MATH 25800 (Honors Basic Algebra II) Notes

Steven Labalme

February 22, 2023

Weeks

List of Figures

List of Tables

Week 1

Rings Intro

1.1 Rings, Subrings, and Ring Homomorphisms

1/4:

- Intro to the course.
- What will be covered: Most of Chapters 7-12 in Dummit and Foote (2004).
  - Mostly rings, a bit of modules.
    - Modules tend to get more complicated.
  - The topics covered in class will all be in the book, but not necessarily in the same order.
  - Some of Nori's definitions will be different from those used in the book.
    - Different enough, in fact, to get us the wrong answers in PSet and Exam questions.
    - We should use his, though.
    - He diverges from the book because his is the mathematical literature standard.
    - Three main differences: Definition of a ring, subring, and ring homomorphism.
- Homework will be due every Wednesday.
  - The first will be due next week (on Wednesday, 1/11).
  - Rings, subrings, and ring homomorphisms, only, are needed for the first HW.
- Grading breakdown.
  - HW (30%).
  - Midterm (30%) — third or fourth week.
  - Final (40%).
- Office hours for Nori in Eckhart 310.
  - M (3:00-4:30).
  - Tu (3:30-5:00).
  - Th (3:00-4:30).
- Callum is our TA; Ray is for the other section. Their OH are TBA.
- All important course info will be in Files on Canvas.
- There will be course notes provided for the course.
- If we think something Nori writes down looks suspicious, feel free to ask!

- We now start the course content.
- **Ring**[1]: A triple $(R, +, \times)$ comprising a set R equipped with binary operations $+$ and $\times$ that satisfies the following three properties.

  (i) $(R, +)$ is an abelian group.

  (ii) $(R, \times)$ is associative, i.e.,
  $$a \times (b \times c) = (a \times b) \times c$$
  for all $a, b, c \in R$.

  (iii) The left and right distributive laws hold, i.e.,
  $$a \times (b + c) = (a \times b) + (a \times c) \qquad (b + c) \times a = (b \times a) + (c \times a)$$
  for all $a, b, c \in R$.

- Misc comments.
  - The parentheses on the RHSs in (iii) indicate the "standard" order of operations.
  - We still often drop the $\times$ in favor of $a \cdot b$ or simply ab.
  - We haven't postulated multiplicative inverses. That makes things more tricky :)
- We define left- and right-multiplication functions for every element $a \in R$.
  - These are denoted $l_a : R \to R$ and $r_a : R \to R$. In particular,
  $$l_a(b) = a \times b \qquad r_a(b) = b \times a$$
  for all $b \in R$.
  - The statement "l_a, r_a are group homomorphisms[2] from $(R, +)$ to itself, i.e.,
  $$l_a(b + c) = l_a(b) + l_a(c)$$
  for all $b, c \in R$" is equivalent to (iii).
- **Additive identity** (of R): The unique element of R that satisfies the following constraint. *Denoted by* $\mathbf{0_R}$.
  $$0_R + a = a + 0_R = a$$
  for all $a \in R$.
  - The existence and uniqueness of 0_R follows from property (i) of rings (groups must have an identity element, which in this case is the *additive* identity since it corresponds to the addition operation).
- Similarly, we know that unique additive inverses exist for all $a \in R$. We denote these by $\boldsymbol{-a}$.
- Since l_a is a group homomorphism, this must mean that
  $$l_a(0_R) = 0_R \qquad l_a(-b) = -l_a(b)$$
  $$a \times 0_R = 0_R \qquad a \times (-b) = -(a \times b)$$
  for all $a, b \in R$.
  - The same holds for r_a/positions interchanged.
  - These are consequences of the distributive law.

[1] Definition from Dummit and Foote (2004).

[2] Since we will soon introduce other types of homomorphisms (e.g., ring homomorphisms) beyond the one type with which we are familiar, we now have to specify that a homomorphism of the type dealt with in MATH 25700 is a *group* homomorphism.

- In Part 1, Dummit and Foote (2004) defines rings as above.
  - In Part 2, Dummit and Foote (2004) takes R to be **commutative**.
  - In Part 3, Dummit and Foote (2004) takes R to be a **ring with identity**.
- **Commutative ring**: A ring R such that

$$a \times b = b \times a$$

for all $a, b \in R$.

- **Ring with identity**: A ring R containing a 2-sided identity, i.e., an element $e \in R$ such that

$$e \times a = a \times e = a$$

for all $a \in R$.

- We now justify that it's ok to denote the 2-sided identity with a single letter.
- Exercise: The identity is unique.

Proof. If e' is also a 2-sided identity, then

$$e = e \times e' = e'$$

□

- In this course, we will always take "ring" to mean "ring with identity." That is, we will always assume that our rings contain a 2-sided identity $e = 1_R$.
- Examples of rings.
  1. $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ all have two binary operations, but are they all rings?
     - $\mathbb{N}$ is not a ring since $(\mathbb{N}, +)$ is not an abelian group (or even a group — no additive inverses).
     - The rest are rings. In fact, they are commutative rings.
     - $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are also **fields**.
  2. Let X be a set, and $f, g : X \to \mathbb{R}$. We can define $f + g : X \to \mathbb{R}$ by $(f + g)(x) = f(x) + g(x)$ and $f \times g : X \to \mathbb{R}$ by $(f \times g)(x) = f(x)g(x)$.
     - Thus, the set of all functions from $X \to \mathbb{R}$ — denoted $\mathrm{Fun}(X; \mathbb{R})$ or $\mathbb{R}^X$ — has two binary operations and is a ring.
     - This follows from the fact that the real numbers form a ring.
  3. More generally, let X be a set and let R be a ring. Then $\mathrm{Fun}(X; R) = R^X$ is a ring.
     - The constant function taking the value $1_R \in R$ is the identity of R^X.
  4. Let $X = \{1, 2\}$. Then $R^X \cong R \times R$.
     - Correct topology:

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \qquad (a_1, a_2) \times (b_1, b_2) = (a_1 \times b_1, a_2 \times b_2)$$

     - Implication: The same "formula" shows that if R_1, R_2 are rings, then $R_1 \times R_2$ is a ring.
  5. If R_i is a ring for all $i \in I$, where I could be any indexing set (e.g., $\mathbb{N}$, but need not be countable), then $\prod_{i \in I} R_i$ is also a ring.
     - The identity is $(e_i, e_j, \dots)$.
- **Field**: A commutative ring R with multiplicative inverses for every element except 0_R.

- In the context of groups, we've discussed subgroups, group homomorphisms, the fact that the inclusion of a subgroup into a bigger group is a group homomorphism, and the fact that the image of a group homomorphism is a subgroup.
- Today, let's define subrings and ring homomorphisms and make sure that the corresponding properties remain true.
- Intuitively, a **subring** should be a subset of a ring that is itself a ring under the restricted operations.
- **Subring**: A subset S of a ring R such that...
  (i) For all $a, b \in S$, both $a + b, ab \in S$. For all $a \in S$, $-a \in S$.
  (ii) $1_R \in S$.
- Check that these conditions are sufficient!
- **Ring homomorphism**: A function $f : A \to B$, where A, B are rings, such that

$$\begin{aligned} f(a_1 + a_2) &= f(a_1) + f(a_2) \\ f(a_1 \times a_2) &= f(a_1) \times f(a_2) \\ f(1_A) &= 1_B \end{aligned}$$

  for all $a_1, a_2 \in A$.
- Note that we need the third constraint because we are not postulating the existence of multiplicative inverses.
- Examples:
  1. If S is a subring of a ring R and $i : S \to R$ is the inclusion map, then it is a ring homomorphism.
  2. R_1, R_2 are rings. Then $\pi : R_1 \times R_2 \to R_1$ defined by $\pi(a_1, a_2) = a_1$ for all $(a_1, a_2) \in R_1 \times R_2$ is a ring homomorphism.
  3. $i : R_1 \to R_1 \times R_2$ defined by $i(a) = (a, 0)$ is not a ring homomorphism unless R_2 is trivial since $i(1_{R_1}) = (1_{R_1}, 0) \neq (1_{R_1}, 1_{R_2}) = 1_{R_1 \times R_2}$.
  4. $f : M_2(\mathbb{R}) \to M_3(\mathbb{R})$ defined by inclusion in the upper lefthand corner is not a ring homomorphism for the same reason as the above. To be clear, the functional relation considered here is

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \left(\begin{array}{cc|c} a & b & 0 \\ c & d & 0 \\ \hline 0 & 0 & 0 \end{array}\right)$$

- The integers have no subrings except for itself.
  - Consider $\mathbb{Z}/10\mathbb{Z}$, for instance. Doesn't work because we postulate the existence of an identity, but $1 \notin \mathbb{Z}/10\mathbb{Z}$.
- Subrings of $\mathbb{Q}$:
  - $\mathbb{Z}, \mathbb{Q}$, the p-adic rationals $\{a/p^n : a \in \mathbb{Z}, n = 0, 1, \dots\}$, $\{a/(p_1 p_2 \cdots p_r)^n : a \in \mathbb{Z}, n = 0, 1, \dots\}$, arbitrary subsets of primes in the denominator.
  - Exercise: There's a bijective correspondence between the subrings of $\mathbb{Q}$ and the power set of the prime numbers.

1.2 Office Hours (Nori)

1/5:

- Is $\mathbb{Z}$ a commutative ring?
  - Yes it is.
- Can you clarify the statement of Problem 1.4?
  - For any ring R, define a function $\Delta : R \to R \times R$ by
$$\Delta(a) = (a, a)$$
  - Clearly Δ is a ring homomorphism.
  - Then consider the image $\Delta(R) \subset R \times R$.
  - We are asked to show that if $\Delta(\mathbb{Q}) \subset B \subset \mathbb{Q} \times \mathbb{Q}$ for B a subring of $\mathbb{Q} \times \mathbb{Q}$, then either $B = \Delta(\mathbb{Q})$ or $B = \mathbb{Q} \times \mathbb{Q}$.

1.3 Polynomial Rings and Power Series Rings

1/6:

- End of last time: The subrings of $\mathbb{Q}$.
- Today: The subrings an arbitrary ring R.
- Question 1: Let R a ring, $x \in R$ arbitrary. What is the "smallest" subring $M \subset R$ such that $x \in M$?
  - We know that $1_R \in M$. Thus, $1_R + 1_R = 2_R \in M$. It follows by induction that
$$n_R \in M$$
for all $n \in \mathbb{Z}$.
  - Moving on, $x \in M$ implies that $n_R x, x n_R \in M$. Is it true that $n_R x = x n_R$? Yes it is. Here's why.
    - Let $C = \{c \in R : cx = xc\}$, where x is the element we've been talking about.
    - We can prove that C is a subring of R; this is Exercise 7.1.9 of Dummit and Foote (2004); see HW2.
    - If C is a subring, then $1_R \in C$ implies $1_R + 1_R = 2_R \in C$, implies $n_R \in C$. Therefore,
$$n_R x = x n_R \in M$$
for all $n \in \mathbb{Z}$.
  - The above and additive closure:
$$\{a_R + b_R x : a, b \in \mathbb{Z}\} \subset M$$
  - Multiplicative closure: $x \cdot x = x^2 \in M$. In general, defining x^n in the usual way (i.e., inductively), shows that
$$x^n \in M$$
for all $n \in \mathbb{Z}_{\geq 0}$.
    - To be explicit, the inductive definition of x^n is $x^0 = 1_R$ and $x^{n+1} = x \cdot x^n$.
  - Multiplicative closure and $n_R y = y n_R$ for $y \in R$ arbitrary (see above argument):
$$a_R x^n = x a_R x^{n-1} = \cdots = x^n a_R \in M$$
for all $a \in \mathbb{Z}$, $n \in \mathbb{Z}_{\geq 0}$.
  - Additive closure:
$$(a_0)_R + (a_1)_R x + \cdots + (a_n)_R x^n \in M$$
for all $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ and $n \in \mathbb{Z}_{\geq 0}$.
    - Naturally, terms of this form are called **polynomials**.
    - As the set of polynomials is at last closed under $+, \times$, M must be a **polynomial ring**.

- **Polynomial ring** (over $\mathbb{Z}$): The ring defined as follows. *Denoted by* $\boldsymbol{\mathbb{Z}[X]}$. *Given by*

$$\mathbb{Z}[X] = \bigcup_{m=0}^{\infty} \{a_0 + a_1 X + \cdots + a_m X^m : a_0, a_1, \ldots, a_m \in \mathbb{Z}\}$$

  - Note that we *insist* on using uppercase for the indeterminate. The motivation for doing so is illustrated by the next example.

- $\mathbb{Z}[X]$ induces[3] a collection of ring homomorphisms $\phi_x : \mathbb{Z}[X] \to R$, one for every R and $x \in R$. These are defined by

$$\phi_x(f) = f(x)$$

  where $f = a_0 + a_1 X + \cdots + a_m X^m$, $f(x) = (a_0)_R + (a_1)_R x + \cdots + (a_m)_R x^m$, and all $a_i \in \mathbb{Z}$.

- Implication.
  - For any R and any $x \in R$, $\phi_x(\mathbb{Z}[X]) \subset R$.
  - In layman's terms, the set of all polynomials of a single element of any ring is necessarily a subset of the ring overall.

