_h \cong R/\operatorname{Ann}(e_1) \oplus \cdots \oplus R/\operatorname{Ann}(e_h)$.
- R is a PID: $\operatorname{Ann}(e_j) = (a_{\ell+j})$ for some $a_{\ell+j}$ and all $j = 1, \dots, h$.
- Let $I_i = (a_i)$.
- WLOG, order them. How do I guarantee the subset condition??
- Then $M \cong R/I_1 \oplus \cdots \oplus R/I_{\ell+h}$.
- If no $I_i = R$, define $I_{\ell+h+1}, I_{\ell+h+2}, \dots$ to be equal to R.

$\square$

- That concludes torsion modules over PIDs; we now do torsion modules over fields, which should be easier.
- ***R*-linearly independent** (elements of M): A set of elements $u_1, \dots, u_\ell \in M$ such that the constraints

$$(a_1, \dots, a_\ell) \in R^\ell \qquad\qquad \sum_{i=1}^{\ell} a_i u_i = 0$$

imply that $(a_1, \dots, a_\ell) = 0$. Equivalently, $H : R^\ell \to M$ defined by

$$H(a_1, \dots, a_\ell) = \sum_{i=1}^{\ell} a_i u_i$$

is 1-1, i.e., $R^\ell \cong H(M)$.

- Lemma: Let R be an integral domain, and let M be a finitely generated R-module. Then there exists a submodule $M' \subset M$ such that...

(i) $M' \cong R^h$ for some $h \geq 0$;

Proof. Let $S \subset M$ be a finite generating set. Select $T \subset S$ such that (i) T is linearly independent and (ii) $T \subsetneq W \subset S$ implies that W is *not* linearly independent. In other words, we are picking T to be a maximal linear independence set. Now suppose $|T| = h$ so that $T = \{u_1, \dots, u_h\}$. Then by definition,

$$M' = \sum_{i=1}^{h} Ru_i \cong R^h$$

where the latter isomorphism follows from Proposition 10.5. $\square$

(ii) There exists a nonzero $a \in R$ such that $aM \subset M'$ (equivalently, $a(M/M') = 0$).

Proof. Pick $w \in S$ such that $w \notin T$. Then since we picked T to be a *maximal* linear independence set, $T \cup \{w\}$ is linearly *dependent*. It follows that there exists a nonzero $(a_1, \dots, a_{h+1}) \in R^{h+1}$ such that

$$a_1u_1 + \cdots + a_hu_h + a_{h+1}w = 0$$

If $a_{h+1} = 0$, then $(a_1, \dots, a_h) \neq 0$ makes $a_1u_1 + \cdots + a_hu_h = 0$, contradicting the assumed linear independence of T. Thus, $a_{h+1} \neq 0$. It follows that

$$a_{h+1}w = -\sum_{i=1}^{h} a_i u_i \in M'$$

We may repeat this process for any $w \in S - T$ to obtain a nonzero a_w such that $a_w w \in M'$. Additionally, if $w \in T$, take $a_w = 1$. Now define

$$a = \prod_{w \in S} a_w$$

Since R is an integral domain by hypothesis and each a_w in the above product is nonzero, a is nonzero. Moreover, by its construction, $aw \in M'$ for all $w \in S$. Therefore,

$$aM = a\left(\sum_{s\in S} As\right) \subset M'$$

as desired. $\square$

- Note that you can make stronger statements than the above; you'll just have to use Zorn's lemma to do so.
- We now return to PID-land.
- Corollary: Every finitely generated torsion-free module M over a PID R is isomorphic to R^h for some $h \in \mathbb{Z}_{\geq 0}$.

  Proof. Apply the lemma to obtain a submodule M' of M such that $M' \cong R^h$ and a nonzero $a \in R$ such that $aM \subset M'$. Consider $H : M \to M'$ defined by $H(m) = am$. Since H is just left-multiplication, H is an R-module homomorphism. Additionally, since M is torsion free, $am = 0$ iff $m = 0$ so we have $\ker H = 0$. Thus, since H is injective, $M \cong H(M) \subset M' \cong R^h$. Furthermore, since R is a PID, the submodule $H(M)$ of R^h must be isomorphic to R^n for some $0 \leq n \leq h$ by the Theorem from Week 6. It follows by transitivity that $M \cong H(M) \cong R^n$, as desired. $\square$

- Takeaway: The torsion-free part is far easier to handle than the torsion part.
- Theorem: Let M be a finitely generated R-module, where R is a PID. Then...
  (i) $\operatorname{Tor}(M) \oplus R^h \cong M$ for some $h \geq 0$;

  Proof. To prove that $\operatorname{Tor}(M) \oplus R^h \cong M$, the second theorem from Lecture 6.3 tells us that it will suffice to show that $M/\operatorname{Tor}(M) \cong R^h$ for some $h \geq 0$. By part (ii) of the lemma from last time (Lecture 7.2), we have that $M/\operatorname{Tor}(M)$ is torsion-free. This combined with the fact that $M/\operatorname{Tor}(M)$ is a finitely generated (since M is finitely generated) module over a PID allows us to invoke the above corollary, yielding the desired result.

  Note that the isomorphism $T : \operatorname{Tor}(M) \oplus R^h \to M$ is given by

  $$T(m, (a_1, \dots, a_h)) = m + \sum a_i e_i$$

  where $e_1, \dots, e_h$ generate R^h. $\square$

  (ii) $\operatorname{Tor}(M)$ is finitely generated.

