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 an action $\cdot : A \times M \to M$ defined by $(a, m) \mapsto am$ (or $a \cdot m$ in the case of potential ambiguity) satisfying the following. *Also known as* **left module** (over A). *Constraints*

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

  (1) $a(v_1 + v_2) = av_1 + av_2$;

  (2) $(a + b)v = av + bv$;

  (3) $a(bv) = (ab)v$;

  (4) $1_A v = v$.
- We need the last one so that multiplication is nontrivial.

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

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

    is a ring with identity under componentwise addition and composition (i.e., $g \cdot f = g \circ f$).
  - $\text{End}(M)$ is formally defined in Dummit and Foote (2004) at this point!
- 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 is a (left) A-module for all $i \in I$ an indexing set, then the product $\prod_{i \in I} M_i$ is also an A-module.
     - The binary operation obeys the product topology: If we denote an element of $\prod_{i\in I} M_i$ by $\prod_{i \in I} m_i$, then we define $\cdot$ by

       $$a \cdot \left(\prod_{i \in I} m_i \right) = \prod_{i \in I} (am_i)$$
  3. Special case of 2: 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 Example 2 under the same binary operation.
  4. Special case of 2: A^m is an A-module with $a(b_1, \dots, b_n) = (ab_1, \dots, ab_n)$.
     - These are considered in much greater depth in Dummit and Foote (2004).
- ***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

  $$T(a_1 v_1 + a_2 v_2) = a_1 T(v_1) + a_2 T(v_2)$$

  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 $a \in A$. Thus, we see that defining $T(1)$ is sufficient to define T.
  - In other words, there exists a unique $T : A \to M$ for all $v \in M$ such that $T(1) = v$
  - This is very related to linear algebra!
- Question: What are all linear transformations $T : A^n \to M$?
  - Suppose $e_1 = (1, 0, \dots, 0)$, $e_2 = (0, 1, 0, \dots, 0)$, etc. Then
  $$(a_1, \dots, a_n) = \sum_{i=1}^{n} a_i e_i$$
  - Therefore,
  $$T(a_1, \dots, a_n) = \sum_{i=1}^{n} a_i T e_i$$
  - Take any ordered n-tuple of elements in M; then given $v_1, \dots, v_n \in M$, there is a unique A-module homomorphism $T : A^n \to M$ such that $T(e_i) = v_i$ $(i = 1, \dots, n)$.
- **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.
  - Note that it suffices to use the bijectivity definition here, not the left and right inverse one.
- 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.

  See Proposition 10.3. □
- FIT: Let $\phi : M \to N$ be a module homomorphism. Then $\ker(\phi)$ is a submodule of M and $\operatorname{im}(\phi)$ is a submodule of N.

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

Figure 6.1: First isomorphism theorem of modules.

  Proof. See Theorem 10.4(1). □
- Example: $A = \mathbb{Z}$ and $M = \mathbb{Z}/(27)$.
- For all of this module stuff, 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.
- Theorem: Let R be a PID. Then every R-submodule of R^n is isomorphic to R^m for some $0 \leq m \leq n$.

  Proof. We induct on n. For the base case $n = 1$, let M be an R-submodule of R^1. As a submodule of a ring, M is an ideal. Thus, since R is a PID, we know that $M = (b)$ for some $b \in R$. If $b = 0$, then we're done (pick $m = 0$). Thus, assume $b \neq 0$. Consider $T : R \to (b)$ given by $T(a) = ab$ for all $a \in A$. We have that T is onto. From the fact that R is an integral domain, we have that $0 = T(a) = ab$ implies that $a = 0$, so $\ker T = \{0\}$ and T is 1-1. Hence $M \cong R$.

  Now suppose inductively that we have proven the claim for $n-1$; we now seek to prove it for n. Define $i : R^{n-1} \hookrightarrow R^n$ by
  $$i(a_1, \dots, a_{n-1}) = (a_1, \dots, a_{n-1}, 0)$$
  Let M be an R-submodule of R^n. We know that $R^{n-1} \times \{0\} \hookrightarrow R^n$ and, by the induction hypothesis, that $M \cap (R^{n-1} \times \{0\}) \cong R^\ell$ for $0 \leq \ell \leq n-1$. Now define the ideal I as follows: Let $\pi(a_1, \dots, a_n) = a_n$, and let $I = \pi(M)$. Let $M' = \ker \pi$. $M/M' \cong I$. At this point, there are only two cases ($a = 0$ and $a = M$). □

- 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): $\{a_1b_1 + \cdots + a_nb_n : n \in \mathbb{N},\ a_1, \dots, a_n \in I,\ b_1, \dots, b_n \in J\}$.
- **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).
        - $a = q_0 b + r_0$, $b = q_1 r_0 + r_1$, $r_0 = q_2 r_1 + r_2$, $\dots$, $r_{n-1} = q_{n+1} r_n$.
- Wrap my head around an elementary statement of the Chinese Remainder Theorem!
- Stuff from OH on Monday.

6.5 Midterm

Questions and Answers

2/8: 1. *No proof required for this problem.*

How many homomorphisms $\phi : \mathbb{Z}[X]/(f) \to \mathbb{R}$ are there in each of the cases listed below?

General treatment.

My write-up: We know that all ring homomorphisms $\mathbb{Z}[X] \to \mathbb{R}$ are given by evaluation at some $a \in R$. (This follows somewhat from the universal property of a polynomial ring, since the value of any $p(X)$ under said ring homomorphism will depend on the value of X under it.) Let $\text{ev}_a : \mathbb{Z}[X] \to \mathbb{R}$ be the ring homomorphism such that $\text{ev}_a = \phi \circ \pi$. (That there is a *unique* ev_a corresponding to ϕ follows directly from the universal property of a quotient, since we have define $\text{ev}_a(f) = 0$.) We know that $\phi(\bar{f}) = 0$ and $\pi(f) = \bar{f}$; thus, $0 = \text{ev}_a(f) = f(a)$. It follows that the only possible values of a are the (real) roots of f. In particular, each distinct real root of f corresponds to a homomorphism $\phi : \mathbb{Z}[X]/(f) \to \mathbb{R}$.