- Question 2: Let $R \subset B$ be rings, and let $x \in B$. Find the smallest subring $M \subset B$ such that $R \subset M$ and $x \in M$.
  - Last time, we only knew that 1_R had to be in M. This time, we have a whole set of elements R to choose from!
  - Let $a \in R$ be arbitrary. We see that $a, x \in M$; this means that $ax, xa \in M$. But we may not have $ax = xa$ as we did so nicely for the integers n_R, so we have to postulate commutativity if we want to avoid a messy answer.
  - Henceforth, we assume
$$ax = xa \in M$$
    for all $a \in R$.
  - As in Question 1, $ax = xa$ implies
$$ax^m = x^m a \in M$$
    for all $a \in R$, $m \in \mathbb{Z}_{\geq 0}$.
  - Thus,
$$a_0 + \cdots + a_m x^m \in M$$
    for $a_0, \ldots, a_m \in R$, $m \in \mathbb{Z}_{\geq 0}$.
  - This set of polynomials is already a subring. Thus, it is not only contained in M, but must also equal M.
  - Difference between these polynomials and the ones from Question 1: These are the polynomials with coefficients in $R \supset \mathbb{Z}$, where this containment is homomorphic (not necessarily injective).
    - Therefore, we need to define a broader type of polynomial ring.

- **Polynomial ring** (over R): The ring defined as follows. *Denoted by* $\boldsymbol{R[X]}$. *Given by*

$$R[X] = \bigcup_{m=0}^{\infty} \{a_0 + a_1 X + \cdots + a_m X^m : a_0, a_1, \ldots, a_m \in R\}$$

  - We do not require that R is commutative.
  - Note that $R[X]$ will be commutative, however, owing to the way it's defined.

[3] Recall that the terminology "induce" means that to every $R'[X]$, we can assign a set of ring homomorphisms of the given form. In other words, the set of polynomial rings over rings R' is in bijective correspondence with the set of collections of functions ϕ_x.

- We now seek to generalize polynomial rings to **power series rings**.
- To do so, we'll need to get more precise than the infinite unions we've been using.
  - Consider the set of nonnegative integers $\mathbb{Z}_{\geq 0} = \{0, 1, 2, \dots\}$.
    - This is a **monoid** under both addition and multiplication.
  - Let $(R, +)$ be an abelian group.
  - Then $(R^{\mathbb{Z}_{\geq 0}}, +)$ is also an abelian group.
    - As per last class, all elements $a \in (R^{\mathbb{Z}_{\geq 0}}, +)$ are functions $a : \mathbb{Z}_{\geq 0} \to R$.
    - We write that $a : n \mapsto a_n$, i.e., the value of a at n will be denoted a_n, not $a(n)$.
  - Every element $a \in R^{\mathbb{Z}_{\geq 0}}$ will be represented by $\sum_{n=0}^{\infty} a_n X^n$.
    - This is allowable because there is a natural bijective correspondence between each a and each power series $\sum_{n=0}^{\infty} a_n X^n$.
    - Essentially, what we are doing here is using the rigorously defined set of functions $R^{\mathbb{Z}_{\geq 0}}$ to theoretically stand in for the intuitive concept of a power series. This is acceptable since both objects have very similar properties, especially as pertains to adding and multiplying them.
    - This is like defining the real numbers (intuitive) in terms of Dedekind cuts (rigorous).
    - Note that alternatively, we could introduce the entire sequences/series analytical framework from Honors Calculus IBL to logically underpin power series, but this technique will be much less bulky and suit our purposes just fine.
  - We define addition and multiplication on $R^{\mathbb{Z}_{\geq 0}}$ as follows.

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

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

  - This is the **power series ring**.
- **Monoid**: A set equipped with an associative binary operation and an identity element.
- **Power series ring** (over R): The ring defined as follows, with $+, \times$ defined as above. *Denoted by* $\boldsymbol{(R[[X]], +, \times)}$. *Given by*

$$R[[X]] = R^{\mathbb{Z}_{\geq 0}}$$

- Note that the definitions of addition and multiplication for $R[[X]]$ are precisely the ones needed for $R[X]$, too, (just the finite version) even though we didn't state them earlier.
- Two observations about power series rings which will also hold for polynomial rings.
  1. R is a subring of $R[[X]]$ with the inclusion ring homomorphism $a \mapsto a1 + 0X^1 + 0X^2 + \cdots$.
  2. Additionally, we can map $X \in R$ to $0X^0 + 1X^1 + 0X^2 + \cdots \in R[[X]]$.
- $aX = Xa$ for all $a \in R$.
  - Why?? Ask in OH.
- Alternate definition of $R[X]$: The subring of $R[[X]]$ given by

$$R[X] = \left\{ \sum_{m=0}^{\infty} a_m X^m \in R[[X]] \,\middle|\, |\{m \in \mathbb{Z}_{\geq 0} : a_m \neq 0\}| < \infty \right\}$$

- Theorem (Universal Property of a Polynomial Ring): Let R be a ring, $\alpha : R \to B$ a ring homomorphism, and $x \in B$. Assume that $x \cdot \alpha(a) = \alpha(a) \cdot x$ for all $a \in R$. Then there is a unique ring homomorphism $\beta : R[X] \to B$ such that $\beta(a) = \alpha(a)$ for all $a \in R$ and $\beta(X) = x$.

  Proof. We first prove that such a ring homomorphism exists. Then we address uniqueness.

  Let $\beta(X) = x$. Then if β is to be a ring homomorphism, we must have

  $$\beta(X^m) = x^m$$

  for all $m \in \mathbb{Z}_{\geq 0}$. We also require that $\beta(a_m) = \alpha(a_m)$ for all $a_m \in R$ (at this point, a_m is just suggestive notation). Again, if β is to be a ring homomorphism, it must follow that

  $$\beta(a_m X^m) = \beta(a_m)\beta(X^m) = \alpha(a_m)x^m$$

  for all $a_m \in R$, $m \in \mathbb{Z}$. Lastly, if β is to be a ring homomorphism, it must follow that

  $$\beta\left(\sum_{i=0}^{m} a_i X^i\right) = \sum_{i=0}^{m} \beta(a_i X^i) = \sum_{i=0}^{m} \alpha(a_i)x^i$$

  But then by its construction, β is defined on every element in $R[X]$ and is a ring homomorphism satisfying the desired properties.

  Suppose $\beta, \beta' : R[X] \to B$ are ring homomorphisms satisfing $\beta(a) = \beta'(a) = \alpha(a)$ for all $a \in R$ and $\beta(X) = \beta'(X) = x$. Let $\sum_{i=0}^{m} a_i X^i \in R[X]$ be arbitrary. Then

  $$\beta\left(\sum_{i=0}^{m} a_i X^i\right) = \sum_{i=0}^{m} \alpha(a_i)x^i = \beta'\left(\sum_{i=0}^{m} a_i X^i\right)$$

  as desired. □

- The idea of the theorem.
  - Evaluation of a function ($f \in R[X]$) at a point ($x \in B$): If $R \subset B$ and $\alpha(a) = a$ for all $a \in R$, then $\beta(f) = f(x)$. Recall the ϕ_x from earlier.
  - α is like a coordinate change function, allowing us to evaluate variants of each f.
  - In fact, this idea is highly related to the linear algebra concept that specifying the action of a map on a basis specifies its action on all elements.
    - However, here we are dealing with a **module homomorphism**, not a linear transformation.

1.4 Chapter 7: Introduction to Rings

From Dummit and Foote (2004).

A Word on Ring Theory

1/7:

- Plan for Part II: Ring theory.
  - Study analogues of group-related objects, such as "subrings, quotient rings, ideals (which are the analogues of normal subgroups), and ring homomorphisms" (Dummit & Foote, 2004, p. 222).
  - Answer questions about general rings, leading to fields and finite fields.
  - Arithmetic over general rings, and applications of these results to polynomial rings.
- Part II grounds the remaining four parts of the book.
  - Part III is modules (ring actions).
  - Part IV is fields and polynomial equations over them (applications of ring structure theory).
  - Part V is ring applications.
  - Part VI is specific kinds of rings and the objects on which they act.

Section 7.1: Basic Definitions and Examples

- Definition of a **ring** (Dummit & Foote, 2004, p. 223).
- Motivation for requiring $(R, +)$ to be abelian.
  - If R is a ring with identity, then the distributive laws imply commutativity of addition anyway, as follows.[4]
  - Let $a, b \in R$ be arbitrary. We have from the ring axioms that

$$(1+1)(a+b) = 1(a+b) + 1(a+b) = 1a + 1b + 1a + 1b = a + b + a + b$$
$$(1+1)(a+b) = (1+1)a + (1+1)b = 1a + 1a + 1b + 1b = a + a + b + b$$

  - Thus, by transitivity and the cancellation law,

$$b + a = a + b$$

- One of the most important examples of a ring is a **field**.
- **Division ring**: A ring R with identity $1 \neq 0$ such that every nonzero element $a \in R$ has a multiplicative inverse, i.e., there exists $b \in R$ such that $ab = ba = 1$. *Also known as* **skew field**.
- **Field**: A commutative division ring.
- **Trivial ring**: A ring R for which $a \times b = 0$ for all $a, b \in R$.
  - So named because "although trivial rings have two binary operations, multiplication adds no new structure to the additive group, and the theory of rings goves no information which could not already be obtained from (abelian) group theory" (Dummit & Foote, 2004, p. 224).
- **Zero ring**: The trivial ring where $R = \{0\}$. *Denoted by* $\boldsymbol{R = 0}$.
- Excluding the zero ring, trivial rings do not contain a multiplicative identity.
  - Suppose for the sake of contradiction that there exists $1 \in R$ trivial and nonzero. Let a be a nonzero element of R. Then

$$a = 1 \times a = 0$$

    a contradiction.
- $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with identity under modular arithmetic.
- **Hamilton Quaternions**: The set of elements of the form

$$a + bi + cj + dk$$

  where $a, b, c, d \in \mathbb{R}$, under componentwise addition

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k$$

  and distributive noncommutative multiplication subject to the relations

$$i^2 = j^2 = k^2 = -1 \qquad ij = -ji = k \qquad jk = -kj = i \qquad ki = -ik = j$$

  Also known as **real Hamilton Quaternions**. *Denoted by* $\mathbb{H}$.
  - Dummit and Foote (2004) provides an example multiplication.
  - $\mathbb{H}$ is a ring, specifically a *noncommutative* ring with identity $(1 = 1 + 0i + 0j + 0k)$.

[4] Thus, our definition of a ring in class is somewhat redundant. Indeed, if we're defining a ring to be a ring with identity, then we can omit the abelian condition and know that the distributive laws will still imply it.

  - Historically, it was one of the first noncommutative rings discovered.
    - Sir William Rowan Hamilton discovered it in 1843.
    - Quaternions have been very influential in the development of mathematics and continue to be important in certain areas of mathematics and physics.
  - The Quaternions form a division ring with

$$(a+bi+cj+dk)^{-1} = \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}$$

  - We can also define the rational Hamilton Quaternions by only taking $a, b, c, d \in \mathbb{Q}$.

- $R = A^X$ is commutative iff A is commutative.
  - R has 1 iff A has 1 (in which case $1_R : X \to A$ sends $x \mapsto 1_A$ for all $x \in X$).
- $C([a,b], \mathbb{R})$ is a ring with identity, though we need limit theorems to prove this.
- Basic properties of arbitrary rings.

  Proposition 7.1. Let R be a ring. Then

  1. $0a = a0 = a$ for all $a \in R$;
  2. $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$;
  3. $(-a)(-b) = ab$ for all $a, b \in R$;
  4. If R has an identity 1, then the identity is unique and $-a = (-1)a$.

  Proof. Given. □

- **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** (in R a nonzero ring with identity): An element $u \in R$ to which there corresponds some $v \in R$ such that $uv = vu = 1$.
  - As the phrasing of the term implies, the property of being a unit depends on the ring in which an element is viewed. For example, 2 is not a unit in $\mathbb{Z}$, but 2 is a unit in $\mathbb{Q}$.
- **Group of units** (of R): The set of all units in R. *Denoted by* $\boldsymbol{R^\times}$, $\boldsymbol{R^*}$.
  - As the name implies, $R^\times$ is a group under multiplication.
- Alternate definition of field: A commutative ring F with identity $1 \neq 0$ in which every nonzero element is a unit, i.e., $F^\times = F - \{0\}$.
- A zero divisor can never be a unit.
  - Suppose for the sake of contradiction that a is a unit in R and $ab = 0$ for some nonzero $b \in R$. Then $va = 1$ for some $v \in R$. It follows that

$$b = 1b = (va)b = v(ab) = v0 = 0$$

    a contradiction. The argument is symmetric if we assume $ba = 0$.
  - It follows that fields contain no zero divisors.
- Examples of zero divisors and units.
  1. $\mathbb{Z}$.
     - No zero divisors and $\mathbb{Z}^\times = \{\pm 1\}$.