  Proof. Since M is finitely generated, part (i) implies that $\operatorname{Tor}(M) \oplus R^h$ is finitely generated. Now consider the projection $\pi : \operatorname{Tor}(M) \oplus R^h \to \operatorname{Tor}(M)$. Since it is a surjection, the (finite number of) images of the generators of $\operatorname{Tor}(M) \oplus R^h$ generate $\operatorname{Tor}(M)$. $\square$

- Nori reproves the claim that $M/\operatorname{Tor}(M)$ is torsion-free (see the first lemma from last lecture).
- If $\pi : M \to M/M'$ and $S : M/M' \to R_h$ is an isomorphism, then there exists $\varphi : R^h \to M$ such that the diagram commutes, i.e., $S\pi\varphi = \mathrm{id}_{R^h}$.
- Next week is going to be straight linear algebra.
- Nori would try to do tensors in one week (the last week), but it'd be ridiculous to do something on Friday and put it on a test on Tuesday.
- Imaginary quadratic fields, curves, Dedekind domains, etc.
- Content from this week in the book.

- Section 12.1.
  - The material before Theorem 12.5 is OMITTED from the course.
  - Theorem **??** is also OMITTED from the course.
  - The rest of this section will be covered.
  - The main theorems are: The existence theorem (Theorem 12.5) and the uniqueness theorem (Theorem **??**)
- Section 12.2 deals with the PID $F[X]$ and its applications to linear algebra; this will be covered on Monday next week.

7.6 Office Hours (Callum)

- Problem 6.5?
  - Go with the explicit route, not the universal property of the ring of fractions route.
  - Explicit: Define
    $$F(v) = \frac{1}{a} f(av)$$
  - We need to prove that $1/af(av) = 1/bf(bv)$ for valid a, b. Multiply both sides by ab and use commutativity. Thus, $F(v)$ is well defined.
- Problem 6.8?
  - The hardest one. Doesn't really use any of the previous parts.
  - Define $\phi : A \oplus M \to A^2$ to be the isomorphism. Consider $(1,0) \in A \oplus M$. In particular, let $\phi(1,0) = (a,b)$. We know that it will generate a copy of A in A^2. Essentially, $A(a,b) = A^2$. We know that $\phi^{-1} : A^2 \to A \oplus M$ and $P : A \oplus M \to A$. Suppose $P \circ \phi^{-1} : (1,0) \mapsto c$ and $(0,1) \mapsto d$.
  - Consider
    $$A \hookrightarrow A \oplus M \xrightarrow{\phi} A^2 \xrightarrow{\phi^{-1}} A \oplus M \xrightarrow{P} A$$
    which is the identity on A. Then
    $$1 \mapsto (1,0) \mapsto (a,b) = a(1,0) + b(0,1) \mapsto ac + bd$$
    so $ac + bd = 1$.
  - Consider the matrix
    $$\begin{pmatrix} a & d \\ b & c \end{pmatrix}$$
    - Determinant??
    - $(-d, c)$
    - So thus, $M = A(-d,c)$??
  - $(-d,c) \in A^2$ defines a map from $A^2 \to M$ with kernel A. $(-d,c) \in \ker(P \circ \phi^{-1})$. Thus, $\phi^{-1}(-d,c) \in \{0\} \oplus M \cong M$.
  - Thus, at this point, we may define a map
    $$A \hookrightarrow A^2 \xrightarrow{\phi^{-1}} A \oplus M \xrightarrow{P} M$$
    by
    $$1 \mapsto (-d,c)$$
    and this should be an isomorphism.
  - $(-d,c)$ generates a submodule of A^2 that is isomorphic to M.
  - Injectivity follows from that of all of the components.

- Surjectivity: Pull m back to $(0,m)$ and then $\phi(0,m)\in A^2$. The subset of A^2 equal to all $\phi(0,m)$ is equal to
$$\{(u,v)\in A^2:\phi^{-1}(u,v)\in 0\oplus M\}=\{(u,v)\in A^2:uc+vd=0\}$$
- We want to find $k\in A$ such that $(u,v)=k(-d,c)$. In other words, we want $u=-kd$ and $v=kc$. $ua=-kda=k(1-bc)=k-kbc=k-bv$. Thus, $k=ua+bv$. Now we have to substitute that back in and show that it works.
- Thus, we have that
$$kc=ua+bvc=uac+b(1-ad)=v+uac-vad=v+a(bc-ad)$$
- Saying $A\cong M$ is kind of like saying that there's a change of basis. That's why matrices keep coming up.
- Summary of what we did.
  1. We have
  $$A\hookrightarrow A\oplus M\xrightarrow{\phi}A^2\xrightarrow{\phi^{-1}}A\oplus M\xrightarrow{P}A$$
  and this is the identity.
  2. We define $(1,0)\mapsto(a,b)$, which will generate a copy of A in A^2.
  3. We now need to find a basis vector corresponding to M (which we hope is A).
  4. $\{(1,0),(0,1)\}$ is the standard basis for A^2.
  5. We need to solve for x,y such that
  $$\begin{pmatrix}a&x\\b&y\end{pmatrix}$$
  is invertible.
  6. $\{\phi^{-1}(1,0),\phi^{-1}(0,1)\}$ is another basis of A^2.
  7. We want $ac+bd=1$.

7.7 Chapter 11: Vector Spaces

From Dummit and Foote (2004).

Section 11.1: Definitions and Basic Theory

2/20:
- Reviewing Labalme (2021) is probably a good idea.
  - Many of Dummit and Foote (2004)'s proofs more elegant, though.
- Goal of this chapter:
  - Brief overview of results that will be used later on; more in-depth (even introductory level) linear algebra topics, such as Gauss-Jordan elimination, row echelon forms, etc., will not be covered.
  - Only finite-dimensional vector spaces are discussed in the text; some stuff on infinite dimensional vector spaces is included in the exercises.
  - Characteristic polynomials and eigenvalues: Next chapter.
- Module terminology vs. vector space terminology.
- In this chapter, F denotes a field and V denotes a vector space over F.
- **Linearly independent** (subset $S\subset V$): A subset S of V for which the equation $\alpha_1v_1+\cdots+\alpha_nv_n=0$ with $\alpha_1,\dots,\alpha_n\in F$ and $v_1,\dots,v_n\in S$ implies $\alpha_1=\cdots=\alpha_n=0$.
- **Basis**: An ordered set of linearly independent vectors which span V. *Also known as* **ordered basis**.