Misc. note: $(f) \neq \ker(\text{ev}_a)$ in general: If $f = 10(X - 75)$, for instance, $(10(X-75)) = (f) \neq \ker(\text{ev}_a) = (X - 10)$. Nori's write-up: By the **universal property of a quotient**, giving a ring homomorphism $\phi : \mathbb{Z}[X]/(f) \to \mathbb{R}$ is equivalent to giving a ring homomorphism $\psi : \mathbb{Z}[X] \to \mathbb{R}$ such that $\psi(f) = 0$. Explicitly, for ψ to factor through $\mathbb{Z}[X]/(f)$, we need $(f) \subset \ker(\psi)$. To do so, it will suffice to check that $\psi(f) = 0$. Thus, up to this point, we have shown that

$$\text{Hom}_{\text{Ring}}(\mathbb{Z}[X]/(f), \mathbb{R}) = \{\psi : \mathbb{Z}[X] \to \mathbb{R} : \psi(f) = 0\}$$

However, we also know (by the universal property of the ring of fractions) that giving a ring homomorphism $\psi : \mathbb{Z}[X] \to \mathbb{R}$ is equivalent to choosing an element $r \in \mathbb{R}$. That is, if $\psi(X) = r$, then $\psi = \text{ev}_r$. Combining the last two results, we have that if ev_r is to factor through $\mathbb{Z}[X]/(f)$, then we need to know that $0 = \text{ev}_r(f) = f(r)$. Thus,

$$\text{Hom}_{\text{Ring}}(\mathbb{Z}[X]/(f), \mathbb{R}) = \{r \in \mathbb{R} : f(r) = 0\}$$

From this, we see that giving ring homomorphisms of a quotient ring can be thought of as being related to whether certain polynomial equations can be solved in the target. Moreover,

$$|\text{Hom}_{\text{Ring}}(\mathbb{Z}[X]/(f), \mathbb{R})| = |\{r \in \mathbb{R} : f(r) = 0\}|$$

allowing us to compute all desired results. □

(a) $f = X^2 + 1$.

Answer. f has $\boxed{0}$ distinct real roots. □

(b) $f = X^2 - 3$.

Answer. f has $\boxed{2}$ distinct real roots. □

(c) $f = X^3 - 7$.

Answer. f has $\boxed{1}$ distinct real roots. □

(d) $f = X(X+1)^2(X+2)^3$.

Answer. f has $\boxed{3}$ distinct real roots. □

2. *No proof required for this problem.*

   Recall the notation R_f: Given an integral domain R and a nonzero $f \in R$, we have the multiplicative subset $D = \{1, f, f^2, \dots\} \subset R$; R_f is then defined to be $D^{-1}R$.

   How many ring homomorphisms $\phi : \mathbb{Z}[X]_f \to \mathbb{F}_2$ are there? Here, $\mathbb{F}_2$ is the field of two elements. In each case, list the possible values of $\phi(X)$.

   General treatment.

   My write-up: By the universal property of rings of fractions, each $\psi : \mathbb{Z}[X] \to \mathbb{F}_2$ such that $\psi(D) \subset (\mathbb{F}_2)^\times$ corresponds to a unique $\phi : \mathbb{Z}[X]_f \to \mathbb{F}_2$ such that $\psi = \phi \circ \pi$. Thus, to characterize the ring homomorphisms ϕ, we need only characterize the ψ of the appropriate type. Let's start applying the constraints. To show that $\psi(D) \subset (\mathbb{F}_2)^\times = \{1\}$, it will suffice to show that $\psi(1) = 1$ and $\psi(f) = 1$. We have the former constraint by the definition of ψ as a ring homomorphism; the latter, however, is helpful. In particular, invoking the universal property of polynomial rings, we have that ψ is either ev_1 or ev_0, where the evaluation is carried out in $\mathbb{F}_2[X]$, i.e., we evaluate $\tilde{f} = \tilde{\pi}(f)$, where $\tilde{\pi} : \mathbb{Z}[X] \to \mathbb{F}_2[X]$ is a canonical surjection. This means that f must satisfy either $1 = \text{ev}_0(f) = \tilde{f}(0)$ or $1 = \text{ev}_1(f) = \tilde{f}(1)$ for any ϕ to exist; if it satisfies both, then two ϕ exist; no more than two ϕ may exist by the constraint of the universal property of polynomial rings.

   If $\text{ev}_i(f) = 1$ ($i = 0, 1$), then $\phi(X) = \text{ev}_i(X) = i$.

   Nori's write-up: Essentially mirrors mine, just with equations to make it all more concrete. The important given equations are

$$\text{Hom}(\mathbb{Z}[X]_f, R) \cong \{r \in R : f(r) \in R^\times\}$$
$$\text{Hom}(\mathbb{Z}[X]_f, \mathbb{F}_2) \cong \{r \in \mathbb{F}_2 : f(r) \in (\mathbb{F}_2)^\times\} = \{r \in \mathbb{F}_2 : f(r) = 1\}$$
$$0 \leq |\text{Hom}(\mathbb{Z}[X]_f, \mathbb{F}_2)| = |\{r \in \mathbb{F}_2 : f(r) = 1\}| \leq |\mathbb{F}_2| = 2$$

□

   (a) $f = X^2 + X + 1$.