2. $\mathbb{Z}/n\mathbb{Z}$.
   - The elements $\bar{u}$ for which u, n are relatively prime are units (see proof in Chapter 8).
   - If a, n are not relatively prime, then $\bar{a}$ is a zero divisor in $\mathbb{Z}/n\mathbb{Z}$ ($a \cdot n/a = 0$).
   - Thus, every nonzero element of $\mathbb{Z}/n\mathbb{Z}$ is either a unit or a zero divisor.
   - $\mathbb{Z}/n\mathbb{Z}$ is a field iff n is prime (every nonzero element is a unit iff they are all relatively prime to n).
3. $\mathbb{R}^{[0,1]}$.
   - The units are all functions that are nonzero on the entire domain.
   - f not a unit and nonzero implies f is a zero divisor: Choose

$$g(x) = \begin{cases} 0 & f(x) \neq 0 \\ 1 & f(x) = 1 \end{cases}$$

4. $C([0,1], \mathbb{R})$.
   - There exist units (same as above), zero divisors (consider a function that is nonzero on $[0, 0.5)$ and zero on $[0.5, 1]$), and functions that are neither (consider a function that is only zero at $x = 0.5$; then its complement would necessarily be discontinuous at $x = 0.5$).
5. **Quadratic fields** (see Section 13.2).

- **Quadratic field**: A ring of the following form, where D is a rational number and not a perfect square in $\mathbb{Q}$. *Denoted by* $\mathbb{Q}(\sqrt{D})$. *Given by*

$$\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$$

  - Addition is componentwise and multiplication is "as expected" based on the notation, i.e.,

$$(a + b\sqrt{D}) + (c + d\sqrt{D}) = (a + c) + (b + d)\sqrt{D}$$
$$(a + b\sqrt{D}) \times (c + d\sqrt{D}) = (ac + bdD) + (ad + bc)\sqrt{D}$$

    - It follows that multiplication is commutative; hence, $\mathbb{Q}(\sqrt{D})$ is a commutative ring.
  - $\mathbb{Q}(\sqrt{D})$ is a subring of $\mathbb{C}$.
    - If $D > 0$, then it is a subring of $\mathbb{R}$.
  - The assumption that D is not a perfect square implies that every element in $\mathbb{Q}(\sqrt{D})$ can be written uniquely in the form $a + b\sqrt{D}$.
    - Consequence: $a^2 - Db^2 \neq 0$ if a, b are nonzero.
  - Since $(a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2$, the inverse of $a + b\sqrt{D} \neq 0$ is

$$\frac{a - b\sqrt{D}}{a^2 - Db^2}$$

  - Thus, all nonzero elements in $\mathbb{Q}(\sqrt{D})$ are units; hence, $\mathbb{Q}(\sqrt{D})$ is a field.

- **Squarefree part** (of $D \in \mathbb{Q}$): The unique integer D' that is not divisible by the square of any integer greater than 1 and such that $D = f^2 D'$ for some $f \in \mathbb{Q}$.
  - Since $\sqrt{D} = f\sqrt{D'}$, we may take D to be a squarefree integer in the definition of $\mathbb{Q}(\sqrt{D})$ in general and WLOG.
  - Indeed, we just combine f into b.

- **Integral domain**: A commutative ring with identity $1 \neq 0$ that has no zero divisors.
  - $\mathbb{Z}$ is the prototypical integral domain.

- Properties of integral domains.

  Proposition 7.2 (Cancellation law)**.** Assume a, b, c are elements of any ring with a not a zero divisor. If $ab = ac$, then either $a = 0$ or $b = c$ (i.e., if $a \neq 0$, then we can cancel the a's).

  In particular, if a, b, c are any elements of an integral domain and $ab = ac$, then either $a = 0$ or $b = c$.

  Proof. $ab = ac$ implies $a(b - c) = 0$. Thus, since a is not a zero divisor, either $a = 0$ or $b - c = 0$ (equivalently, $b = c$). □

  Corollary 7.3. Any finite integral domain is a field.

  Proof. Let R be a finite integral domain, and a be an arbitrary, nonzero element of R. We seek to find b such that $ab = 1$, which will imply that a (i.e., every element) is a unit in R.

  Define the map $x \mapsto ax$. By the cancellation law, this map is injective. Injectivity plus the fact that R is finite proves that this map is surjective. Thus, there exists $b \in R$ such that $ab = 1$, as desired. □

- Wedderburn: A finite division ring is necessarily commutative, i.e., is a field.
  - See Exercise 13.6.13 for a proof.
- "Every nonzero element of a commutative ring that is not a zero divisor has a multiplicative inverse in some larger ring" (Dummit & Foote, 2004, p. 228).
  - See Section 7.5.
- **Subring** (of R): A subgroup of R that is closed under multiplication.
- To confirm that $S \subset R$ is a subring, check that is is nonempty, closed under subtraction, and closed under multiplication.
- The property "is a subring of" is transitive.
- "If R is a subring of a field F that contains the identity of F, then R is an integral domain. The converse of this is also true, namely any integral domain is contained in a field" (Dummit & Foote, 2004, p. 229).
  - See Section 7.5.
- **Ring of integers** (in the quadratic field $\mathbb{Q}(\sqrt{D})$): The subring defined as follows. *Denoted by* $\boldsymbol{\mathcal{O}}$, $\boldsymbol{\mathcal{O}_{\mathbb{Q}(\sqrt{D})}}$. *Given by*

  $$\mathcal{O} = \mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$$

  where

  $$\omega = \begin{cases} \sqrt{D} & D \equiv 2, 3 \mod 4 \\ \frac{1+\sqrt{D}}{2} & D \equiv 1 \mod 4 \end{cases}$$

  - Etymology: Elements of the subring $\mathcal{O}$ in the field $\mathbb{Q}(\sqrt{D})$ have many analogous properties to those of the of the subring $\mathbb{Z}$ in the field $\mathbb{Q}$.
  - $\mathcal{O}$ is the **integral closure** of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{D})$ — see Section 15.3.
- **Gaussian integers**: The ring of integers in the quadratic field $\mathbb{Q}(\sqrt{-1})$. *Denoted by* $\boldsymbol{\mathbb{Z}[i]}$.
  - Gauss originally introduced these in 1800 to state the **biquadratic reciprocity law**.
- **Biquadratic reciprocity law**: A statement dealing with the "beautiful relations that exist among fourth powers modulo primes" (Dummit & Foote, 2004, p. 229).

- **Field norm**: The function from $\mathbb{Q}(\sqrt{D}) \to \mathbb{Q}$ defined as follows. *Denoted by* $\boldsymbol{N}$. *Given by*

$$N(a+b\sqrt{D}) = (a+b\sqrt{D})(a-b\sqrt{D}) = a^2 - Db^2$$

  - N is nonzero when $a+b\sqrt{D} \neq 0$ (see above).
  - Measures "size" — for example, if $D=-1$, then $N(a+bi) = a^2+b^2$, which is the length of this complex number considered as a vector in the complex plane.
  - Useful for establishing many properties of $\mathcal{O}$.
  - N is multiplicative: $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$.
  - Defining N on $\mathcal{O}$ shows that $N(\alpha)$ is an *integer* for every $\alpha \in \mathcal{O}$.
- $\alpha \in \mathcal{O}^\times$ iff $N(\alpha) = \pm 1$.
  - Dummit and Foote (2004) proves this from the definition.
- **Pell's equation**: The following equation, where $x, y, D \in \mathbb{Z}$. *Given by*

$$x^2 - Dy^2 = \pm 1$$

  - Finding solutions is equivalent to finding units in $\mathcal{O}$.
- Proves via Pell's equation that

$$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\} \qquad\qquad \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \{\pm 1, \pm\rho, \pm\rho^2\}$$

  where $\rho = (1+\sqrt{-3})/2$.
  - When $D<0$ and $D \neq -1, -3$, $\mathcal{O}^\times = \{\pm 1\}$.
  - When $D>0$, $\mathcal{O}^\times$ is infinite.
- This whole discussion on the ring of integers in a quadratic field is highly related to HW4 Q4.3-4.4.
- **Nilpotent** (element): An element $x \in R$ such that $x^m = 0$ for some $m \in \mathbb{N}$.

Section 7.2: Examples – Polynomial Rings, Matrix Rings, and Group Rings

- **Polynomial rings**, **matrix rings**, and **group rings** are often related.
  - Example: The group ring of a group G over the complex numbers $\mathbb{C}$ is a direct product of matrix rings over $\mathbb{C}$.
- Example applications of these three classes of rings.
  - Study them in their own right.
  - Polynomial rings help prove classification theorems for matrices which, in particular, determine when a matrix is similar to a diagonal matrix.
  - Group rings help study group actions and prove additional classification theorems.
- We begin with polynomial rings.
- Fix a commutative ring R with identity.
- **Indeterminate**: The "variable" X.
- **Polynomial** (in X with coefficients a_i in R): The formal sum

$$a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$$

  with $n \geq 0$ and each $a_i \in R$.

- **Degree n** (polynomial): A polynomial for which $a_n \neq 0$.
- **Leading term**: The $a_n X^n$ term.
- **Leading coefficient**: The a_n coefficient.
- **Monic** (polynomial): A polynomial for which $a_n = 1$.
- Definition of $R[X]$ (Dummit & Foote, 2004, p. 234).
- **Constant polynomials**: The set of polynomials $R \subset R[X]$.
- It follows from its construction that $R[X]$ is a commutative ring with identity (specifically 1_R).
- Definition of $\mathbb{Z}[X], \mathbb{Q}[X]$.
- We can also define polynomial rings like $\mathbb{Z}/3\mathbb{Z}[X]$.
  - This ring consists of the set of polynomials with coefficients $0, 1, 2$ and calculations on the coefficients performed modulo 3.
  - Example: If $p(X) = X^2 + 2X + 1$ and $q(X) = X^3 + X + 2$, then $p(X) + q(X) = X^3 + X^2$.
- The ring in which the coefficients are taken makes a substantial difference in the polynomials' behavior.
  - Example: $X^2 + 1$ is not a perfect square in $\mathbb{Z}[X]$, but is in $\mathbb{Z}/2\mathbb{Z}[X]$ since here,

$$(X + 1)^2 = X^2 + 2X + 1 = X^2 + 1$$

- Properties of polynomials over integral domains.

Proposition 7.4. Let R be an integral domain and let $p(X), q(X)$ be nonzero elements of $R[X]$. Then

1. $\deg p(X)q(X) = \deg p(X) + \deg q(X)$;

   Proof. If $p(X), q(X)$ are polynomials with leading terms $a_n X^n, b_m X^m$, respectively, then the leading term of $p(X)q(X)$ is $a_n b_m X^{n+m}$, provided $a_n b_m \neq 0$. But since $a_n, b_m \neq 0$ (as leading coefficients) and R has no zero divisors (as an integral domain), we have that $a_n b_m \neq 0$. Applying the definition of degree completes the proof. □

2. The units of $R[X]$ are just the units of R;

   Proof. Suppose $p(X) \in R[X]$ is a unit. Then $p(X)q(X) = 1$ for some $q(X) \in R[X]$. It follows by part (1) that

$$\deg p(X) + \deg q(X) = \deg p(X)q(X) = 0 \quad \iff \quad \deg p(X) = \deg q(X) = 0$$

   Therefore, $p(X), q(X) \in R$ and hence are units of R, as desired. □

3. $R[X]$ is an integral domain.

   Proof. We have already established that the commutativity and identity of $R[X]$ follow from R. As to no zero divisors, this constraint follows from part (1). □

- If R has zero divisors, then so does $R[X]$.
  - If $f \in R[X]$ is a zero divisor, then $cf = 0$ for some nonzero $c \in R$ (see Exercise 7.2.2).
- If S is a subring of R, then $S[X]$ is a subring of $R[X]$.
  - Think back to the definition.
- More on polynomial rings in Chapter 9.

1/9:

- We now move onto matrix rings.
- **Matrix ring** (over R): The set of all $n \times n$ matrices (a_{ij}) with entries from R under componentwise addition and matrix multiplication, where R is an arbitrary ring and $n \in \mathbb{N}$. *Denoted by* $\boldsymbol{M_n(R)}$.
- $M_n(R)$ is *not* commutative for all nontrivial R and $n \geq 2$.

  Proof. Since R is nontrivial, we may pick $a, b \in R$ such that $ab \neq 0$. Let A be the matrix with $a_{1,1} = a$ and zeroes elsewhere, and let B be the matrix with $b_{1,2} = b$ and zeroes elsewhere. Then ab is the nonzero entry in position $1, 2$ of AB whereas $BA = 0$. □

- The matrices defined in the above proof are also zero divisors.
  - Thus, $M_n(R)$ has zero divisors for all nonzero rings R where $n \geq 2$.
- **Scalar matrix**: An element $(a_{ij}) \in M_n(R)$ such that

  $$a_{ij} = a \cdot \delta_{ij}$$

  for some $a \in R$ and all $i, j \in \{1, \ldots, n\}$.
  - The scalar matrices form a subring of $M_n(R)$, specifically one that is isomorphic to R.
  - We have that

    $$\operatorname{diag}(a) + \operatorname{diag}(b) = \operatorname{diag}(a + b) \qquad \operatorname{diag}(a) \cdot \operatorname{diag}(b) = \operatorname{diag}(a \cdot b)$$

  - If R is commutative, the scalar matrices commute with all elements of $M_n(R)$.
- **Identity matrix**: The scalar matrix for which $a = 1$, where 1 is the identity of R.
  - Only exists if R is a ring with identity.
  - If it exists, this matrix is the 1 of $M_n(R)$.
  - The existence of a 1 in $M_n(R)$ allows us to define the units in $M_n(R)$, as follows.
- **General linear group** (of degree n): The group of units of $M_n(R)$. *Denoted by* $\boldsymbol{GL_n(R)}$.
  - Alternative definition: The set of $n \times n$ invertible matrices with entries in R.
- If S is a subring of R, then $M_n(S)$ is a subring of $M_n(R)$.
- **Upper triangular matrix**: The set of all matrices (a_{ij}) for which $a_{pq} = 0$ whenever $p > q$.
  - The set of upper triangular matrices is a subring of $M_n(R)$.
- Lastly, we address group rings.
- **Group ring** (of G with coefficients in R): The set of all formal sums

  $$a_1 g_1 + \cdots + a_n g_n$$

  under componentwise addition

  $$(a_1 g_1 + \cdots + a_n g_n) + (b_1 g_1 + \cdots + b_n g_n) = (a_1 + b_1) g_1 + \cdots + (a_n + b_n) g_n$$

  and multiplication defined by the distributive law as well as $(ag_i)(bg_j) = (ab)g_k$ (where $g_k = g_i g_j$) such that the coefficient of g_k in the product $(a_1 g_1 + \cdots + a_n g_n) \times (b_1 g_1 + \cdots + b_n g_n)$ is

  $$\sum_{g_i g_j = g_k} a_i b_j$$

  where $a_i \in R$, a commutative ring with identity $1 \neq 0$, and $g_i \in G$, a finite group with group operation written multiplicatively, for all $1 \leq i \leq n$. *Denoted by* $\boldsymbol{RG}$.