Terminology for R any Ring	**Terminology for R a Field**
M is an R-module	M is a vector space over R
m is an element of M	m is a vector in M
α is a ring element	α is a scalar
N is a submodule of M	N is a subspace of M
M/N is a quotient module	M/N is a quotient space
M is a free module of rank n	M is a vector space of dimension n
M is a finitely generated module	M is a finite dimensional vector space
M is a nonzero cyclic module	M is a 1-dimensional vector space
$\varphi : M \to N$ is an R-module homomorphism	$\varphi : M \to N$ is a linear transformation
M and N are isomorphic as R-modules	M and N are isomorphic vector spaces
The subset A of M generates M	The subset A of M spans M
$M = RA$	Each element of M is a linear combination of elements of A, i.e., $M = \text{Span}(A)$

Table 7.1: Module vs. vector space terminology.

- In particular, two bases will be considered different even if one is simply a rearrangement of the other.

- Examples.
  1. $V = F[X]$.
     - Basis: $1, X, X^2, \ldots$ is linearly independent by definition since a polynomial is zero iff all of its coefficients are 0.
  2. The collection of solutions of a linear, homogeneous, constant coefficient differential equation over $\mathbb{C}$.
     - A vector space since differentiation is a linear operator.
     - Elements are linearly independent if they are linearly independent as functions.
       - Example: $\mathrm{e}^t, \mathrm{e}^{2t}$ are easily seen to be solutions of the equation $y'' - 3y' + 2y = 0$.
       - They are linearly independent since $a\mathrm{e}^t + b\mathrm{e}^{2t} = 0$ implies $a+b = 0$ ($t = 0$) and $a\mathrm{e} + b\mathrm{e}^2 = 0$ ($t = 1$), and the only solution to this system of two equations is $a = b = 0$.
       - It is a theorem of differential equations that these elements span the set of solutions of this equation.

- Vector spaces are free modules.

Proposition 11.1. Assume the set $\mathcal{A} = \{v_1, \ldots, v_n\}$ spans the vector space V but no proper subset of $\mathcal{A}$ spans V. Then $\mathcal{A}$ is a basis of V. In particular, any finitely generated (i.e., finitely spanned) vector space over F is a free F-module.

Proof. Given. □

- Example.
  1. Consider $F[X]/(f)$, where $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$.
     - (f) is a subspace of $F[X]$.
     - Euclidean Algorithm: Every $a \in F[X]$ can be written uniquely in the form $qf + r$ where $0 \leq \deg(r) \leq n - 1$. Thus, every element of the quotient is represented by a polynomial r of degree $\leq n - 1$.
     - It follows that $\overline{1}, \overline{X}, \overline{X^2}, \ldots, \overline{X^{n-1}}$ spans $F[X]/(f)$.

- Spanning sets contain bases.

  Corollary 11.2. Assume the finite set $\mathcal{A}$ spans the vector space V. Then $\mathcal{A}$ contains a basis of V.

  Proof. Given. □

- A new property of bases.

  Theorem 11.3 (Replacement Theorem)**.** Assume $\mathcal{A} = \{a_1, \ldots, a_n\}$ is a basis for V containing n elements and $\{b_1, \ldots, b_m\}$ is a set of linearly independent vectors in V. Then there is an ordering $a_1, \ldots, a_n$ such that for each $k \in \{1, \ldots, m\}$, the set

  $$\{b_1, \ldots, b_k, a_{k+1}, \ldots, a_n\}$$

  is a basis of V. In other words, the elements $b_1, \ldots, b_m$ can be used to successively replace the elements of the basis $\mathcal{A}$, still retaining a basis. In particular, $n \geq m$.

  Proof. Given. □

- Linear independence, span, and cardinality.

  Corollary 11.4.

  1. Suppose V has a finite basis with n elements. Any set of linearly independent vectors has $\leq n$ elements. Any spanning set has $\geq n$ elements.
  2. If V has some finite basis, then any two bases of V have the same cardinality.

  Proof. Given. □

- **Dimension**: The cardinality of any basis of V. *Denoted by* $\boldsymbol{\dim_F V}$, $\boldsymbol{\dim V}$.
- **Finite dimensional** (vector space): A vector space V that is finitely generated.
- **Infinite dimensional** (vector space): A vector space V that is not finitely generated.
  - We write $\dim V = \infty$ for these.
- Examples.
  1. The dimension of the solution space to $y'' - 3y' + 2y = 0$ is 2.
     - Recall from above that a basis is $\mathrm{e}^t, \mathrm{e}^{2t}$.
     - In general, it is a theorem in differential equations that the space of solutions of an n^{th} order linear, homogeneous, constant coefficient differential equation of degree n over $\mathbb{C}$ is a vector space over $\mathbb{C}$ of dimension n.
  2. The dimension of $F[X]/(f)$ is $\deg(f)$.
     - $F[X]$ and (f) are infinite dimensional vector spaces.
- Linearly independent lists and bases.

  Corollary 11.5 (Building-Up Lemma)**.** If A is a set of linearly independent vectors in the finite dimensional space V, then there exists a basis of V containing A.

  Proof. Given. □

- Characterizing finite dimensional vector spaces.

Theorem 11.6. If V is an n-dimensional vector space over F, then $V \cong F^n$. In particular, any two finite dimensional vector spaces over F of the same dimension are isomorphic.