   Answer. As written, $f = \tilde{f}$. Thus,

$$\tilde{f}(0) = f(0) = 0^2 +_2 0 +_2 1 = 1 \qquad \tilde{f}(1) = f(1) = 1^2 +_2 1 +_2 1 = 1$$

   Therefore, there are $\boxed{2}$ possible homomorphisms ϕ_0 and ϕ_1. Additionally, $\phi_0(X) = \text{ev}_0(X) = 0$ and $\phi_1(X) = \text{ev}_1(X) = 1$, so the possible values of $\phi(X)$ are $\boxed{0, 1}$. □

   (b) $f = X^2 - 13$.

   Answer. CliffsNotes version: $\tilde{f} = X^2 +_2 1$, so $\tilde{f}(0) = 1$ and $\tilde{f}(1) = 0$. Thus, there is only $\boxed{1}$ possible homomorphism ϕ, and the only possible value of $\phi(X)$ is $\boxed{0}$. □

   (c) $f = X^3 - 71$.

   Answer. Similar to part (b): $\tilde{f} = X^3 +_2 1$, $\tilde{f}(0) = 1$ and $\tilde{f}(1) = 0$. Thus, there is only $\boxed{1}$ possible homomorphism ϕ, and the only possible value of $\phi(X)$ is $\boxed{0}$. □

   (d) $f = X(X + 1)^2(X + 2)^3$.

   Answer. $\tilde{f}(0) = 0 \cdot_2 1^2 \cdot_2 0^3 = 0$, and $\tilde{f}(1) = 1 \cdot_2 0^2 \cdot_2 1^3 = 0$. Thus, there are $\boxed{0}$ possible homomorphisms ϕ. □

3. Let $f \in \mathbb{R}[X]$ be a polynomial of degree d such that $f(a_1) = \cdots = f(a_d) = 0$, where $a_1, \dots, a_d$ are d distinct real numbers. Prove that there are $g, h \in \mathbb{R}[X]$ such that $gf' + hf = 1$, where f' is the derivative of f.

Proof.

My write-up:[1] We have that

$$f = r(X - a_1) \cdots (X - a_d) \qquad\qquad f' = r \sum_{i=1}^{d} \prod_{\substack{j=1 \\ j \neq i}}^{d} (X - a_j)$$

for some unit $r \in \mathbb{R}[X]^\times = \mathbb{R}^\times = \mathbb{R} - \{0\}$, where decomposition of f follows straight from the given constraint, and the decomposition of f' comes from differentiating that of f using the d^{th}-order product rule. It follows that the only divisors of f are products of the factors in its decomposition; however, any one of these factors of degree 1 is *not* a divisor of f' since f' contains at least one term that will not contain it (by definition). Thus, if r is sufficiently big, $\gcd(f, f') = r$; otherwise, $\gcd(f, f') = 1$. In the latter case, we are done, and in the former case, we just need to divide the generated polynomials by r.

Nori's write-up: Since $\mathbb{R}[X]$ is a PID, Bezout's identity tells us that it will suffice to show that $\gcd_{\mathbb{R}[X]}(f, f') = 1$. As in my write up, we factor $f(X)$ into "irreducibles[2]" and seek to prove that $X - a_i$ does not divide f' for any i. That is, we need to prove that $f'(a_i) \neq 0$ for any i.

Since $f(a_i) = 0$ for all i, we can write $f(X) = (X - a_i)g(X)$ for any i. Since f has no repeated roots, we can assume that $g(a_i) \neq 0$. Taking the derivative of the previous expression, we see that

$$f'(X) = g(X) + (X - a_i)g'(X)$$

In particular,

$$f'(a_i) = g(a_i) + (a_i - a_i)g'(a_i) = g(a_i) \neq 0$$

Thus, f' does not have any $a_i \in \mathbb{R}$ as a root, so we're done. □

4. Let F be a field. Let $\phi : F[X, Y] \to F(X)$ be a homomorphism such that $\phi(g) = g$ for all $g \in F[X]$. Show that there is some nonzero $f \in F[X]$ such that $F[X]_f = \operatorname{im}(\phi)$.

Proof.

My write-up: We are given that $\phi(X) = X$; figuring out what $\phi(Y)$ is will fully characterize ϕ (and $\operatorname{im}(\phi)$ by extension). We know that $\phi(Y) \in F(X)$, so let $\phi(Y) = g/f$ where $f, g \in F[X]$, $f \neq 0$, and we take f, g to have $\gcd(f, g) = 1$. We now seek to put further constraints on g, f. We know that

$$\operatorname{im}(\phi) = \phi(F[X, Y]) = (\phi(X), \phi(Y)) = (X, \tfrac{g}{f})$$

Since $\gcd(f, g) = 1$, there exist $a, b \in F[X]$ such that $af + bg = 1$. Dividing both sides by f, we obtain

$$a + b\frac{g}{f} = \frac{1}{f}$$

Thus, since $a, b \in (X)$, $1/f = a + bg/f \in (X, g/f)$. Moreover, we know that $g/f = g \cdot 1/f$, so $g/f \in (X, 1/f)$. It follows that $(X, g/f) = (X, 1/f)$. But this is just $F[X]_f$, as desired.

Nori's write-up: Essentially the same as mine; Nori just did it more from the perspective of a bidirectional inclusion proof. There's also the interesting step $1/f = \phi(a + bY)$ to imply that $1/f \in \operatorname{im}(\phi)$. □

[1] Nori did give full credit for this, but his write-up is probably better, regardless.

[2] Clearly, Nori has no problem with us identifying monomials as irreducibles without proof.