  - Note that the commutativity of R is not technically needed.
  - The associativity of multiplication follows from the associativity of the group operation in G.
  - RG is commutative iff G is abelian.
  - If $g_1 \in G$ is the identity of G, then we denote $a_1 g_1$ by a_1.
  - Similarly, if $1 \in R$ is the multiplicative identity of R, then we denote $1g_i$ by g_i.
- Dummit and Foote (2004) gives an example sum and product evaluation in $\mathbb{Z}D_8$.
- R appears in RG as the "constant" formal sums, that is, the R-multiples of the identity of G.
  - You can check that addition and multiplication on RG when restricted to these elements is just addition and multiplication on R.
  - These "elements of R" commute with all elements of RG.
  - The identity of R is the identity of RG.
- G appears in RG as the elements $1g_i$.
  - Multiplication in RG when restricted to these elements is just the group operation of G.
- Consequence: Each "element of G" has a multiplicative in RG (namely, its inverse in G).
  - Thus, G is a subgroup of the group of units of RG.
- If $|G| > 1$, then RG always has zero divisors.

  Proof. Pick $g \in G$ of order $m > 1$. Then

  $$(1-g)(1+g+\cdots+g^{m-1}) = 1 - g^m = 1 - 1 = 0$$

  so $1 - g$, for example, is a zero divisor. □
- If S is a subring of R, then SG is a subring of RG.
- **Integral group ring** (of G): The group ring of G with coefficients in $\mathbb{Z}$. *Denoted by* $\mathbb{Z}G$.
- **Rational group ring** (of G): The group ring of G with coefficients in $\mathbb{Q}$. *Denoted by* $\mathbb{Q}G$.
- If $H \leq G$, then RH is a subring of RG.
- Note that $\mathbb{R}Q_8 \neq \mathbb{H}$.
  - One difference is that $\mathbb{R}Q_8$ necessarily contains zero divisors, while $\mathbb{H}$ is a division ring and hence cannot contain zero divisors.
- Group rings over fields will be studied extensively in Chapter 18.

Exercises

1/7: **2.** Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be an element of the polynomial ring $R[X]$. Prove that $p(x)$ is a zero divisor in $R[X]$ iff there is a nonzero $b \in R$ such that $bp(x) = 0$. *Hint*: Let $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ be a nonzero polynomial of minimal degree such that $g(x)p(x) = 0$. Show that $b_m a_n = 0$ and so $a_n g(x)$ is a polynomial of degree less than m that also gives 0 when multiplied by $p(x)$. Conclude that $a_n g(x) = 0$. Apply a similar argument to show by induction on i that $a_{n-i}g(x) = 0$ for $i = 0, 1, \ldots, n$ and show that this implies $b_m p(x) = 0$.

Week 2

Ideals

2.1 Kernels, Ideals, and Quotient Rings

1/9:

- Some kid in the Discord takes photos of all of the boards every day. (link)
- Some announcements to start.
- Definitions of power series and polynomial rings posted in Canvas > Files.
- Next week: More lectures on rings of fractions.
- A note on defining $\mathbb{C}$ from $\mathbb{R}$ both intuitively and rigorously.
  - Intuitive definition: Let $i^2 = -1$, work out the relevant additive and multiplicative identities.
  - Rigorous definition: Proceeds in four steps.
    (i) Define a set: Let the ordered pair (a, b), where $a, b \in \mathbb{R}$, denote an entity called a "complex number," and denote the set of all complex numbers by $\mathbb{C}$.
    (ii) Define operations: Define $+, \times$ on $\mathbb{C}$ using the definitions suggested by the intuitive model.
    (iii) Confirm operations: Check that $+, \times$, as defined, satisfy the requirements of a ring.
    (iv) Introduce alternate notation: Henceforth, we shall denote the entity (a, b) by $a + ib$.
  - What is Step (v)?? Is there one?? Ask in OH.
- In fact, the four steps above are the template for the construction of all new rings from old rings.
  - Notice that we did the same thing with $R[[X]]$ last class, i.e., defined $R^{\mathbb{Z}_{\geq 0}}$, defined and confirmed operations, and introduced alternate notation ($\sum_{n=0}^{\infty} a_n X^n$ instead of $a : \mathbb{Z}_{\geq 0} \to R$).
  - Dummit and Foote (2004) explains this pretty well according to Nori.
- A question from both classes: What is X in the polynomial ring?
  - First ask: What does $a^7 + 6a^5 - 8 = 0$ mean?
    - It is a constraint that a must satisfy, given that a lies in some world (be it $\mathbb{R}$, $\mathbb{C}$, or elsewhere).
  - Then ask: What does $a^7 + 6a^5 - 8$ mean?
    - It is like a function $f(a)$.
    - It means that if $a \in R$, then $f(a)$ is defined in R, where R is a ring.
  - At this point, switch the arbitrary notation to $f(X) = X^7 + 6X^5 - 8$.
    - Then f is a function in $\mathbb{Z}[X]$.
    - But it is more than that, too: We know that if $x \in R$, R a ring, then $f(x) \in R$. Thus, the evaluation function $\mathrm{ev}_x : \mathbb{Z}[X] \to R$ is a ring homomorphism sending $f \mapsto f(x)$.

    - If $R \subset B$ is a subring, and $b \in B$, then $f \mapsto f(b)$ sending $R[X] \to B$ is a ring homomorphism. Additional implication in this case??
    - There is a problem if R is not commutative, though??
    - Also, does the fact that ev is a ring homomorphism follow from the universal property of a polynomial ring??
  - "Evaluation at a point is always a ring homomorphism."
    - Why does $\text{ev}_x : \mathbb{Z}[X] \to R$ send identities to identities? In this case, elements of $\mathbb{Z}[X]$ are of the form $1 + 2X$ and get mapped to elements of R of the form $1 + 2x$. The identity in $\mathbb{Z}[X]$ is 1, and thus it gets mapped to $1 \in R$, as desired.

- We now start the lecture officially.
- Today: Continuing doing what we did with groups but with rings.
- Last time: Extended the notions of subgroups and homomorphisms.
- Other concepts up for grabs:
  - Normal subgroups (recall that these arose as the kernels of group homomorphisms).
  - Quotient groups.
  - The FIT (aka the Noether isomorphism theorem),.
  - The second isomorphism theorem ($H_1, H_2 \triangleleft G$ implies $H_1 \cap H_2$ and H_1H_2 are normal; is this correct??).
- In the context of rings...
  - Normal subgroups become ideals.
    - These are not subrings in general.
  - Quotient groups become quotient rings.
  - The FIT does translate.
  - The other ITs also translate: If I_1, I_2 are two-sided ideals, then $I_1 \cap I_2$, $I_1 + I_2$, and I_1I_2 are also two-sided ideals. See Theorem 7.8.
- Constructing ideals.
- **Kernel** (of a ring homomorphism): The set defined as follows, where $f : A \to B$ is a ring homomorphism. *Denoted by* $\mathbf{\ker(f)}$. *Given by*

$$\ker(f) = \{a \in A : f(a) = 0\}$$

- Immediate consequences.

  (i) $\ker(f)$ is a subgroup of $(A, +)$.

  Proof. This statement follows from the fact that $f : (A, +) \to (B, +)$ is a group homomorphism by definition, and thus by results from last quarter, $\ker(f)$ is a subgroup (a *normal* subgroup even!). □

  (ii) If $h \in \ker(f)$ and $a \in A$, then both $ah, ha \in \ker(f)$.

  Proof. To prove that $ah, ha \in \ker(F)$, it will suffice to show that $f(ah) = 0$ and $f(ha) = 0$. For the first statement, we have

$$f(ah) = f(a)f(h) = f(a)0 = 0$$

  Note that the left distributive law implies the last equality. A symmetric argument holds for $f(ha) = 0$. Therefore, both $ah, ha \in \ker(f)$, as desired. □

- As certain properties of $\ker(f)$ motivated our definition of normal subgroups, some of the properties in the above proof will be used to motivate our definition of **ideals**.
- **Left ideal**: A subset I of a ring R for which $(I,+) \leq (R,+)$ and $aI \subset I$ for all $a \in R$.
- **Right ideal**: A subset I of a ring R for which $(I,+) \leq (R,+)$ and $Ia \subset I$ for all $a \in R$.
- **Two-sided ideal**: A subset I of a ring R for which $(I,+) \leq (R,+)$, and $aI \subset I$ and $Ia \subset I$ for all $a \in R$. *Also known as* **ideal**.
  - A two-sided ideal is both a left and right ideal.
- Having defined an analogy to normal subgroups, we can now construct quotient rings.
  - Much in the same way we can construct a quotient set (set of cosets) for any subset H but G/H is only a sub*group* if H is a normal subgroup, a quotient ring R/I is only a subring if I is an ideal.
- Review of quotient groups.
  - Given $H \leq G$, G/H is the set of left cosets of G (which is a subset of the **power set** of G).
- **Power set** (of A): The set of all subsets of A, where A is a set. *Denoted by* $\boldsymbol{\mathcal{P}(A)}$.
- **Quotient ring**: The following set, where $I \subset R$ is a two-sided ideal of a ring R. *Denoted by* $\boldsymbol{R/I}$. *Given by*
$$R/I = \{a + I : a \in R\}$$
  - A subset of $\mathcal{P}(R)$.
  - We define an associated projection function $\pi : R \to R/I$ by $\pi(a) = a + I$ for all $a \in R$.
- Don't we need I to be normal for R/I to be a group under $+$?
  - No, because $(R,+)$ is already abelian, so that takes care of the normality condition for all subgroups.
- We now define the other binary operation $\cdot$ on R/I.
  - In terms of π, we want $\cdot$ to satisfy $\pi(a \cdot b) = \pi(a) \cdot \pi(b)$ for all $a, b \in R$.
- To build intuition for how to do this, consider the following instructive example.
  - Suppose X has a binary operation $\cdot$ and $\pi : X \to Y$ is onto.
  - Question: Does there exist a binary operation $\cdot$ on Y such that π respects it, i.e.,
$$\pi(x_1 \cdot x_2) = \pi(x_1) \cdot \pi(x_2)$$
  - Let $y_1, y_2 \in Y$. Consider $\pi^{-1}(y_1), \pi^{-1}(y_2)$. They are both nonempty since π is onto by hypothesis. Thus, we can multiply the sets.
$$\pi^{-1}(y_1) \cdot \pi^{-1}(y_2) = \{x_1 \cdot x_2 : x_1 \in \pi^{-1}(y_1),\ x_2 \in \pi^{-1}(y_2)\}$$
  - If $\cdot : Y \times Y \to Y$ exists, then $\pi(\pi^{-1}(y_1) \cdot \pi^{-1}(y_2))$ must be a singleton set, i.e.,
$$\pi(\pi^{-1}(y_1) \cdot \pi^{-1}(y_2)) = \{y_1 \cdot y_2\}$$
  - Conversely, if $\pi(\pi^{-1}(y_1) \cdot \pi^{-1}(y_2))$ is a singleton for all $y_1, y_2 \in Y$, then $\cdot$ exists. Then $\{y_1 \cdot y_2\}$ defines $y_1 \cdot y_2$.
  - It is also useful to note the similarities in this approach to the one used to define $*$ on G/H in MATH 25700.