Proof. Given. $\square$

- Examples.
  1. Bases of ${\mathbb{F}_q}^k$.
     - Dummit and Foote (2004) justifies that the number of distinct bases of ${\mathbb{F}_q}^k$ is
     $$(q^k - 1)(q^k - q)(q^k - q^2) \cdots (q^k - q^{k-1})$$
     - For every vector $v \in {\mathbb{F}_q}^k$, there are $q - 1$ other linearly dependent vectors (corresponding to the q $\mathbb{F}$-multiples of it).
  2. Subspaces of ${\mathbb{F}_q}^n$.
     - Dummit and Foote (2004) justifies that the number of distinct k-dimensional subspaces of ${\mathbb{F}_q}^n$ is
     $$\frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})}$$
- Dimension of the quotient space.

  Theorem 11.7. Let V be a vector space over F, and let W be a subspace of V. Then V/W is a vector space with $\dim V = \dim W + \dim V/W$ (where if one side is infinite, then both are).

  Proof. Given. $\square$

- Dimension of the kernel and image of a linear transformation.

  Corollary 11.8. Let $\varphi : V \to U$ be a linear transformation of vector spaces over F. Then $\ker \varphi$ is a subspace of V, $\varphi(V)$ is a subspace of U, and $\dim V = \dim \ker \varphi + \dim \varphi(V)$.

  Proof. Given. $\square$

- Classifying isomorphic operator.

  Corollary 11.9. Let $\varphi : V \to W$ be a linear transformation of vector spaces of the same finite dimension. Then the following are equivalent.

  1. φ is an isomorphism.
  2. φ is injective, i.e., $\ker \varphi = 0$.
  3. φ is surjective, i.e., $\varphi(V) = W$.
  4. φ sends a basis of V to a basis of W.

  Proof. Given. $\square$

- **Null space** (of a linear transformation): The kernel of the linear transformation.
- **Nullity** (of a linear transformation): The dimension of the kernel of the linear transformation.
- **Rank** (of a linear transformation): The dimension of the image of the linear transformation.
- **Nonsingular** (linear transformation): A linear transformation φ for which $\ker \varphi = 0$.
- **General linear group**: The group of all nonsingular linear transformations from $V \to V$ under the group operation of composition. *Denoted by* $\boldsymbol{GL(V)}$.
  - Dummit and Foote (2004) justifies that if $V = {\mathbb{F}_q}^n$, then
  $$|GL(V)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$$

Exercises

4. Prove that the space of real-valued functions on the closed interval $[a, b]$ is an infinite dimensional vector space over $\mathbb{R}$, where $a < b$.

5. Prove that the space of continuous real-valued functions on the closed interval $[a, b]$ is an infinite dimensional vector space over $\mathbb{R}$, where $a < b$.

10. Prove that any vector space V has a basis (by convention, the null set is the basis for the zero space). *Hint*: Let $\mathcal{S}$ be the set of subsets of V consisting of linearly independent vectors, partially ordered under inclusion; apply Zorn's Lemma to $\mathcal{S}$ and show that a maximal element of $\mathcal{S}$ is a basis.

11. Refine your argument in the preceding exercise to prove that any set of linearly independent vectors of V is contained in a basis of V.

12. If F is a field with a finite or countable number of elements and V is an infinite dimensional vector space over F with basis $\mathcal{B}$, prove that the cardinality of V equals the cardinality of $\mathcal{B}$. Deduce in this case that any two bases of V have the same cardinality.

13. Prove that as vector spaces over $\mathbb{Q}$, $\mathbb{R}^n \cong \mathbb{R}$ for all $n \in \mathbb{Z}^+$. Note that, in particular, this means that $\mathbb{R}^n$ and $\mathbb{R}$ are isomorphic as additive abelian groups.

14. Let $\mathcal{A}$ be a basis for the infinite dimensional vector space V. Prove that V is isomorphic to the direct sum of copies of the field F indexed by the set $\mathcal{A}$. Prove that the direct product of copies of F indexed by $\mathcal{A}$ is a vector space over F and it has strictly larger dimension than the dimension of V (see the exercises in Section 10.3 for the definitions of direct sum and direct product over infinitely many modules).

Section 11.2: The Matrix of a Linear Transformation

- Assumptions for this section.
  - V, W are vector spaces over the field F.
  - $\mathcal{B} = \{v_1, \dots, v_n\}$ is an (ordered) basis of V, and $\mathcal{E} = \{w_1, \dots, w_m\}$ is an (ordered) basis of W.
  - $\varphi \in \operatorname{Hom}(V, W)$.
- **Matrix** (of φ with respect to the bases $\mathcal{B}, \mathcal{E}$): The $m \times n$ matrix whose i, j entry is α_{ij}, where

$$\varphi(v_j) = \sum_{i=1}^{m} \alpha_{ij} w_i$$

  Denoted by $\boldsymbol{M_{\mathcal{B}}^{\mathcal{E}}(\varphi)}$.
- Dummit and Foote (2004) reviews how to recover φ from $M_{\mathcal{B}}^{\mathcal{E}}(\varphi)$.
  - The equivalence of matrix multiplying and linear transforming is sometimes denoted

$$[\varphi(v)]_{\mathcal{E}} = M_{\mathcal{B}}^{\mathcal{E}}(\varphi)[v]_{\mathcal{B}}$$

- **Representation** (of φ with respect to the bases $\mathcal{B}, \mathcal{E}$): The matrix $A = (a_{ij})$ associated with φ.
- Examples.
  1. Computing a matrix with respect to the standard bases of $\mathbb{R}^3, \mathbb{R}^2$.
  2. The matrix of the differentiation operator $\varphi : V \to V$ on the 2-dimensional space of solutions V to $y'' - 3y' + 2y = 0$.