Retrospective

- It is not enough to just have a general understanding of most things in this course; I need a deep knowledge of *everything* to guarantee success on exams.
- Theorem (Universal Property of the Quotient): Let $H \triangleleft G$, and let $\phi : G \to K$ be a group homomorphism such that $H \subset \ker \phi$. Then there is a unique homomorphism $\tilde{\phi} : G/H \to K$ such that $\phi = \tilde{\phi} \circ \pi$.
  - "The universal property of the quotient is an important tool in constructing group maps: To define a map out of a quotient group G/H, define a mpa out of G which maps H to the identity" (Ikenaga, 2018, p. 2).
  - This is also Nori's pet lemma from Dummit and Foote (2004, p. 100): φ is well-defined on G/N iff $N \leq \ker \Phi$, where $\Phi : G \to H$ and $\phi : G/N \to N$.
- A note on efficiency of evaluation in Problem 2(4).
  - When evaluating $\tilde{f}(x)$, we can stop as soon as we find a zero in this case because this zero will make the whole product 0; for example, when computing $\tilde{f}(0)$, as soon as we saw that the first term was 0, we would know that $\tilde{f}(0) = 0$; when computing $\tilde{f}(1)$, as soon as we saw that the second term was 0, we would know that $\tilde{f}(1) = 0$.
- The strategy used in Problem 4 of defining variables shows up repeatedly in challenge questions!
- **Bezout's identity**: Let $a, b \in \mathbb{Z}$ have $\gcd(a, b) = d$. Then there exist $x, y \in \mathbb{Z}$ such that $ax + by = d$.
  - Bezout's identity holds in Bezout domains (by definition) and in PIDs.

6.6 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.
- Picking up with the proof of the theorem from last time.
- 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 $\text{im}(\varphi)$ 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 ($\text{im}(\varphi) = \{0\}$ and otherwise). Suppose first that $\text{im}(\varphi) = \{0\}$. Then $M' = M$. Now suppose that $\text{im}(\varphi) \neq \{0\}$. By hypothesis, R is a PID. In particular, the ideal $\text{im}(\varphi)$ is principal, i.e., that there exists $0 \neq b \in R$ such that $\text{im}(\varphi) = Rb$. 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[3]. ...

  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, $a_h \in \text{im}(\varphi) = Rb$. 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: $M \cong M' \oplus R \cong R^\ell \oplus R = R^{\ell+1}$. □

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

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

- 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 $\varphi(m' + ae) = 0$, $\varphi(m') + a = 0$, $m' = 0$. □

- 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.

6.7 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 $p = 3$?

6.8 Chapter 10: Introduction to Module Theory

From Dummit and Foote (2004).

A Word on Module Theory

2/12:

- Emmy Noether led the way in demonstrating the power and elegance of modules at the beginning of the 20th century.
- "Vector spaces are just special types of modules which arise when the underlying ring is a field" (Dummit & Foote, 2004, p. 336).
- Modules are also very much like group actions, with the underlying structure being a ring as a "scalar field" acting on a set of "vectors."
- Modules are **representation objects** for rings.
- **Representation object**: An object on which something acts.
- End goal: Reveal how the structure of a ring (and in particular, the structure of its ideals) is reflected by the structure of modules and vice versa.
   - Analogous to studying groups via their permutation representations.

Section 10.1: Basic Definitions and Examples

- Definition of a **left *R*-module**.
   - If R is commutative, defining $mr := rm$ makes M into a right R-module. We need R to be commutative so that we still have $a(bv) = (ab)v$.
- **Unital** (module): A module such that $1m = m$ for all $m \in M$.
   - By Nori's definition, all modules we will consider are unital modules. Dummit and Foote (2004) actually does the same here to avoid pathologies.
- When R is a field, the axioms for an R-module are precisely the same as those for a vector space over F.
- Definition of an ***R*-submodule**.
   - Naturally, submodules are just subsets that are themselves modules under the restricted operations.
- Every R-module M has M and 0 as submodules.
- **Trivial submodule**: The submodule 0.
- Examples.
   1. $(R, +)$ is a left R-module for any ring $(R, +, \cdot)$ under $\cdot$.

- Vector space analogy: This formalizes the notion that F is a one-dimensional vector space over itself.
- Submodules: The left ideals of R.
- If R is not commutative, the left and right module structures may be different.

2. Every vector space over F is an F-module and vice versa.
   - Defines **affine $\boldsymbol{n}$-space** and notes that it's a vector space of dimension n over F the same way that **Euclidean $\boldsymbol{n}$-space** is.
3. The **free module of rank $\boldsymbol{n}$** over R.
   - Free modules have the same universal property as **free groups** from Section 6.3.
   - Discussion of direct product of R-modules is coming.
   - Submodules of R^n include those with arbitrary elements in the i^{th} component and zeroes elsewhere.
4. Groups can be modules under multiple rings.
   - If S is a subring of R, R is both an R-module and an S-module.
   - For instance, $\mathbb{R}$ is an $\mathbb{R}$-module, a $\mathbb{Q}$-module, and a $\mathbb{Z}$-module.
5. Quotient-ring modules.
   - Suppose I **annihilates** M.
   - Then M is an (R/I)-module: Define $\cdot : (R/I) \times M \to M$ by
   $$(r+I)\cdot m = rm$$
   - Specific example: If I is maximal and annihilates M, then M is a vector space over the field R/I.