- Therefore, for all $\alpha_1, \alpha_2 \in R/I$, it suffices to check that $\pi(\pi^{-1}(\alpha_1) \cdot \pi^{-1}(\alpha_2))$ is a singleton.
  - More explicitly, we know that there exist $a_1, a_2 \in R$ such that $\alpha_i = a_i + I$ $(i = 1, 2)$.
  - In particular, we know from group theory that $\pi^{-1}(\alpha_i) = a_i + I \subset R$ $(i = 1, 2, \dots)$.
  - Thus,

$$\begin{aligned}\pi^{-1}(\alpha_1) \cdot \pi^{-1}(\alpha_2) &= (a_1 + I) \cdot (a_2 + I) \\ &= \{(a_1 + c_1)(a_2 + c_2) : c_1, c_2 \in I\} \\ &= \{a_1 \cdot a_2 + a_1 \cdot c_2 + c_1 \cdot (a_2 + c_2) : c_1, c_2 \in I\}\end{aligned}$$

    Since c_2, c_1 are part of an ideal, $a_1 c_2$ and $c_1(a_2 + c_2)$ are elements of I. Since $I \leq (R, +)$, the sum of the terms is also an element of I. Thus, we can combine all of these terms into I, leaving only $a_1 a_2$ behind. Therefore, the above is a...

$$\subset a_1 a_2 + I$$

  - Therefore,

$$\pi(\pi^{-1}(\alpha_1) \cdot \pi^{-1}(\alpha_2)) = \{a_1 a_2 + I\}$$

    which is a singleton.

- Implication: Multiplication on R/I is defined as expected, i.e.,

$$(a_1 + I) \cdot (a_2 + I) := a_1 \cdot a_2 + I$$

  is well-defined.

- A consequence: $a_1 - a_1' \in I$ and $a_2 - a_2' \in I$ implies that $a_1 a_2 - a_1' a_2' \in I$.
  - How do we know this??

- We know that (i) $\pi(a + b) = \pi(a) + \pi(b)$, (ii) $\pi(a \cdot b) = \pi(a) \cdot \pi(b)$, and (iii) π is onto.
  - Thus, all laws and formulas that we would expect the quotient ring to obey (as a ring) are trivial to prove.

- Example: Check that

$$\alpha_1 \cdot (\alpha_2 + \alpha_3) = (\alpha_1 \cdot \alpha_2) + (\alpha_1 \cdot \alpha_3)$$

  for all $\alpha_1, \alpha_2, \alpha_3 \in R/I$.
  - Choose $a_i \in R$ such that $\pi(a_i) = \alpha_i$ $(i = 1, 2, 3)$.
  - We know since R is a ring that

$$a_1 \cdot (a_2 + a_3) = (a_1 \cdot a_2) + (a_1 \cdot a_3)$$

  - Apply π. Then

$$\begin{aligned}\alpha_1 \cdot \pi(a_2 + a_3) &= (\alpha_1 \cdot \alpha_2) + (\alpha_1 \cdot \alpha_3) \\ \alpha_1 \cdot (\alpha_2 + \alpha_3) &= (\alpha_1 \cdot \alpha_2) + (\alpha_1 \cdot \alpha_3)\end{aligned}$$

2.2 Office Hours (Nori)

- Can you confirm that in every subring M of a ring R, $n_R x = x n_R$ for all $n \in \mathbb{Z}$?
  - Yes.
- $aX = Xa$ statement?
  - We must have this in order to be able to factor the coefficients out in the definition of multiplication. Otherwise, we would not have $a_p X^p b_q X^q = a_p b_q X^p X^q$ in general.
  - We postulate this as an additional condition.
- What did you mean when you wrote "scratch" at the beginning of your proof of the Universal Property of a Polynomial Ring?
  - Means he isn't writing down a proof nicely, but just giving enough of an idea of the arguments used so that we can write out the rest on our own.
- Step (v) in constructing new rings from old ones?
  - Step (0) is you need to already have something in mind (e.g., $\mathbb{C}$ or power series).
  - Step (iv) is informal and not necessarily justified by the laws of algebra. It can and will be justified in a later course on algebra (namely, a first-year graduate course on algebra) using **completions** of rings.
  - Step (v) is a formal way of introducing new notation. It only works explicitly for the complex numbers; for power series, we would need completions. Here's an outline, though, of what can be done for $\mathbb{C}$:
    - Define $j : \mathbb{R} \to \mathbb{C}$ by $a \mapsto (a, 0)$ and check that it is a ring homomorphism.
    - Define $i = (0, 1) \in \mathbb{C}$.
    - Define a map from $\mathbb{R} \times \mathbb{R} \to \mathbb{C}$ by $(a, b) \mapsto j(a) + ij(b)$. The laws of multiplication on $\mathbb{C}$ will confirm that $j(a) + ij(b)$ is precisely the element (a, b) in the rigorous version of $\mathbb{C}$ we've previously defined.
    - This formally justifies the switch of notation.
- What was the point of switching the context of the evaluation function to a subring?
  - The point is that evaluation at a point outside of the ring is still a ring homomorphism, provided that b commutes with all $a \in R$ and the functions under consideration are polynomials.
    - We need polynomials and commutativity of the elements to guarantee that $(fg)(b) = f(b)g(b)$ — same reason as the earlier $a_p X^p b_q X^q = a_p b_q X^p X^q$ example.
  - Example of where this matters.
    - Consider the ring of functions $f : \mathbb{R} \to \mathbb{R}$, on which the evaluation function is a ring homomorphism.
    - Letting $i \in \mathbb{C}$ be the unit imaginary number, it is not true that $\mathrm{ev}_i : \mathbb{R}^{\mathbb{R}} \to \mathbb{R}$ is a ring homomorphism since only certain functions on the reals can naturally be extended to the complex numbers.
    - However, consider the subring $\mathbb{R}[X]$ of $\mathbb{R}^{\mathbb{R}}$. Since i does commute with every real number and polynomials are made of products of real numbers and i, $\mathrm{ev}_i : \mathbb{R}[X] \to \mathbb{R}$ *is* a ring homomorphism.
  - All of this should be kept in mind, but it's not too important at this point.
  - Misc. note: Think more about why it's so "obvious" that evaluating at a point defines a ring homomorphism.
    - Perhaps it's not so much that it's "obvious" as that it follows directly from the axioms and not much creativity is needed in the proof.

- Was there a problem if R is not commutative with the evaluation function?
  - See above.
- Does the fact that ev is a ring homomorphism follow from the universal property of a polynomial ring?
  - Maybe? Didn't want to belabor the point.
- Is the in-class statement of the SIT correct?
  - That the product of two normal subgroups is normal is true, but it is not part of the SIT. In fact, it is part of one of the other isomorphism theorems. Nori just included these SIT and other statements to show what can be transferred. We will not talk about these results further, though, because they can all be deduced from the FIT.
- How do we know the subtraction/multiplication statement?
  - Two ways of looking at this.
    1. Proof in terms of coset properties.
       - $a_i' \in a_i + I$ iff $a_i' + I = a_i + I$.
       - Thus,
$$(a_1 + I) \cdot (a_2 + I) = (a_1' + I) \cdot (a_2' + I)$$
$$a_1 a_2 + I = a_1' a_2' + I$$
       so
$$a_1 a_2 - a_1' a_2' \in I$$
    2. Proof in terms of a clever trick and properties of ideals.
       - We are given $a_1 - a_1' \in I$ and $a_2 - a_2' \in I$.
       - We can write that
$$a_1 a_2 - a_1' a_2' = (a_1 - a_1')a_2 + a_1'(a_2 - a_2')$$
       - The two terms in parentheses on the RHS above are in I by hypothesis.
       - Since I is a two-sided ideal, $(a_1 - a_1'), (a_2 - a_2') \in I$, and $a_2, a_1' \in R$, we have that $(a_1 - a_1')a_2, a_1'(a_2 - a_2') \in I$.
       - Since I is a subgroup (and hence closed), $(a_1 - a_1')a_2 + a_1'(a_2 - a_2') \in I$, as desired.

2.3 Noether Isomorphism Theorem, Ideal Types, and Intro to Rings of Interest

1/11:

- When mathematicians write papers, they often choose conventions that may not be standard. Nori will presently define a few of these for our class.
- **Canonical surjection**: The function from $R \to R/I$, where R is a ring and I is a two-sided ideal of R, defined as follows. *Denoted by* $\boldsymbol{\pi}$. *Given by*
$$\pi(a) = a + I$$
- **Canonical injection**: The natural inclusion map from $A \to B$, where A is a subring of B, defined as follows. *Denoted by* $\boldsymbol{i}$. *Given by*
$$i(a) = a$$
- Both maps are ring homomorphisms and are onto.

- Theorem (Noether Isomorphism Theorem): Let $f : A \to B$ be a ring homomorphism, and let $I = \ker(f)$. Then f has a (unique) factorization

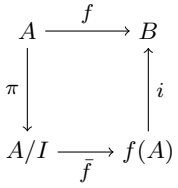

Figure 2.1: Noether isomorphism theorem.

where $\bar{f}$ is an isomorphism of rings.

Proof. If we ignore $\times$ and regard A, B as additive abelian groups, the FIT applies and yields the above (unique) factorization. In it, $\bar{f}$ is a bijective additive isomorphism (group homomorphism). Thus, this takes care of proving that $\bar{f}$ respects addition.

We now just need to prove that $\bar{f}$ respects multiplication and sends 1 to 1 to complete our verification that it is a ring homomorphism. We will do this indirectly. First, observe that f is a ring homomorphism and i is an injective ring homomorphism. Thus, $\bar{f} \circ \pi = i^{-1} \circ f$ is a ring homomorphism (as we can confirm). This combined with the fact that π is onto implies that $\bar{f}$ is a ring homomorphism (as we can confirm).

This essentially completes our proof; we just need the formal definition of an isomorphism of rings to take it to the finish line. □

- Notes on the Noether Isomorphism Theorem.
  - Nori leaves out some of the grueling detail in this proof in favor of a simple statement of the idea (the "as we can confirm" statements) because we can work out that detail for ourselves.
    - Nori accidentally presented all of the detail last class, and people got very confused.
    - The language used in the proof we have now is not intended to confuse but to provide intuition; we can investigate rigor to whatever depth we choose.
  - More on the structure of the decomposition: π is the canonical surjection and i is the canonical injection; $\bar{f}$ is in the middle.
  - See Theorem 7.7.

- **Isomorphism** (of rings): A ring homomorphism $f : A \to B$ for which...

  (i) There exists a corresponding ring homomorphism $g : B \to A$ such that...

  (ii) $f \circ g = \mathrm{id}_A$ and $g \circ f = \mathrm{id}_B$.

- Notes on the definition of an isomorphism of rings.
  - If f is a ring homomorphism, then (ii) implies that f is a bijection of sets.
    - Implication: If f is a ring homomorphism and if f is a bijection, then there exists a function $g : B \to A$ such that (ii) holds.
    - It is fairly clear that this g is also a ring homomorphism.
  - "Iso" means bijective homomorphism.
  - We need bijectivity because continuous functions don't necessarily have continuous inverses??
    - Essentially, there are two different but related definitions of an isomorphism.
    - Typically, we just say that it's a bijective homomorphism. But sometimes, we actually *need* the f, g definition. See OH.

- Let's go back to talking about ideals.
- **Principal left ideal**: An ideal of the following form, where R is a ring and $b \in R$. *Denoted by* $\boldsymbol{Rb}$. *Given by*
$$Rb = \{ab : a \in R\}$$
  - $(Rb, +)$ is an additive subgroup of R.
    - This follows from the fact that $r_b : (R, +) \to (R, +)$ is a group homomorphism and Rb is equal to the image $r_b(R)$ of R under this group homomorphism.
  - This motivates some of the linear algebra exercises in HW2.
    - In particular, it underlies HW2 Q9.
  - There also exist principal right ideals and principal two-sided ideals.
  - It is correct that Rb is a principal "left" ideal (closed under *left* multiplication by elements of R), even though Hg is a "right" coset (multiplying the coset by an element of G on the right).
- Let $c \in R$, let $h \in Rb$. Is $ch \in Rb$?
  - Yes, because $h = ab$ implies that there exists $a \in R$ such that $ch = (ca)b \in Rb$.
- We now look at three constructions originating from ideals: Sums, intersections, and products.
- **Sum** (of ideals): The ideal defined as follows, where $I, J \subset R$ are ideals. *Denoted by* $\boldsymbol{I + J}$. *Given by*
$$I + J = \{a + b : a \in I,\ b \in J\}$$
  - Definitions for left, right, and two-sided ideals.
  - We can check all of the properties to confirm that this is an ideal.
  - Let $\alpha \in R$, $\alpha I \subset I$. Well $\alpha I \subset J$ implies $\alpha(I + J) \subset I + J$.
- Let $\{I_\lambda\}_{\lambda \in \Lambda}$ be a (finite??) family of ideals (left, right, or two-sided). Then
$$\sum_{\lambda \in \Lambda} I_\lambda = \{a_1 + a_2 + \cdots + a_n : n \in \mathbb{N}, a_i \in I_{\lambda_i} \text{ for some } \lambda_i \in \Lambda\}$$
  is a (left, right, or two-sided) ideal.
- Example: Given $a_1, a_2 \in R$, $Ra_1 + Ra_2$ is a left ideal.
  - Note that it is not a principal ideal, however.
- R a ring implies that $R[X]$ is a ring, which in turn implies that $R[X][Y] = R[X, Y]$ is also a ring.
  - Let $R[X, Y] = A$ and $R = \mathbb{R}$. Then, for instance,
$$AX + AY = \{f(X, Y)X + g(X, Y)Y : f, g \in A\}$$
  - All of these functions vanish at $(0, 0)$. Thus, this ideal is not prime.
    - It'll be a while before we treat such rings formally.
    - We can take this claim as an exercise for now, though.
  - Note that similarly, AX is the set of all functions vanishing on the y-axis.
- **Intersection** (of ideals): The ideal defined as follows, where $\{I_\lambda\}_{\lambda \in \Lambda}$ is a family of ideals. *Given by*
$$\bigcap_{\lambda \in \Lambda} I_\lambda$$
  - If all I_λ are left (resp. right, two-sided) ideals, then the intersection is a the same kind of ideal.