  - Since
$$\varphi(v_1) = \frac{\mathrm{d}}{\mathrm{d}t}(\mathrm{e}^t) = \mathrm{e}^t = v_1 \qquad \varphi(v_2) = \frac{\mathrm{d}}{\mathrm{d}t}(\mathrm{e}^{2t}) = 2\mathrm{e}^{2t} = 2v_2$$
the representation of φ is
$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

3. Computing a matrix with respect to the standard bases of $\mathbb{Q}^3, \mathbb{Q}^3$.

- Isomorphism between the space of linear transformations and the space of matrices.

Theorem 11.10. Let V be a vector space over F of dimension n and let W be a vector space over F of dimension m, with respective bases $\mathcal{B}, \mathcal{E}$. Then the map $\mathrm{Hom}_F(V,W) \to M_{m\times n}(F)$ from the space of linear transformations from V to W to the space of $m \times n$ matrices with coefficients in F defined by $\varphi \mapsto M_{\mathcal{B}}^{\mathcal{E}}(\varphi)$ is a vector space isomorphism. In particular, there is a bijective correspondence between linear transformations and their associated matrices with respect to a fixed choice of bases.

Proof. Given. □

- There is no *natural* isomorphism between $\mathrm{Hom}_F(V,W)$ and $M_{m\times n}(F)$.
  - This is because the choices of bases are arbitrary (there is no natural choice of them).
- Dimension of the space of linear transformations.

Corollary 11.11. The dimension of $\mathrm{Hom}_F(V,W)$ is $(\dim V)(\dim W)$.

Proof. Given. □

- **Nonsingular** (matrix): An $m \times n$ matrix A such that $Ax = 0$ with $x \in F^n$ implies that $x = 0$. *Also known as* **invertible**.
- Nonsingular linear transformations vs. nonsingular matrices.
  - Independent of the choice of bases, a matrix is nonsingular iff the corresponding linear transformation is nonsingular.
- Dummit and Foote (2004) uses the definition of the matrix to deduce the formula for matrix multiplication.
- Relating matrix multiplication to linear transformation composition.

Theorem 11.12. Let U, V, W be finite dimensional vector spaces over F with ordered bases $\mathcal{D}, \mathcal{B}, \mathcal{E}$, and assume $\psi : U \to V$ and $\varphi : V \to W$ are linear transformations. Then
$$M_{\mathcal{D}}^{\mathcal{E}}(\varphi \circ \psi) = M_{\mathcal{B}}^{\mathcal{E}}(\varphi) M_{\mathcal{D}}^{\mathcal{B}}(\psi)$$
In words, the product of the matrices representing the linear transformations φ, ψ is the matrix representing the composite linear transformation $\varphi \circ \psi$.

- Properties of matrix multiplication.

Corollary 11.13. Matrix multiplication is associative and distributive (whenever the dimensions are such as to make products defined). An $n \times m$ matrix A is nonsingular if and only if it is invertible.

Proof. Given. □

- Ring-like properties of $M_n(F)$, as induced by those of $\mathrm{Hom}_F(V,V)$.

Corollary 11.14.

1. If $\mathcal{B}$ is a basis of the n-dimensional space V, the map $\varphi \mapsto M_{\mathcal{B}}^{\mathcal{B}}(\varphi)$ is a ring and a vector space isomorphism of $\mathrm{Hom}_F(V,V)$ onto the space $M_n(F)$ of $n \times n$ matrices with coefficients in F.
2. $GL(V) \cong GL_n(F)$, where $\dim V = n$. In particular, if F is a finite field, the order of the finite group $GL_n(F)$ (which equals $|GL(V)|$) is given by the formula at the end of Section 11.1.

Proof. Given. $\square$

- **Row rank** (of a matrix): The maximal number of linearly independent rows of the matrix, where the rows are considered as vectors in affine m-space.
- **Column rank** (of a matrix): The maximal number of linearly independent columns of the matrix, where the columns are considered as vectors in affine n-space.
- Relating ranks.
  - The rank of ψ equals the column rank of $M_{\mathcal{B}}^{\mathcal{E}}(\psi)$.
- **Similar** (matrices): Two $n \times n$ matrices A, B for which there exists an invertible $n \times n$ matrix P such that $P^{-1}AP = B$.
- **Similar** (linear transformations): Two linear transformations $\varphi, \psi : V \to V$ for which there exists a nonsingular linear transformation ξ such that $\xi^{-1}\varphi\xi = \psi$.
  - This is an equivalence relation whose equivalence classes are the orbits of $GL(V)$ acting by conjugation on $\mathrm{Hom}_F(V,V)$.
- **Transition** (matrix from $\mathcal{B}$ to $\mathcal{E}$): The matrix defined as follows, where I is the identity transformation. *Also known as* **change of basis** (matrix). *Denoted by* $\boldsymbol{P}$. *Given by*

$$P = M_{\mathcal{B}}^{\mathcal{E}}(I)$$

  - $P = M_{\mathcal{B}}^{\mathcal{E}}(I)$ satisfies $P^{-1}M_{\mathcal{B}}^{\mathcal{B}}(I)P = M_{\mathcal{E}}^{\mathcal{E}}(\varphi)$.
    - If $\mathcal{B} \neq \mathcal{E}$, then P is not the identity matrix.
  - Note that we need *ordered* bases to have a unique $P = M_{\mathcal{B}}^{\mathcal{E}}(I)$!
- **Change of basis**: The similarity action of $M_{\mathcal{B}}^{\mathcal{E}}(I)$ on $M_{\mathcal{B}}^{\mathcal{B}}(\varphi)$.
- Dummit and Foote (2004) proves that any two similar matrices represent the same linear transformation with respect to two different choices of bases.
- Example of similarity given.
- **Canonical forms**: The study of the simplest possible matrix representing a given linear transformation (and which basis to choose to realize it).
- We now move on to linear transformations on tensor products of vector spaces.
- Return to later.
- **Idempotent** (linear transformation): A linear transformation ψ satisfying $\psi^2 = \psi$.
  - Characterized in Exercise 11.2.11.