- **Affine $\boldsymbol{n}$-space** (over F): The vector space defined as follows. *Denoted by* $\boldsymbol{F^n}$. *Given by*
$$F^n = \{(a_1,\dots,a_n) : a_i \in F \ \forall\ i\}$$
with
$$\begin{aligned}(a_1,\dots,a_n) + (b_1,\dots,b_n) &= (a_1+b_1,\dots,a_n+b_n)\\ \alpha(a_1,\dots,a_n) &= (\alpha a_1,\dots,\alpha a_n)\end{aligned}$$

- **Euclidean $\boldsymbol{n}$-space**: The vector space defined as follows. *Denoted by* $\mathbb{R}^{\boldsymbol{n}}$. *Given by*
$$\mathbb{R}^n = \{(a_1,\dots,a_n) : a_i \in \mathbb{R} \ \forall\ i\}$$
with analogous addition and scalar multiplication to the above.

- **Free module of rank $\boldsymbol{n}$** (over R): The module defined as follows. *Denoted by* $\boldsymbol{R^n}$. *Given by*
$$R^n = \{(a_1,\dots,a_n) : a_i \in R \ \forall\ i\}$$
with analogous addition and scalar multiplication to the above.

- **Annihilator** (of M): A two-sided ideal I of a ring R corresponding to an R-module M such that $am = 0$ for all $a \in I$ and $m \in M$.

2/18: - Example: $\mathbb{Z}$-modules.
  - These are critical to the Fundamental Theorem of Finitely Generated Abelian Groups.
  - Every abelian group is a $\mathbb{Z}$-module.

- Let $(A,+)$ be any abelian group. We can make A into a $\mathbb{Z}$-module by defining $\cdot : \mathbb{Z}\times A \to A$ by
$$n\cdot a = \begin{cases} \underbrace{a+\cdots+a}_{n \text{ times}} & n>0\\ 0 & n=0\\ \underbrace{-a-\cdots-a}_{n\text{ times}} & n<0 \end{cases}$$
for all $n\in\mathbb{Z}$ and $a\in A$, where 0 above denotes the identity of the additive group A.
- The module axioms actually show that the above is the *only* possible action of $\mathbb{Z}$ on A.

- Conversely, every $\mathbb{Z}$-module is also an abelian group.
- Takeaways.
  - It follows that "$\mathbb{Z}$-modules are the same as abelian groups" (Dummit & Foote, 2004, p. 339).
  - Similarly, "$\mathbb{Z}$-submodules are the same as subgroups" (Dummit & Foote, 2004, p. 339).
- Note: Checking that the exponential notation satisfies the usual laws of exponents in a cyclic group $\langle a\rangle$ is equivalent to checking the $\mathbb{Z}$-module axioms.
- $\mathbb{Z}$ is commutative $\Rightarrow$ left and right $\mathbb{Z}$-modules are equivalent.
- $\mathbb{Z}$-modules may have zero divisors (in contrast to vector spaces).
  - In particular, if A is an abelian group of order m, then A is a module over $\mathbb{Z}/m\mathbb{Z}$.
- If A is an abelian group and $p\in\mathbb{Z}$ is a prime such that $px=0$ for all $x\in A$, then A is a $\mathbb{Z}/p\mathbb{Z}$-module.
  - This means that A can be considered to be a vector space over the field $\mathbb{Z}/p\mathbb{Z}$.
  - Example: The Klein 4-group is a 2-dimensional vector space over $\mathbb{Z}/2\mathbb{Z}$.
  - Such groups are the elementary abelian p-groups discussed last quarter.

- Example: $F[X]$-modules.
  - These are critical to canonical forms of matrices.
  - Defining $F[X]$-modules.
    - Let F be a field, X be an indeterminate, V be a vector space over F, and $T:V\to V$ be a linear transformation.
    - Preliminaries: Note that V is an F-modules, and recall that T^n denotes the composition of T with itself n times and addition and scalar multiplication of linear transformations is defined pointwise.
    - In an $F[X]$-module, $F[X]$ acts on V. Thus, we now define the action of $p(X)=a_nX^n+\cdots+a_0\in F[X]$ on $v\in V$. In particular, we let
    $$p(X)v=(a_nT^n+\cdots+a_0)(v)=a_nT^n(v)+\cdots+a_0v$$
    - Alternate definition: X acts on V as T, and we extend this action to $F[X]$ in a natural way.
    - Alternate definition: All $f\in F$ act on V by left multiplication, and we extend this action to $F[X]$.
      - In particular, notice that F is a subring of $F[X]$ and that the action of $F\subset F[X]$ on V is identical to the action of F on V when V is viewed as an F-module.
  - The action of $F[X]$ on V depends on T, so there are many different $F[X]$-module structures on V in general.
    - Specific examples given.
  - The given construction of an $F[X]$ module in fact describes *all* $F[X]$-modules.
    - In particular, an $F[X]$-module is a vector space together with a linear transformation which specifies the action of X.

    - Thus, there is a bijection between the collection of $F[X]$-modules and the collection of pairs V, T.
    - This is getting very close to the universal property of a polynomial ring!
  - $F[X]$-submodules.
    - Let W be an $F[X]$-submodule of V.
    - W must be an F-submodule of V, i.e., a vector subspace.
    - X must send $W \to W$, i.e., W must be an **invariant** subspace under the action of X.
    - It follows from the T-invariance of W that W is $p(T)$-invariant for any $p(X) \in F[X]$.
    - Takeaway: The $F[X]$-submodules of V are precisely the T-stable subspaces of V.
    - Rephrasing this takeaway as a bijection.
- ***T*-stable** (subspace): A vector subspace U of V such that $T(U) \subset U$. *Also known as* ***T*-invariant**.

2/12:

- M may have many different R-module structures, even for the same R.
  - These correspond to changes in $\cdot$.
- Determining if a subset of a module is a submodule.

  Proposition 10.1 (The Submodule Criterion)**.** *Let R be a ring and let M be an R-module. A subset N of M is a submodule if and only if*

  1. $N \neq \emptyset$;
  2. $x + ry \in N$ *for all* $r \in R$, $x, y \in N$.