- **Product** (of ideals): The ideal defined as follows, where I, J are ideals. *Denoted by* $\boldsymbol{IJ}$. *Given by*

$$IJ = \{a_1b_1 + \cdots + a_nb_n : n \in \mathbb{N},\ a_1, \ldots, a_n \in I,\ b_1, \ldots, b_n \in J\}$$

  - Note that $IJ \neq \{ab : a \in I, b \in I\}$. This is not even a subgroup under addition.
  - IJ as defined, however, is a subgroup with respect to $+$.
  - The fact that IJ is an ideal is justified by the distributive law:

$$\alpha(a_1b_1) + \cdots + \alpha(a_nb_n) = (\alpha a_1)b_1 + \cdots + (\alpha a_n)b_n$$

    - Note that the term on the far right is an element of IJ since $\alpha a_i \in I_{\lambda_i}$ by the definition of I_{λ_i} as an ideal.
  - Alternate form:

$$IJ = \sum_{b \in J} Ib$$

- Let R be a commutative ring, and let I, J be ideals. Do we know that $IJ \subset I$?
  - Yes, since the set is closed under multiplication as an ideal.
    - In particular, $a \in I$ and $b \in R$ imply $ab \in I$.
  - Same logic: $IJ \subset J$.
  - Combining these results: $IJ \subset I \cap J$.
  - $IJ = I \cap J$ iff I, J are both two-sided ideals??
  - In fact, if I is a left ideal and J is a right ideal, then IJ is a 2-sided ideal.
- Example: Let $R = \mathbb{Z}$.
  - Then ideals I, J are necessarily of the form $I = \mathbb{Z}d$, $J = \mathbb{Z}e$ for $d, e \in R$.
  - It follows that $IJ = \mathbb{Z}de$ and $I \cap J = \mathbb{Z}f$ where $f = \operatorname{lcm}(d, e)$.
- We now start talking about the rings we'll focus on for the rest of the course.
- Zero rings.
  - Nothing much to be said here.
- **Field**: A commutative ring F such that...

  (i) $0_F \neq 1_F$.

  (ii) $a \in F$ and $a \neq 0$ implies that there exists $b \in F$ such that $ab = 1$.
- Observation: If $I \subset F$ is an ideal in a field F, then either $I = \{0\}$ or $I = F$.

  Proof. If $I \neq \{0\}$, then there exists $a \in I$ which is nonzero. It follows since F is a field that $1 = a^{-1}a \in I$. Therefore, $b = b \cdot 1 \in I$ for all $b \in F$, i.e., $I = F$. □
- The converse of this observation is also true (for commutative rings).
  - Namely, if the only ideals of a commutative ring R are $\{0\}$ and R, then R is a field.
- Examples of fields: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ where p is prime.
  - $\mathbb{Z} \subset \mathbb{Q}$ is not a field.
- **Integral domain**: A commutative ring A for which

  1. $0_A \neq 1_A$;
  2. $a, b \in A$, $a \neq 0$, and $ab = 0$ imply $b = 0$.
- The cancellation lemma holds in integral domains.
  - Namely, if A is an integral domain and $a, b, c \in A$, then $ab = ac$ and $a \neq 0$ imply that $b = c$.

2.4 Office Hours (Callum)

- HW1 Q11.
  - I need to factor in some -1's to account for all integers $\mathbb{Z}$.
- Do we have to justify $0 \cdot x = 0$ in our proof of HW1 Q1?
  - It's ok to assume things like this that were either covered in class or in the relevant sections of Dummit and Foote (2004).
- Do we need to go more formal for HW1 Q2, explaining different forms of addition, functional equality, etc.?
- Additional sophistication in HW1 Q10?
- Using HW1 Q7 to solve HW1 Q9?
  - Use the diagonal $\Delta : R \to R \times R$[1] defined by $r \mapsto (r, r)$.
  - We know that Δ is a ring homomorphism (see HW1 Q4) and that $A \times B \subset R \times R$ is a subring.
  - It follows from the set theoretic definition that $A \cap B = \Delta^{-1}(A \times B)$; apply HW 1 Q7.

2.5 Properties of Ideals

1/13:

- **Integral domain**: A commutative ring R satisfying the following two conditions.
  (a) $0_R \neq 1_R$.
  (b) $a, b \in R$ with $a, b \neq 0$ implies $ab \neq 0$.
- All subrings of fields are integral domains (proved later).
- **Degree** (of $f \in R[X]$ nonzero): The number $\max S$, where
$$S = \{n \in \mathbb{Z}_{\geq 0} : a_n \neq 0\}$$
Denoted by $\boldsymbol{\deg(f)}$.
  - Some people call the degree of the zero polynomial "-1."
  - f a polynomial implies that S is finite.
  - $f \neq 0$ implies $S \neq \emptyset$.
- **Leading coefficient** (of $f \in R[X]$ nonzero): The number a_d, where $d = \deg(f)$. *Denoted by* $\boldsymbol{\ell(f)}$.
- Proposition: If R is an integral domain, then $R[X]$ is an integral domain.

  Proof. Let $f, g \in R[X]$ both be nonzero polynomials of degrees d, e with leading coefficients a_d, a_e. In particular, let
  $$f = a_0 + \cdots + a_d X^d \qquad\qquad g = b_0 + \cdots + b_e X^e$$
  Thus, by the definition of multiplication on $R[X]$,
  $$fg = a_0 b_0 + \cdots + a_d b_e X^{d+e}$$
  Since $a_d, b_e \neq 0$ by the hypothesis that they are the leading coefficients of nonzero polynomials and since R is an integral domain, we know that $a_d b_e \neq 0$. Thus, $\deg(fg) = d + e$ and the leading coefficient is $a_d b_e$, so fg is nonzero, as desired. □

[1] It is standard notation to use Δ for this function.

- Corollary: $R[X][Y] = R[X, Y]$ is an integral domain.
- Corollary: $R[X_1, \ldots, X_n]$ is an integral domain for all $n \in \mathbb{N}$.
- **Monic** (polynomial): A polynomial with leading coefficient 1.
  - Examples: $1, X + a, X^2 + aX + b$.
- Multiplying any polynomial by a monic polynomial yields a nonzero polynomial.
- Exercise: If $f \in R[X]$ is monic, then $l_f : R[X] \to R[X]$ is injective.

  Proof. Let $d = \deg(f)$ and let $e = \deg(g)$ for some nonzero $g \in R[X]$. $g \neq 0$ implies that the leading coefficient of g is some $b \neq 0$. Hence, the leading coefficient of fg has no term of degree greater than $d + e$, and the coefficient of the X^{d+e} term is $1b$.

  This shows nonzero; technically also need to show distinctness under left multiplication. □

- **Characteristic** (of a ring): 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 $m \mapsto m_R$. *Denoted by* $\mathbf{char(}\boldsymbol{R}\mathbf{)}$.
- If $\text{char}(R) = 1$, then R is the zero ring.
- We have $\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/\ker(j) \hookrightarrow R$.
- All polynomials (the fields we have considered thus far) have characteristic 0.
- The subrings of an integral domain are integral domains.

  Proof. char(integral domain) is either 0 or a prime number. □

- Question: Given an ideal I in a ring R, when is R/I a field? An integral domain?
- Recall that if R is a commutative ring, then TFAE.
  1. $1_R \neq 0_R$ and $a \in R$, $a \neq 0$ implies that there exists $b \in R$ such that $ab = 1$.
  2. There are exactly two ideals of R (specifically, $\{0\}$ and R).

  Proof. (2) ⇒ (1) is easy. Implies $1 \neq 0$ check. If $a \in R$, $a \neq 0$, then $\{0\} \subsetneq Ra$. The hypothesis implies that $Ra = R$ and $1 \in R$. Thus, there exists $b \in R$ such that $ba = 1$.

  (1) ⇒ (2): Not covered in class. □

- R is a field if it satisfies $1 \sim 2$.
- Question: I is an ideal of R. How is $\{\text{ideals in } R\}$ related to $\{\text{ideals in } R/I\}$?
  - Consider the canonical surjection $\pi : R \to R/I$, often denoted by $\pi(a) = \bar{a}$ for all $a \in R$.
    (a) If $J \subset R$ is an ideal, is $\pi(J)$ an ideal in R/I?
      - $(J, +)$ is a subgroup of $(R, +)$. This implies that $\pi(J)$ is a subgroup of $(R/I, +)$. Let $a \in R$. Then J an ideal implies that $aJ \subset J$, which implies that $\pi(a)\pi(J) = \pi(aJ) \subset \pi(J)$. If $\alpha \in R/I$, then there exists $a \in R$ such that $\pi(a) = \alpha$, so this holds, as desired.

    (b) $H \subset R/I$ is an ideal. Is $\pi^{-1}(H)$ an ideal?
      - Yes. Additionally, no luck was required (we didn't use any assumptions).
      - This is pretty close to a homework problem (HW2 Q3).
      - We're assuming I is a nonzero ideal here.
      - Consider a map from the set of ideals in R/I to the set of ideals of R that contain I. H is in the first set; $\pi^{-1}(H)$ is in the second set. But $\pi(\pi^{-1}(H)) = H$ because π is onto.

    - Injectivity: If H_1, H_2 are ideals of R/I and $\pi^{-1}(H_1) = \pi^{-1}(H_2)$, then $\pi\pi^{-1}H_1 = \pi\pi^{-1}H_2$, i.e., $H_1 = H_2$.
    - Surjectivity: If $R \supset J \supset I$, J an ideal, then $\pi(J)$ is also an ideal of R/I and J/I.
- Takeaway: Every ideal of R/I equals J/I for a unique ideal J of R such that $J \supset I$.
- Exercise: $R/J \cong (R/I)/(J/I)$ using nothing but the FIT. See Theorem 7.8(2).
- Recall that we got into this discussion trying to figure out what properties of I make R/I into a field. Now that we have more tools, we return to the problem directly.
- Let $I \subset R$ be an ideal such that R/I is a field. This is true iff R/I has exactly two ideals, and iff there are exactly two ideals $R \supset J \supset I$.
  - This is true if $I \neq R$ and J an ideal of R and $I \subset J$ implies $J = R$ is called a **maximal ideal**.
  - Ideals I with this property are **maximal ideals**.
  - Proposition: R/I is a field implies I is a maximal ideal.
- HW3: Basic problems and some easy linear algebra problems.
- There will be Nori office hours on Monday. He will come in-person unless it's very cold, and in that case, they will be virtually.

2.6 Chapter 7: Introduction to Rings

From Dummit and Foote (2004).

Section 7.3: Ring Homomorphisms and Quotient Rings

1/9:

- Definition of a **ring homomorphism** and a **kernel** (of a ring homomorphism).
- **Isomorphism**: A bijective ring homomorphism. *Denoted by* $\cong$.
- Examples of ring homomorphisms.
  1. The map $\varphi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ which sends even integers to 0 and odd integers to 1.
     - Dummit and Foote (2004) proves that this map satisfies the requisite stipulations.
     - Note that φ can be viewed as a projection function from the fiber bundle $\mathbb{Z}$ to be base space $\mathbb{Z}/2\mathbb{Z}$, where the even and odd integers are the two fibers.
  2. $\phi_n : \mathbb{Z} \to \mathbb{Z}$ defined by $\phi_n(x) = nx$ is *not* a ring homomorphism in general.
     - Reason: We only have
     $$\phi_n(xy) = nxy = n^2xy = nxny = \phi_n(x)\phi_n(y)$$
     when $n = n^2$, i.e., when $n = 0, 1$.
     - ϕ_0 is the **zero homomorphism** (on $\mathbb{Z}$) and ϕ_1 is the **identity homomorphism** (on $\mathbb{Z}$).
     - Note that ϕ_n is a *group homomorphism* from $(\mathbb{Z}, +)$ to itself for all n.
  3. $\varphi : \mathbb{Q}[X] \to \mathbb{Q}$ defined by $\varphi(p) = p(0)$.
     - Just like the evaluation function discussed in class.
     - $\ker\varphi$ is the set of all polynomials with constant term 0.
- Images and kernels of ring homomorphisms are subrings.

  Proposition 7.5. Let R, S be rings and let $\varphi : R \to S$ be a homomorphism.

  1. The image of φ is a subring of S.

2. The kernel of φ is a subring of R. Furthermore, if $\alpha \in \ker\varphi$, then $r\alpha, \alpha r \in \ker\varphi$ for every $r \in R$, i.e., $\ker\varphi$ is closed under multiplication by elements from R.