Section 11.3: Dual Vector Spaces

- **Dual space** (of a vector space): The space of linear transformations from V to F. *Denoted by* $\boldsymbol{V^*}$.
- **Linear functional**: An element of V^*.
- **Dual basis** (to a basis of V): The basis related to a basis $\{v_1, \dots, v_n\}$ of V by

$$v_i^*(v_j) = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

  for $1 \leq j \leq n$. *Denoted by* $\boldsymbol{\{v_1^*, \dots, v_n^*\}}$.

- The dual basis to a basis of V is a basis of V^*.

  Proposition 11.18. With notations as above, $\{v_1^*, \dots, v_n^*\}$ is a basis of V^*. In particular, if V is finite dimensional, then V^* has the same dimension as V.

  Proof. Given. □

- If V is infinite dimensional, then $\dim V < \dim V^*$.
- **Algebraic** (dual space to V): The dual space V^* taken for V of arbitrary dimension.
- If V has additional structure (e.g., a topology), we can get other types of dual spaces, such as the following.
- **Continuous** (dual of V): A dual of V in which the linear functionals must be continuous.
- Example.
  1. Let $V = C([a,b], \mathbb{R})$.
     - If $a < b$, then V is infinite dimensional.
     - For each $g \in V$, the function $\varphi_g : V \to \mathbb{R}$ defined by

$$\varphi_g(f) = \int_a^b f(t)g(t)\,\mathrm{d}t$$

       is a linear functional on V.
- **Double dual** (of V): The dual of V^*. *Also known as* **second dual**. *Denoted by* $\boldsymbol{V^{**}}$.
- For finite dimensional V, $\dim V = \dim V^{**}$ and hence $V \cong V^{**}$.
  - There is a **natural** (i.e., basis independent/coordinate free) isomorphism.
    - More detail on this is given.
  - This is different for infinite dimensional V, as per the above.
- Existence of a natural map $V \to V^{**}$.

  Theorem 11.19. There is a natural injective linear transformation from V to V^{**}. If V is finite dimensional, then this linear transformation is an isomorphism.

  Proof. Given. □

- $\boldsymbol{\varphi^*}$: The induced function from $W^* \to V^*$ defined by

$$f \mapsto f \circ \varphi$$

  - This is just the **pullback** or **dual map**.

- Pullback: Linearity and matrix.

  Theorem 11.20. With notations as above, φ^* is a linear transformation from W^* to V^* and $M_{\mathcal{E}^*}^{\mathcal{B}^*}(\varphi^*)$ is the transpose of the matrix $M_{\mathcal{B}}^{\mathcal{E}}(\varphi)$.

  Proof. Given. □

- A partial statement of the rank-nullity theorem.

  Corollary 11.21. For any matrix A, the row rank of A equals the column rank of A.

  Proof. Given. □

- **Annihilator** (of S in V): The set of all $v \in V$ for which $f(v) = 0$ for all $f \in S \subset V^*$. *Denoted by* **Ann(S)**. *Given by*

$$\text{Ann}(S) = \{v \in V : f(v) = 0 \ \forall \ f \in S\}$$

7.8 Chapter 12: Modules over Principal Ideal Domains

From Dummit and Foote (2004).

Introduction

- Goal of this chapter.
  - Characterize the structure of finitely generated modules over PIDs.
  - This is an example of the ideal structure of a ring being reflected in the structure of its modules.
- **Fundamental Theorem of Finitely Generated Abelian Groups**: Any finitely generated abelian group is isomorphic to the direct sum of cyclic abelian groups (either $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ for some $n > 0$).
  - See Chapter 5.
- Applying this theorem when the PID is $\mathbb{Z}$ proves the Fundamental Theorem of Finitely Generated Abelian Groups.
  - The relation: Abelian groups are $\mathbb{Z}$-modules!
  - In the language of modules, this theorem states that "any finitely generated $\mathbb{Z}$-module is the direct sum of modules of the form $\mathbb{Z}/I$ where I is an ideal of $\mathbb{Z}$" (Dummit & Foote, 2004, p. 456).
    - We will also need a uniqueness statement for the direct sum.
- Applying this theorem when the PID is $F[X]$ leads to the rational and Jordan canonical forms for a matrix.
  - Recall that $F[X]$-modules require the specification of a linear transformation T.
  - Thus, applying this theorem to $F[X]$-modules can be walked backwards to obtain information about T.
  - The Jordan canonical form requires that F contains all eigenvalues of T; the rational canonical form does not.
  - Similarity will somehow be involved here.
- Example of JCF.
  - Mirrors the example from the end of Section 11.2.

- Section 12.1 gives some definitions and then states and proves the Fundamental Theorem of Finitely Generated Modules over a PID.
- Section 12.2-12.3 cover the applications of the Fundamental Theorem to canonical forms, specifically the rational and Jordan ones, respectively.
- The application to abelian groups mentioned above will not be discussed further herein (it was discussed in Chapter 5).
- Note that an alternate and computationally useful proof of the Fundamental Theorem valid for Euclidean Domains (so also $\mathbb{Z}$ and $F[X]$ in particular) along the lines of row and column operations is outlined in Exercises 16-22 of Section 12.1.