  Proof. Given. □

- ***R*-algebra**: A ring A together with a ring homomorphism $f : R \to A$ such that the subring $f(R)$ of A is contained in the center of A, where R is a commutative ring.
- More on R-algebras (return to later).

Section 10.2: Quotient Modules and Module Homomorphisms

- Definition of an ***R*-module homomorphism**, ***R*-module isomorphism**, **kernel**, and **image**.
  - Naturally, module homomorphisms respect the *module* structure of M, N.
- $\mathbf{Hom}_{\boldsymbol{R}}\boldsymbol{(M, N)}$: The set of all R-module homomorphisms from M into N.
- Kernels and images are submodules.
  - Prove this with Proposition 10.1
- Examples.
  1. Module homomorphisms and ring homomorphisms are distinct.
     - Example: The $\mathbb{Z}$-module homomorphism $x \mapsto 2x$ is not a ring homomorphism since $1 \not\mapsto 1$.
  2. The projection map $\pi_i : R^n \to R$ is an R-module homomorphism.
  3. **Linear transformations**.
  4. $\mathbb{Z}$-module homomorphisms are the same as abelian group homomorphisms.
     - This is because the action of integers on any $\mathbb{Z}$-module amounts to adding or subtracting within the additive abelian group.
  5. Any R-module homomorphism from N to M (where $NI = MI = 0$ for an annihilator I) is a homomorphisms of (R/I)-modules.

  - More on $GL(A)$ (return to later).

- **Linear transformation**: An F-module homomorphism.
- Turning a set of maps into a group and/or ring (see Q1.14).

  Proposition 10.2. Let M, N, L be R-modules.

  1. A map $\varphi : M \to N$ is an R-module homomorphism if and only if $\varphi(rx + y) = r\varphi(x) + \varphi(y)$ for all $x, y \in M$ and $R \in R$.
  2. Let $\varphi, \psi \in \text{Hom}_R(M, N)$. Define $\varphi + \psi$ by
  $$(\varphi + \psi)(m) = \varphi(m) + \psi(m)$$
  for all $m \in M$. Then $\varphi + \psi \in \text{Hom}_R(M, N)$ and with this operation, $\text{Hom}_R(M, N)$ is an abelian group.
  If R is a commutative ring, then for $r \in R$, define $r\varphi$ by
  $$(r\varphi)(m) = r(\varphi(m))$$
  for all $m \in M$. Then $r\varphi \in \text{Hom}_R(M, N)$ and with this action of the commutative ring R, the abelian group $\text{Hom}_R(M, N)$ is an R-module.
  3. If $\varphi \in \text{Hom}_R(L, M)$ and $\psi \in \text{Hom}_R(M, N)$, then $\psi \circ \varphi \in \text{Hom}_R(L, N)$.
  4. With addition as above and multiplication defined as function composition, $\text{Hom}_R(M, M)$ is a ring. When R is commutative, $\text{Hom}_R(M, M)$ is an R-algebra.

  Proof. Given. □

- **Endomorphism ring** (of M): The ring defined as follows. *Denoted by* $\mathbf{End}_{\boldsymbol{R}}\boldsymbol{(M)}$, $\mathbf{End}\boldsymbol{(M)}$. *Given by*
$$\text{End}(M) = (\text{Hom}_R(M, M), +, \circ)$$
- **Endomorphism**: An element of $\text{End}(M)$.
  - When R is commutative, there is a natural map $R \to \text{End}_R(M)$ which sends every $r \in R$ to the endomorphism defined by left multiplication by r.
  - More on $\text{End}(M)$ in the context of algebras (return to later).
- Every submodule N of an R-module M induces a quotient module M/N.

  Proposition 10.3. Let R be a ring, let M be an R-module, and let N be a submodule of M. The (additive abelian) quotient group M/N can be made into an R-module by defining an action of element of R by
  $$r(x + N) = (rx) + N$$
  for all $r \in R$ and $x + N \in M/N$. The natural projection map $\pi : M \to M/N$ defined by $\pi(x) = x + N$ is an R-module homomorphism with kernel N.

  Proof. To prove that M/N is an R-module, it will suffice to show that it is an abelian group, that the action $\cdot$ defined on it above is well-defined, and that said action satisfies the four axioms. Let's begin.

  Since M is an abelian group under $+$, N is abelian (hence normal) and thus the (additive) quotient group $(M/N, +)$ is defined and is abelian.

  To confirm that $\cdot$ is well-defined, it will suffice to demonstrate that if $x + N = y + N$, then $r(x + N) = r(y + N)$. Pick $x, y \in M$ arbitrary but such that $x + N = y + N$. It follows that $x - y \in N$. Thus, since N is a submodule, $rx - ry = r(x - y) \in N$. Consequently,
  $$rx + N = ry + N$$
  $$r(x + N) = r(y + N)$$

as desired.

Since the action of R on M/N is "compatible" with the action of r on M (see subsequent example), the four axioms may be easily, procedurally checked. For example, axiom 3 may be confirmed as follows: Let $a,b \in R$ and $x+N \in M/N$ be arbitrary. Then by consecutive applications of definitions, we have that

$$\begin{aligned}(ab)(x+N) &= abx+N\\ &= a(bx+N)\\ &= a(b(x+N))\end{aligned}$$

as desired.

This concludes the proof of the first claim.

To prove that π is a module homomorphism, it will suffice to show that it is a group homomorphism and commutes with scalar multiplication. Treating $M, M/N$ purely as groups, we may recall from group theory that π is a group homomorphism. With respect to the other condition, we have for all $a \in R$ and $m \in M$ that

$$\begin{aligned}\pi(am) &= am+N\\ &= a(m+N)\\ &= a\pi(m)\end{aligned}$$

as desired.