Proof. Given. □

- Motivating the definition of a quotient ring.
  - Let $\varphi : R \to S$ have kernel I.
  - The fibers of φ are the additive cosets $r + I$ of the kernel I.
  - Recall that in the FIT, we saw that the fibers of φ have the structure of a group naturally isomorphic to the image of φ, which led to the notion of a quotient group by a normal subgroup.
  - An analogous result holds for rings, i.e., the fibers of a ring homomorphism have the structure of a ring naturally isomorphic to the image of φ, and this motivates the definition of a quotient ring.
  - The whole passage about this on Dummit and Foote (2004, pp. 240–41) is very well written and worth rereading!
- Dummit and Foote (2004) motivates ideals from the perspective of, "what properties must I have such that R/I is a subring?"
- "The ideals of R are exactly the kernels of the ring homomorphisms of R (the analogue for rings of the characterization of normal subgroups as the kernels of group homomorphisms)" (Dummit & Foote, 2004, p. 241).
- Dummit and Foote (2004) motivates and defines the definition of **ideals**.
  - There are differences from the in-class definition, though: In particular, according to Dummit and Foote (2004)'s definition of subrings, an ideal is a subring, but according to the in-class definition (which additionally requires that $1_R \in I$), ideals are not subrings in general.
  - All definitions of an ideal coincide for commutative rings.
- R/I is a ring iff I is an ideal.

  Proposition 7.6. Let R be a ring and let I be an ideal of R. Then the (additive) quotient group R/I is a ring under the binary operations

  $$(r + I) + (s + I) = (r + s) + I \qquad (r + I) \times (s + I) = (rs) + I$$

  for all $r, s \in R$. Conversely, if I is any subgroup such that the above operations are well-defined, then I is an ideal of R.
- Definition of a **quotient ring**.
- Isomorphism theorem analogies.

  Theorem 7.7.

  1. (The First Isomorphism Theorem for Rings) If $\varphi : R \to S$ is a homomorphism of rings, then the kernel of φ is an ideal of R, the image of φ is a subring of S, and $R/\ker\varphi$ is isomorphic as a ring to $\varphi(R)$.
  2. If I is any ideal of R, then the **natural projection** of R onto R/I is a surjective ring homomorphism with kernel I. Thus, every ideal is the kernel of a ring homomorphism and vice versa.

  Proof. Given (see Lecture 2.2). □
- **Natural projection** (of R onto R/I): The map from $R \to R/I$ defined as follows. *Denoted by* $\boldsymbol{\pi}$. *Given by*

  $$\pi(r) = r + I$$

- As with groups, we shall often use the bar notation for reduction mod I: $\bar{r} = r + I$.
  - With this notation, addition and multiplication in the quotient ring become

$$\bar{r} + \bar{s} = \overline{r+s} \qquad\qquad \bar{r}\bar{s} = \overline{rs}$$

- Examples.
  1. R and $\{0\}$ are ideals. **Trivial** and **proper** ideals.
  2. $n\mathbb{Z}$ for any $n \in \mathbb{Z}$.
     - These are also the only ideals of $\mathbb{Z}$ since they are the only subgroups of $\mathbb{Z}$.
     - The associated quotient rings are $\mathbb{Z}/n\mathbb{Z}$.
     - Addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ is re-explained as normal addition and multiplication followed by **reducing mod n**.
  3. $I \subset \mathbb{Z}[X]$ consisting of all polynomials whose terms are of degree at least 2.
     - Operations: Normal and then reduction, similar to Example 2.
     - Note that $\mathbb{Z}[X]/I$ has zero divisors (e.g., $\bar{x}$ since $\bar{x}\bar{x} = \overline{x^2} = \bar{0}$) even though $\mathbb{Z}[X]$ does not.
  4. The kernel of the **evaluation** function.
     - This is the set of all functions $f : X \to A$, where X is a set and A is a ring, such that $f(c) = 0$.
     - Since E_c is surjective (consider all constant functions), $A^X / \ker E_c \cong A$.
     - Dummit and Foote (2004) also considers the special case $C([0,1], \mathbb{R})$, and notes that more generally, the fiber of E_c above the real number y_0 is the set of all continuous functions that pass through the point (c, y_0).
  5. $\ker E_0 : R[X] \to R$.
     - We can compose E_0 with any other homomorphism from $R \to S$ to obtain a ring homomorphism from $R[X] \to S$. For instance, if the latter homomorphism is reduction mod 2, then the fibers of the overall homomorphism are the polynomials with even constant terms and those with odd constant terms.
  6. $M_n(J)$ is a two-sided ideal of $M_n(R)$, provided J is any ideal of R.
     - This ideal is the kernel of the surjective homomorphism from $M_n(R) \to M_n(R/J)$. Example: $M_3(\mathbb{Z})/M_3(2\mathbb{Z}) \cong M_3(\mathbb{Z}/2\mathbb{Z})$.
     - If R is a ring with identity, then every two-sided ideal of $M_n(R)$ is of the form $M_n(J)$ for some two-sided ideal J of R.
  7. The **augmentation ideal**.
     - The augmentation map is surjective, so the augmentation ideal is isomorphic to R.
     - Another ideal in RG is the formal sums whose coefficients are all equal, i.e., the R-multiples of $g_1 + \cdots + g_n$.
  8. $L_j \subset M_n(R)$ consisting of all $n \times n$ matrices with arbitrary entries in the j^{th} column and zeroes in all other columns is a left ideal of $M_n(R)$.
     - If $A \in L_j$ and $T \in M_n(R)$, the matrix multiplication implies that $TA \in L_j$.
     - Showing that L_j is not a right ideal: $E_{1j} \in L_j$ but $E_{1j}E_{ji} = E_{1i} \notin L_j$ if $i \neq j$.
     - We can develop an analogous selection of right ideals in $M_n(R)$.

- **Trivial ideal**: The ideal $\{0\}$. *Denoted by* $\mathbf{0}$.
- **Proper** (ideal): An ideal I such that $I \neq R$.
- **Reduction mod n**: The natural projection $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.

- **Evaluation** (at c): The map from $A^X \to A$, where A is a ring and X is a nonempty set, defined as follows, where $c \in X$. *Denoted by* $\boldsymbol{E_c}$. *Given by*

$$E_c(f) = f(c)$$

- **Augmentation map**: The map from $RG \to R$ defined as follows. *Given by*

$$\sum_{i=1}^{n} a_i g_i \mapsto \sum_{i=1}^{n} a_i$$

- **Augmentation ideal**: The set of elements of RG whose coefficients sum to 0.
  - The kernel of the augmentation map.
  - Example: $g_i - g_j$ is an element of the augmentation ideal for all $1 \leq i, j \leq n$.
- $\boldsymbol{E_{pq}}$: The matrix with 1 in the p^{th} row and q^{th} column and zeroes elsewhere.

1/11:

- Dummit and Foote (2004) does a deep dive on reduction mod n and how it relates to the foundations of **Diophantine equations** (interesting but irrelevant).
- The remaining isomorphism theorems.

Theorem 7.8.

1. (The Second Isomorphism Theorem for Rings) Let A be a subring and let B be an ideal of R. Then $A+B = \{a+b : a \in A, b \in B\}$ is a subring of R, $A \cap B$ is an ideal of A, and $(A+B)/B \cong A/(A \cap B)$.
2. (The Third Isomorphism Theorem for Rings) Let I, J be ideals of R with $I \subset J$. Then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.
3. (The Fourth Isomorphism Theorem for Rings) Let I be an ideal of R. The correspondence $A \leftrightarrow A/I$ is an inclusion-preserving bijection between the set of subrings A of R that contain I and the set of subrings of R/I. Furthermore, A (a subring containing I) is an ideal of R if and only if A/I is an ideal of R/I.

Proof. All proofs follow the same structure: "First use the corresponding theorem from group theory to obtain an isomorphism of *additive groups* (or correspondence of groups, in the case of the Fourth Isomorphism Theorem) and then check that this group isomorphism (or correspondence, respectively) is a multiplicative map, and so defines a *ring* isomorphism. In each case the verification is immediate from the definition of multiplication in quotient rings" (Dummit & Foote, 2004, p. 246). □

- Definition of **sum**, **product** of ideals.
  - Note that n is not fixed in the product definition, so that all *finite* sums (not just all sums of length n for n fixed) are included in the set.
- $\boldsymbol{n^{\text{th}}}$ **power** (of I): The set consisting of all finite sums of elements of the form $a_1 a_2 \cdots a_n$ with $a_i \in I$ for all i. *Denoted by* $\boldsymbol{I^n}$.
  - Alternate definition: Define $I^1 = I$ and $I^n = II^{n-1}$.
- $I + J$ is the smallest ideal of R containing both I and J.
- IJ is an ideal contained in $I \cap J$ (but may be strictly smaller).
- Examples.
  1. Let $I = 6\mathbb{Z}$ and $J = 10\mathbb{Z}$.
     - $I + J$ consists of all integers of the form $6x + 10y$.

- In particular, all of these integers are divisible by 2, so $I + J \subset 2\mathbb{Z}$. On the other hand, $2 = 6(2) + 10(-1) \in I + J$ implies that $2\mathbb{Z} \subset I + J$. Therefore, $I + J = 2\mathbb{Z}$.
- In general, $m\mathbb{Z} + n\mathbb{Z} = \gcd(m, n)\mathbb{Z}$

– IJ consists of all integers of the form $(6x)(10y)$ (note that this does account for all finite sums due to the distributive law), i.e., in $60\mathbb{Z}$.

2. Let I be the ideal in $\mathbb{Z}[X]$ consisting of the polynomials with integer coefficients whose constant term is even.
   – We know, for example, that $2, x \in I$. Thus, $4 = 2 \cdot 2$ and $x^2 = x \cdot x$ are elements of $I^2 = II$, as is their sum $x^2 + 4$; however, $x^2 + 4$ cannot be written as a single product $p(x)q(x)$ of two elements of I.

Section 7.4: Properties of Ideals

1/18:

- **Ideal generated by A**: The smallest (two-sided) ideal of R containing $A \subset R$. *Denoted by* **(A)**.
  – When $A = \{a\}$ or $\{a_1, a_2, \dots\}$, we drop the set brackets and simply write (a) or $(a_1, a_2, \dots)$ for (A), respectively.
  – This idea is analogous to that of subgroups generated by subsets.
- Defines **products** of ideals.
  – $RA = 0$ if $A = \emptyset$.
- **Principal** (ideal): An ideal generated by a single element.
- **Finitely generated** (ideal): An ideal generated by a finite set A.
- (A) is the intersection of all ideals of R that contain A.

$$(A) = \bigcap_{\substack{I \text{ an ideal} \\ A \subset I}} I$$

  – This is because the intersection of any nonempty collection of ideals of R is also an ideal of R, and A is always contained in at least one ideal (namely, R).
- **Left ideal generated by A**: The intersection of all left ideals of R that contain A.
- We now prove that RA is the left ideal generated by A.
  – It follows from its definition that RA is closed under addition and left multiplication by any element of R. Thus, RA is a left ideal.
  – There exists $1_R \in R$. Thus, $A \subset RA$ (consider all finite sums $1_R a$ for $a \in A$).
  – Conversely, any left ideal I containing A must contain all finite sums of elements of the form ra ($r \in R$ and $a \in A$), so $RA \subset I$.
  – Therefore, RA is left ideal containing A, and is the smallest such ideal, so it must be the left ideal generated by A.
- Similar results.
  – AR is the right ideal generated by A.
  – RAR is the (two-sided) ideal generated by A.
  – If R is commutative, then $RA = AR = RAR = (A)$.

1/23:

  – Note that if R is not commutative, then

$$\{r_1 a s_1 + \cdots + r_n a s_n : n \in \mathbb{N},\ r_1, \dots, r_n, s_1, \dots, s_n \in R\} = RaR = (a) \neq \{ras : r, s \in R\}$$

- Principal ideals are analogous to cyclic subgroups in some ways.
  - For example, they are both generated by a single element.
  - They are also both easy ways of making subgroups and ideals, respectively.
- Containment relations between ideals (esp. principal ideals) in commutative rings captures some of the arithmetic of general commutative rings. In particular, if R is a commutative ring, then...
  - $b \in (a)$ iff $b = ra$ for some $r \in R$.
    - Alternatively, all elements of (a) are **multiples** of a in R.
    - Alternatively, a **divides** all elements of (a) in R.
  - $b \in (a)$ iff $(b) \subset (a)$.
- "Commutative rings in which all ideals are principal are among the easiest to study, and these will play an important role in Chapters 8 and 9" (Dummit & Foote, 2004, p. 252).
- Examples of generatable ideals.
  1. $0, R$ are always both principal since
  $$0 = (0) \qquad\qquad 1 = (1)$$
  2. $n\mathbb{Z} = \mathbb{Z}n = (n) = (-n)$ are principal ideals.
     - This rigorously justifies our notation $n\mathbb{Z}$, i.e., as an instance of aR.
     - Every ideal of $\mathbb{Z}$ is of this form; hence, every ideal of $\mathbb{Z}$ is principal.
     - $n\mathbb{Z} \subset m\mathbb{Z}$ iff $m \mid n$.
     - $(n, m) = (d)$, where $d = \gcd(n, m)$.
       - This justifies the notation (n, m) for gcd!!!
       - We do have to assert that $d > 0$, though.
     - In particular, $(n, m) = (1) = \mathbb{Z}$ iff n, m are relatively prime.
  3. $(2, X) \subset \mathbb{Z}[X]$ is *not* a principal ideal.
     - Suppose for the sake of contradiction that $(2, X) = (a(X))$ for some $a(X) \in \mathbb{Z}[X]$. Since $2 \in (a(X))$, there must be some $p(X) \in (a(X))$ such that $2 = p(X)a(X)$. Since $0 = \deg(pa) = \deg p + \deg a$, we have that $\deg p = \deg a = 0$. It follows that p, a are integers. In particular, since $p, z \in \mathbb{Z}$ and $pa = 2$, we must have $p, a \in \{\pm 1, \pm 2\}$. We now divide into two cases ($a = \pm 1$ and $a = \pm 2$). If $a = \pm 1$, then $(2, X) = (1) = \mathbb{Z}[X]$, i.e., $(2, X)$ is *not* a proper ideal. However,
     $$(2, X) = \{2p(X) + Xq(X) : p(X), q(X) \in \mathbb{Z}[X]\}$$
     This means that $(2, X)$ is the set of all polynomials with integer coefficients and even constant term (as discussed in Example 5, Section 7.3). But this clearly *is* a proper ideal (i.e., it excludes all polynomaials with integer coefficients and odd constant term), a contradiction. If $a = \pm 2$, then we may note that $X \in (a(X)) = (2) = (-2)$, i.e., $X = 2q(X)$ for some polynomial $q(X) \in \mathbb{Z}[X]$. But since q has integer coefficients, this is impossible (we would need $q(X) = \frac{1}{2}X \in \mathbb{Q}[X]$), a contradiction.
     - It follows from the above that $(2, X) \subset \mathbb{Q}[X]$ *is* a principal ideal. Thus, (A) is ambiguous if the ring is not specified.
     - More generally (see Chapter 9), all ideals of $F[X]$ are principal given that F is a field.
  4. $M = \{f : f(1/2) = 0\} = \ker(\mathrm{ev}_{1/2}) \subset \mathbb{R}^{[0,1]}$ is a principal ideal.
     - $M = (g)$, where $g : [0, 1] \to \mathbb{R}$ is any function that sends $1/2 \mapsto 0$.
     - If $R = C([0, 1], \mathbb{R})$, then M is not principal or even finitely generated (see the exercises).
  5. The augmentation ideal is generated by $\{g - 1 : g \in G\}$.