Section 12.1: The Basic Theory

- **Ascending chain condition of submodules**: The condition pertaining to a module M that no infinite increasing chain of submodules $N_i \subset M$ exists, that is, whenever

$$N_1 \subset N_2 \subset \cdots$$

  is an increasing chain of submodules of M, then there is a positive integer m such that for all $k \geq m$, $M_k = M_m$ (so the chain becomes stationary at stage m: $M_m = M_{m+1} = \cdots$). *Also known as* **ACC of submodules**.
  - There exist analogous notions of the ACC on right and two-sided ideals in a (possibly noncommutative) ring R.
- **Noetherian** (R-module): A left R-module M that satisfies that ACC on submodules.
- **Noetherian** (ring): A ring R that is Noetherian as a left module over itself.
- Characterizing Noetherian modules.

  Theorem 12.1. Let R be a ring and let M be a left R-module. Then TFAE.

  1. M is a Noetherian R-module.
  2. Every nonempty set of submodules of M contains a maximal element under inclusion.
  3. Every submodule of M is finitely generated.

  Proof. Given. □

- PIDs are Noetherian.

  Corollary 12.2. If R is a PID, then every nonempty set of ideals of R has a maximal element and R is a Noetherian ring.

  Proof. Given. □

- Recall that finitely generated modules need not have finitely generated submodules; see Example 2 from Section 10.3.
  - Thus, the Noetherian condition is stronger in general than the finite generation condition.
- A useful linear dependence result.

  Proposition 12.3. Let R be an integral domain, and let M be a free R-module of rank $n < \infty$. Then any $n+1$ elements of M are R-linearly dependent, i.e., for any $y_1, \ldots, y_{n+1} \in M$, there are elements $r_1, \ldots, r_{n+1} \in R$, not all zero, such that

$$r_1 y_1 + \cdots + r_{n+1} y_{n+1} = 0$$

Proof. Given. □

- **The torsion submodule** (of M): The submodule of a R-module M, where R is an integral domain, equal to all elements of M such that $rx = 0$ for some nonzero $r \in R$. *Denoted by* $\mathbf{Tor}(\boldsymbol{R})$. *Given by*

$$\text{Tor}(M) = \{x \in M : rx = 0 \text{ for some nonzero } r \in R\}$$

- **A torsion submodule** (of M): Any submodule of $\text{Tor}(M)$.
- **Torsion module**: A module M for which $\text{Tor}(M) = M$.
- **Torsion-free** (module): A module M for which $\text{Tor}(M) = 0$.
- **Annihilator** (of a submodule): The ideal of R defined as follows, where M is an R-module and N is the submodule of M in question. *Denoted by* $\mathbf{Ann}(\boldsymbol{N})$. *Given by*

$$\text{Ann}(N) = \{r \in R : rn = 0 \ \forall \ n \in N\}$$

  - If N is not a torsion submodule of M, then $\text{Ann}(N) = 0$.
  - $N \subset L$ submodules of M implies $\text{Ann}(L) \subset \text{Ann}(N)$.
  - R a PID, $N \subset L \subset M$, $\text{Ann}(N) = (a)$, and $\text{Ann}(L) = (b)$ implies that $a \mid b$.
    - This follows from Lagrange's theorem when $R = \mathbb{Z}$.
- **Rank** (of a module): The maximum number of R-linearly independent elements of M.
  - Proposition 12.3 states that for a free R-module M over an integral domain, the rank of a submodule is bounded by the rank of M.
  - This definition agrees with the previous one over fields: If $R = F$ is a field, then the rank of any R-module M is the dimension of M since any maximal set of F-linearly independent elements is a basis.
  - Note that general modules over integral domains need not have a basis, i.e., need not be free even if they are torsion-free.
- Relating free modules, PIDs, rank, and generators.

Theorem 12.4. Let R be a PID, let M be a free R-module of finite rank n, and let N be a submodule of M. Then...

1. N is free of rank $m \leq n$;
2. There exists a basis $y_1, \dots, y_n$ of M such that $a_1y_1, \dots, a_my_m$ is a basis of N where $a_1, \dots, a_m$ are nonzero elements of R that satisfy the divisibility relations

$$a_1 \mid a_2 \mid \cdots \mid a_m$$

Proof. Given. □

- Warm-up to the Fundamental Theorem: The special case of *cyclic* (not finitely generated) R-modules.
  - Let C be a cyclic R-module. Then $C = Rx$ for some $x \in C$.
  - Define $\pi : R \to C$ by $\pi(r) = rx$.
  - π is surjective by the assumption that $C = Rx$. Thus, by the FIT, $R/\ker\pi \cong C$.
  - We are assuming that R is a PID, so we must have $\ker\pi = (a)$ for some $a \in R$. In particular, note that $(a) = \text{Ann}(C)$ by definition.
  - Essentially, $C \cong R/(a)$, and the classification is complete.

- We now treat the broader case of finite generation.

  Theorem 12.5 (Fundamental Theorem, Existence: Invariant Factor Form). Let R be a PID and let M be a finitely generated R-module. Then...

  1. M is isomorphic to the direct sum of finitely many cyclic modules. More precisely,
  $$M \cong R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$$
  for some integer $r \geq 0$ and nonzero elements $a_1, \dots, a_m \in R$ which are not units in R and which satisfy the divisibility relations
  $$a_1 \mid a_2 \mid \cdots \mid a_m$$
  2. M is torsion-free iff M is free.
  3. In the decomposition in part (1),
  $$\mathrm{Tor}(M) \cong R/(a_1) \oplus \cdots \oplus R/(a_m)$$
  In particular, M is a torsion module iff $r = 0$ and in this case, the annihilator of M is the ideal (a_m).