The fact that $\ker\pi = N$ follows from group theory. □

- Note that Proposition 10.3 makes intuitive sense since N (as an abelian group) is a normal subgroup of M. All that we needed to do above was confirm the module parts of the definition.
- **Sum** (of 2 submodules): The submodule defined as follows, where $A,B \subset M$ are submodules. *Denoted by* $\boldsymbol{A+B}$. *Given by*
$$A+B = \{a+b : a \in A,\ b \in B\}$$
- $A+B$ is the smallest submodule containing both A,B, as expected.
- We conclude by restating the isomorphism theorems for modules.

Theorem 10.4 (Isomorphism Theorems)**.**

1. (The First Isomorphism Theorem for Modules) Let M,N be R-modules and let $\varphi : M \to N$ be an R-module homomorphism. Then $\ker\varphi$ is a submodule of M and $M/\ker\varphi \cong \varphi(M)$.
2. (The Second Isomorphism Theorem) Let A,B be submodules of the R-module M. Then $(A+B)/B \cong A/(A\cap B)$.
3. (The Third Isomorphism Theorem) Let M be an R-module, and let A,B be submodules of M with $A \subset B$. Then $(M/A)/(B/A) \cong M/B$.
4. (The Fourth or Lattice Isomorphism Theorem) Let N be a submodule of the R-module M. There is a bijection between the submodules of M which contain N and the submodules of M/N. The correspondence is given by $A \longleftrightarrow A/N$ for all $A \supset N$. This correspondence commutes with the processes of taking sums and intersections (i.e., is a lattice isomorphism between the lattice of submodules of M/N and the lattice of submodules of M which contain N).

Proof. Not given; see the Exercises. □

Section 10.3: Generation of Modules, Direct Sums, and Free Modules

2/16:
- **Sum** (of n submodules): The set of all finite sums of elements from the submodules $N_1, \dots, N_n$ of the R-module M. *Denoted by* $\boldsymbol{N_1 + \cdots + N_n}$ *Given by*

$$N_1 + \cdots + N_n = \{a_1 + \cdots + a_n : a_i \in N_i \ \forall \ i\}$$

- **Submodule of $\boldsymbol{M}$ generated by $\boldsymbol{A}$**: The submodule of an R-module M equal to the set of all finite sums of elements from some subset $A \subset M$, each of which may be left-multiplied by an element of R. *Denoted by* $\boldsymbol{RA}$. *Given by*

$$RA = \{r_1a_1 + \cdots + r_ma_m : r_1, \dots, r_m \in R, \ a_1, \dots, a_m \in A, \ m \in \mathbb{Z}^+\}$$

  - Convention: $RA = \{0\}$ if $A = \emptyset$.
  - If $A = \{a_1, \dots, a_n\}$ is finite, we do not write RA but write $\boldsymbol{Ra_1 + \cdots + Ra_n}$.
- **Set of generators** (for N): Any set A such that $N = RA$. *Also known as* **generating set**.
- **Finitely generated** (submodule): A submodule N of M for which there exists a finite subset $A \subset M$ such that $N = RA$.
- **Cyclic** (submodule): A submodule N of M for which there exists an element $a \in M$ such that $N = Ra$.
- $N_1 + \cdots + N_n$ is the submodule generated by the set $N_1 \cup \cdots \cup N_n$.
  - $N_1 + \cdots + N_n$ is also the smallest submodule containing each N_i.
  - If $N_1, \dots, N_n$ are generated by $A_1, \dots, A_n$, respectively, then $N_1 + \cdots + N_n$ is generated by $A_1 \cup \cdots \cup A_n$.
- When R is commutative, we often write AR or aR as we have been with $n\mathbb{Z}$.
- **Minimal set of generators** (for a finitely generated submodule): Any set A of generators for a finitely generated submodule N such that $|A| = d$, where d is the smallest nonnegative integer such that N is generated by d elements (and no fewer).
- This idea of generation is very similar to the idea of **span** from vector space theory.
- Examples.
  1. $\mathbb{Z}a = \langle a \rangle$.
  2. $R = R1$.
     - Thus, all rings R when viewed as R-modules are cyclic.
     - "I is a cyclic R-submodule of the left R-module R" $\iff$ "I is a principal ideal of R."
     - Submodules of finitely generated modules need not be finitely generated: Consider the R-module $R = F[X_1, X_2, \dots]$. We know from the above that $R = R1$ is cyclic. However, the submodule $R\{X_1, X_2, \dots\}$ cannot be generated by any finite set.
  3. R^n is generated by the n elements e_i.
     - If R is commutative, then $\{e_i\}$ is a minimal generating set.

2/18:

  4. **Cyclic** $F[X]$-modules.
     - If $T = I$, then $p(X)v = \alpha v$, so $\dim V = 1$.
     - Considers when T is the shift operator.
- **Cyclic** ($F[X]$-module with generator v): An $F[X]$-module V such that $V = \{p(X)v : p(X) \in F[X]\}$, that is, every element of V can be written as an F-linear combination of elements of the set $\{T^nv : n \geq 0\}$.

- Alternate definition: The set $\{v, Tv, T^2v, \dots\}$ spans V.

2/16:

- **Direct product** (of $M_1, \dots, M_k$): The collection of k-tuples $(m_1, \dots, m_k)$ where $m_i \in M_i$ under addition and a componentwise action of R, where $M_1, \dots, M_k$ is a collection of R-modules. *Also known as* **external direct sum**, **direct sum**. *Denoted by* $\boldsymbol{M_1 \times \cdots \times M_k}$, $\boldsymbol{M_1 \oplus \cdots \oplus M_k}$.
  - The direct product is an R-module.
  - Note that we use the times notation to refer to the "direct product" and the O-plus notation to refer to the "direct sum."
  - The concepts of direct sum and direct product are equivalent for finitely many modules M_i, but they are different in general, that is, the direct product of an infinite number of modules may not equal the direct sum of those infinitely many modules.
    - See Exercise 10.3.20.
- Conditions for when a module is isomorphic to the direct product of some of its submodules.