  Proof. Given. □

- We will shortly prove that the decomposition in Theorem 12.5(1) is unique; this proof will rely heavily on the divisibility condition.
- **Free rank**: The integer r in Theorem 12.5. *Also known as* **Betti number**.
- **Invariant factors**: The elements $a_1, \dots, a_m \in R$ in Theorem 12.5.
- Applying the Chinese Remainder Theorem allows us to decompose $R/(a)$ further (and to do so uniquely).
  - This gives M as the direct sum of cyclic modules whose annihilators are as simple as possible.
- The above idea is summarized by the following theorem.

  Theorem 12.6 (Fundamental Theorem, Existence: Elementary Divisor Form). Let R be a PID and let M be a finitely generated R-module. Then M is the direct sum of a finite number of cyclic modules whose annihilators are either (0) or are generated by powers of primes in R, i.e.,
  $$M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_t^{\alpha_t})$$
  where $r \geq 0$ is an integer and $p_1^{\alpha_1}, \dots, p_t^{\alpha_t}$ are positive powers of (not necessarily distinct) primes in R.

- **Elementary divisor**: A prime power $p_i^{\alpha_i}$ (defined up to multiplication by units in R), where R is a PID and M is a finitely generated R-module as in Theorem 12.6.
- Grouping together all cyclic factors corresponding to the same prime p_i shows that M can be written as a direct sum $M = N_1 \oplus \cdots \oplus N_n$ where N_i consists of all the elements of M which are annihilated by some power of the prime p_i.
- Summarizing the above idea.

  Theorem 12.7 (The Primary Decompostion Theorem). Let R be a PID and let M be a nonzero torsion R-module (not necessarily finitely generated) with nonzero annihilator a. Suppose the factorization of a into distinct prime powers in R is
  $$a = up_1^{\alpha_1} \cdots p_n^{\alpha_n}$$

and let $N_i = \{x \in M : p_i^{\alpha_i} x = 0\}$ $(1 \leq i \leq n)$. Then N_i is a submodule of M with annihilator $p_i^{\alpha_i}$ and is the submodule of M of all elements annihilated by some power of p_i. In particular, we have

$$M = N_1 \oplus \cdots \oplus N_n$$

If M is finitely generated, then each N_i is the direct sum of finitely many cyclic modules whose annihilators are divisors of $p_i^{\alpha_i}$.

Proof. Given. □

- ***p_i*-primary component** (of M): The submodule of M of all elements annihilated by some power of p_i.
- We now prove the uniqueness statement of the Fundamental theorem.

Lemma 12.8. Let R be a PID and let p be a prime in R. Let F denote the field $R/(p)$.

1. Let $M = R^r$. Then $M/pM \cong F^r$.
2. Let $M = R/(a)$ where a is a nonzero element of R. Then

$$M/pM \cong \begin{cases} F & p \mid a \\ 0 & p \nmid a \end{cases}$$

3. Let $M = R/(a_1) \oplus \cdots \oplus R/(a_k)$ where each a_i is divisible by p. Then $M/pM \cong F^k$.

Proof. Given. □

Theorem 12.9 (Fundamental Theorem, Uniqueness)**.** Let R be a PID.

1. Two finitely generated R-modules M_1 and M_2 are isomorphic iff they have the same free rank and the same list of invariant factors.
2. Two finitely generated R-modules M_1 and M_2 are isomorphic iff they have the same free rank and the same list of elementary divisors.

Proof. Given. □

- Further classification.

Corollary 12.10. Let R be a PID and let M be a finitely generated R-module. Then...

1. The elementary divisors of M are the prime power factors of the invariant factors of M.

Proof. Given. □

- Restatement of Theorem 5.3 and 5.5.

Corollary 12.11 (The Fundamental Theorem of Finitely Generated Abelian Groups)**.**

1. 5.3: Let G be a finitely generated abelian group. Then...
   (a) $G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}$ for some integers $r, n_1, n_2, \dots, n_s$ satisfying the following conditions.
      (i) $r \geq 0$ and $n_j \geq 2$ for all j.
      (ii) $n_{i+1} \mid n_i$ for $1 \leq i \leq s-1$.
   (b) The expression in part (1) is unique, i.e., if $G \cong \mathbb{Z}^t \times \mathbb{Z}_{m_1} \times \cdots \times Z_{m_u}$, where t and $m_1, \dots, m_u$ satisfy a, b (i.e., $g \geq 0$, $m_j \geq 2$ for all j and $m_{i+1} \mid m_i$ for all $1 \leq i \leq u-1$), then $t = r$, $u = s$, and $m_i = n_i$ for all i.

2. 5.5: Let G be an abelian group of order $n > 1$ and let the unique factorization into distinct prime powers be

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

Then...

(a) $G \cong A_1 \times \cdots \times A_k$, where $|A_i| = p_i^{\alpha_i}$;

(b) For each $A \in \{A_1, \ldots, A_k\}$ with $|A| = p^\alpha$,

$$A \cong Z_{p^{\beta_1}} \times \cdots \times Z_{p^{\beta_t}}$$

with $\beta_1 \geq \cdots \geq \beta_t \geq 1$ and $\beta_1 + \cdots + \beta_t = \alpha$ (where t and $\beta_1, \ldots, \beta_t$ depend on i).

(c) The decompositions in part (1) and (2) are unique, i.e., if $G \cong B_1 \times \cdots \times B_m$ with the factors $|B_i| = p_i^{\alpha_i}$ for all i, then $B_i \cong A_i$ and B_i, A_i have the same invariant factors.

Proof. Given. □

- More on the relationship between elementary divisors and invariant factors can be found in Chapter 5.
- Eye ahead: If a finitely generated module is written as a direct sum of cyclic modules of the form $R/(a)$, then the ideals (a) which occur are not in general unique unless some additional conditions are imposed.
  - To decide whether two modules are isomorphic, we must first write them in *canonical* form.