  Proposition 10.5. Let $N_1, \dots, N_k$ be submodules of the R-module M. Then TFAE.

  1. The map $\pi : N_1 \times \cdots \times N_k \to N_1 + \cdots + N_k$ defined by
  $$\pi(a_1, \dots, a_k) = a_1 + \cdots + a_k$$
  is an isomorphism of R-modules. That is,
  $$N_1 \times \cdots \times N_k \cong N_1 + \cdots + N_k$$
  as R-modules.
  2. $N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = 0$ for all $j \in [k]$.
  3. Every $x \in N_1 + \cdots + N_k$ can be written *uniquely* in the form $a_1 + \cdots + a_k$ with $a_i \in N_i$.

  Proof. Given. □

- Note that Theorem 5.9 is an analogous result to Proposition 10.5 but for groups, that is, it determines when a group is the direct product of two of its subgroups.
- **Internal direct sum** (of $N_1, \dots, N_k$): The R-module $N_1 + \cdots + N_k$, where $N_1, \dots, N_k$ satisfy the equivalent conditions of Proposition 10.5. *Also known as* **direct sum**. *Denoted by* $\boldsymbol{N_1 \oplus \cdots \oplus N_k}$.
  - Note that Part 1 of Proposition 10.5 is the statement that the internal and external direct sums are equivalent, justifying the shared notation.
- **Free** (module on A): An R-module F such that for every nonzero $x \in F$, there exist unique nonzero elements $r_1, \dots, r_n \in R$ and $a_1, \dots, a_n \in A$ such that $x = r_1a_1 + \cdots + r_na_n$, where $A \subset F$ and $n \in \mathbb{N}$.
- **Basis** (of a free module): The set A corresponding to a free module on A. *Also known as* **set of free generators**.
- **Rank** (of a free module): The cardinality of the free R-module's basis, where R must be commutative.
- Distinction between the uniqueness property of direct sums (Statement 3 of Proposition 10.5) and the uniqueness property of free modules.
  - The former refers to uniqueness among module elements, while the latter refers to uniqueness among the *ring elements* as well as among the module elements.

  - Example: Let $R = \mathbb{Z}$ and $N_1 = N_2 = \mathbb{Z}/2\mathbb{Z}$. Then each element of $N_1 \oplus N_2$ has a unique representation in the form $n_1 + n_2$. (For instance, $(1,1) = (1,0) + (0,1)$, and no other elements besides $(1,0) \in N_1$ [speaking loosely on calling $(0,1)$ an element of $\mathbb{Z}/2\mathbb{Z}$] and $(0,1) \in N_2$ will add to $(1,1)$.) However, since $n_1 = 3n_1 = 5n_1 = \cdots$ for all $n_1 \in N_1$, each $n_1 + n_2$ does not have a unique representation in the form $r_1a_1 + r_2a_2$. Thus, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is not a free $\mathbb{Z}$-module on $\{(1,0),(0,1)\}$ (or on any set as it turns out).

- Factorization through free modules.

  Theorem 10.6. For any set A, there exists a free R-module $F(A)$ on the set A such that $F(A)$ satisfies the following **universal property**: If M is any R-module and $\varphi : A \to M$ is any map of sets, then there is a unique R-module homomorphism $\Phi : F(A) \to M$ such that $\Phi(a) = \varphi(a)$ for all $a \in A$. That is, the following diagram commutes.

$$\begin{tikzcd}
A \arrow[r, hook, "\text{inclusion}"] \arrow[dr, "\varphi"'] & F(A) \arrow[d, "\Phi"] \\
 & M
\end{tikzcd}$$

  Figure 6.2: Decomposition of a map through a free module.

  When A is the finite set $\{a_1, \dots, a_n\}$, $F(A) = Ra_1 \oplus \cdots \oplus Ra_n \cong R^n$.

  Proof. Given. □

- Using Theorem 10.6 to generate free module isomorphisms.

  Corollary 10.7.

  1. If F_1, F_2 are free modules on the same set A, then there is a unique isomorphism between F_1, F_2 which is the identity map on A.
  2. If F is any free R-module with basis A, then $F \cong F(A)$. In particular, F enjoys the same universal property with respect to A as $F(A)$ does in Theorem 10.6.

- Application of Corollary 10.7(2).

  - It allows us to do the following: If F is a free R-module with basis A, we will often (particularly with vector spaces) define R-module homomorphisms from F into other R-modules simply by specifying their values on the elements of A and then saying "extend by linearity."

- **Free abelian group** (on A): The free R-module on a set A, where $R = \mathbb{Z}$.

  - If $|A| = n$, then $F(A)$ is the free abelian group of rank n and is isomorphic to

$$\underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n \text{ times}}$$

2/20: - **Direct product** (of M_i, $i \in I$): The direct product of the M_i as abelian groups (i.e., their Cartesian product as sets under componentwise addition) with the action of R componentwise multiplication. *Denoted by* $\boldsymbol{\prod_{i \in I} M_i}$.

- **Direct sum** (of M_i, $i \in I$): The restricted direct product of the abelian groups M_i (i.e., the subset of the direct product $\prod_{i \in I} M_i$ which consists of all elements $\prod_{i \in I} m_i$ such that only finitely many of the components m_i are nonzero) with the action of R componentwise multiplication. *Denoted by* $\boldsymbol{\bigoplus_{i \in I} M_i}$.