  - Follows from the definitions; coefficients sum to zero by the distributive law.
  - This need not be the minimal set of generators; for example, if $G = \langle \sigma \rangle$, then the augmentation ideal is $(\sigma - 1)$.

- The ideal structure of fields is trivial.

  Proposition 7.9. Let I be an ideal of R.

  1. $I = R$ iff I contains a unit.

     Proof. Given. □

  2. If R is commutative, then R is a field iff its only ideals are 0 and R.

     Proof. Given (see Lectures 2.2 and 2.3). □

  Corollary 7.10. If R is a field, then any nonzero ring homomorphism from R into another ring is an injection.

  Proof. Let S be a ring for which there exists a nonzero ring homomorphism $\varphi : R \to S$[2]. To prove that φ is an injection, it will suffice to show that $\ker \varphi = \{0\}$. Since φ is a ring homomorphism, $\ker \varphi$ is an ideal. Since φ is nonzero, $\ker \varphi \subsetneq R$. Thus, since the only ideals of R a field are $0, R$ by Proposition 7.9(2), $\ker \varphi = \{0\}$, as desired. □

- Noncommutative analog of Proposition 7.9(2).

  1. If D is a ring with identity $1 \neq 0$ in which the only left ideals and the only right ideals are $0, D$, then D is a division ring.
  2. Conversely, the only (left, right, or two-sided) ideals in a division ring D are $0, D$.

- Dummit and Foote (2004) gives a counterexample to Proposition 7.9(2) for noncommutative rings, using matrix rings.

- **Simple** (ring): A ring R the only two-sided ideals of which are $0, R$.

  - These are studied in Chapter 18.

- **Maximal** (ideal): An ideal $M \subsetneq S$ such that the only ideals containing M are M, S.

- Nonzero rings have maximal ideals in general (zero rings are the trivial exception).

  Proposition 7.11. In a ring with identity, every proper ideal is contained in a maximal ideal.

  Proof. Given. □

- Characterizing maximal ideals by the structure of their quotient rings.

  Proposition 7.12. Let R be commutative. Then the ideal M is a maximal ideal iff the quotient ring R/M is a field.

  Proof. Given (see Lecture 2.3). □

- Notes on Proposition 7.12.

  - Allows us to construct some fields, e.g., by taking the quotient of any commutative ring R with identity by a maximal ideal in R.

[2]Not any ring can be S; for instance, there exists no nonzero *ring homomorphism* $\varphi : \mathbb{R} \to \mathbb{Z}$. So don't worry; it's not like this corollary implies that there is an injection from $\mathbb{R}$ to $\mathbb{Z}$.

  - "We shall use this in Part IV to construct all finite fields by taking quotients of the ring $\mathbb{Z}[X]$ by maximal ideals" (Dummit & Foote, 2004, p. 254).

- Examples of maximal ideals.

  1. $n\mathbb{Z}$ is a maximal ideal if...
     - Proposition 7.12: $\mathbb{Z}/n\mathbb{Z}$ is a field.
     - Recall that $\mathbb{Z}/n\mathbb{Z}$ is a field iff n is prime.
     - This should also make intuitive sense: $n\mathbb{Z}$ contains all ideals $m\mathbb{Z}$ where m is a composite number containing n in its factorization, i.e., is a multiple of n.
  2. $(2, X) \subset \mathbb{Z}[X]$ is a maximal ideal.
     - Recall that $\mathbb{Z}[X]/(2, X) \cong \mathbb{Z}/2\mathbb{Z}$, where $\mathbb{Z}/2\mathbb{Z}$ is a field by the above.
  3. $(X) \subset \mathbb{Z}[X]$ is *not* a maximal ideal.
     - Counterexample: $(X) \subsetneq (2, X) \subsetneq \mathbb{Z}[X]$.
     - Alternate proof: Since $(X) = \ker(\mathrm{ev}_0 : \mathbb{Z}[X] \to \mathbb{Z})$, we know that $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$, which is not a field.
  4. $M_a = \ker(\mathrm{ev}_a : \mathbb{R}^{[0,1]} \to \mathbb{R}) \subset \mathbb{R}^{[0,1]}$ is a maximal ideal.
     - Since ev_a is surjective, $\mathbb{R}^{[0,1]}/M_a \cong \mathbb{R}$ a field.
     - Similarly, $\ker(\mathrm{ev}_a : C([0,1], R) \to \mathbb{R}) \subset C([0,1], R)$ is a maximal ideal.
  5. The augmentation ideal I is a maximal ideal of the group ring FG.
     - It's the kernel of the augmentation map, a surjective homomorphism onto F (i.e., $FG/I \cong F$ a field).
     - Proposition 7.12 does not directly apply, but "I is a maximal ideal if R/I is a field holds for arbitrary rings" (Dummit & Foote, 2004, p. 255).

- **Prime** (ideal): An ideal $P \subsetneq R$, where R is commutative, such that if $a, b \in R$ and $ab \in P$, then at least one of a, b is an element of P.
  - This definition may seem strange, but it is a natural generalization of the concept of prime numbers.
  - Indeed, we can show that "the prime ideals of $\mathbb{Z}$ are just the ideals $p\mathbb{Z}$ of $\mathbb{Z}$ generated by the prime numbers p together with the ideal 0" (Dummit & Foote, 2004, p. 255).

- The maximal ideals and the nonzero prime ideals of $\mathbb{Z}$ coincide.
  - This is not true for general commutative rings R.

- Every maximal ideal is a prime ideal.

- Characterizing prime ideals by the structure of their quotient rings.

  Proposition 7.13. Let R be commutative. Then the ideal P is a prime ideal in R iff the quotient ring R/P is an integral domain.

  Proof. Given. □

- Maximal and prime ideals.

  Corollary 7.14. Let R be commutative. Then every maximal ideal of R is a prime ideal.

  Proof. Let M be a maximal ideal of R. Then by Proposition 7.12, R/M is a field. Hence, R/M is an integral domain. Therefore, by Proposition 7.13, M is a prime ideal. □

- Examples.

  1. $p\mathbb{Z}$ for p prime is a prime and a maximal ideal.
     - The zero ideal in $\mathbb{Z}$ is prime but not maximal.
  2. $(X) \subset \mathbb{Z}[X]$ is a prime ideal but not a maximal ideal.

Week 3

Intro to Ring Types

3.1 Intro to Chapters 8-9

1/18:

- Moving onto Chapter 8 today.
- Friday: Rings of fractions (more than what's in the book; under lesser hypotheses).
  - Def get notes!
- The Chinese Remainder Theorem is at least partially in HW3.
- Today: A leisurely introduction to Chapter 8, as well as Spring Quarter content (which is the most interesting part of the Honors Algebra sequence).
- For the next three weeks or more, all rings will be assumed to be commutative.
  - Excepting matrix rings, which may still appear in exercises.
- At this point, we define $\deg(f) = -\infty$ where f is the zero polynomial.
  - We do this so that $\deg(fg) = \deg(f) + \deg(g)$ still holds.
- Euclidean algorithm for monic polynomials: Let $f \in R[X]$ be a monic polynomial of degree $d \geq 0$, and let $h \in R[X]$. Then there exists a unique pair $q, r \in R[X]$ such that...
  1. $h = qf + r$;
  2. $\deg(r) < \deg(f)$.

  Proof. We tackle uniqueness first, and then existence.

  Uniqueness: Suppose $h = q_1 f + r_1 = q_2 f + r_2$, where $\deg(r_i) < d$ $(i = 1, 2)$. We have that

  $$(q_1 - q_2)f = q_1 f - q_2 f = r_2 - r_1$$

  Now suppose for the sake of contradiction that $q_1 - q_2 \neq 0$. We know that

  $$\deg(r_2 - r_1) = \deg[(q_1 - q_2)f] = \deg(q_1 - q_2) + d \geq d$$

  But since $\deg(r_i) < d$ $(i = 1, 2)$, we have that $\deg(r_2 - r_1) < d$, a contradiction. Thus, $q_1 - q_2 = 0$. It follows easily that $0 = r_2 - r_1$. Therefore, $(q_1, r_1) = (q_2, r_2)$, as desired.

  Existence: If $\deg(h) < d$, then put $q = 0$ and $r = h$. We now induct on $\deg(h)$, starting from d. Our base case is already taken care of via the statement on $\deg(h) < d$. Now suppose using strong induction that we have proven the claim for all nonnegative integers $n < \deg(h)$. Let

  $$h(X) = a_0 + \cdots + a_e X^e$$

where $a_e \neq 0$ and $e \geq d$ by hypothesis. Let

$$f(X) = b_0 + \cdots + b_{d-1}X^{d-1} + X^d$$

Define $g(X)$ by

$$g = h - a_e X^{e-d} f$$

It follows that $\deg(g) < e$, so we may apply the induction hypothesis at this point. We learn from it that there exist q, r such that $g = qf + r$ with $\deg(r) < d$. Therefore, we can deduce that

$$h = (a_e X^{e-d} + q)f + r$$

as desired. □

- Notes on the Euclidean algorithm: Think long polynomial division from high school.
- Example.
  - Let $a \in R$ and $f = X - a$ be a monic polynomial. Let $h \in R[X]$ be arbitrary. Then applying the theorem,
  $$h(X) = q(X)(X - a) + r$$
  - $\deg(r) < 1 = \deg(f)$ implies that r is a constant, and hence $r \in R$.
  - Moreover,
  $$h(a) = q(a)(a - a) + r$$
  $$r = h(a)$$
  implying that
  $$h(X) - h(a) = q(X)(X - a)$$
  for arbitrary polynomials h.
- **Ideal generated by $b \in B$**. *Denoted by* $\boldsymbol{Bb}$, $\boldsymbol{(b)}$.
- **Principal ideal**: ...
- Corollary: Let $a \in R$. $\{h \in R[X] : h(a) = 0\}$ is the principal ideal generated by $X - a$.
- Corollary: Let $f \in R[X]$ be monic of degree d. Then
  $$\{g \in R[X] : \deg(g) < d\} \hookrightarrow R[X] \twoheadrightarrow R[X]/(f)$$
  and, in particular,
  $$\{g \in R[X] : \deg(g) < d\} \cong R[X]/(f)$$
  as groups (in particular, *not* as rings).

  Proof. The existence of the first two maps is obvious (they are just instances of the canonical injection and surjection, respectively).

  We now verify that the last two sets are in bijective correspondence. Define a map φ between them via the canonical surjection (note that since the domain of φ is not $R[X]$, we will still have to verify surjectivity here). As established previously, φ is well defined.

  To prove that φ is injective, it will suffice to show that $\ker \varphi = 0$. Let h be an arbitrary polynomial in $R[X]$ with $\deg(h) < d$. Suppose $\varphi(h) = \bar{0} = 0 + (f) = (f)$. Then $h \in (f)$. It follows that either $h = 0$ or $\deg(h) \geq \deg(f) = d$. But as an element of the domain $\deg(h) < d$ by hypothesis. Therefore, $h = 0$, as desired.

  To prove that φ is surjective, it will suffice to show that for every $h + (f) \in R[X]/(f)$, there exists $r \in R[X]$ with $\deg(r) < d$ such that $\varphi(r) = h + (f)$. Let $h + (f) \in R[X]/(f)$ be arbitrary. By the Euclidean algorithm, $h = qf + r$ for some $q, r \in R[X]$ where $\deg(r) < \deg(f) = d$. Moreover, since $r = h + (-q)f$, $r \in h + (f)$ and hence $h + (f) = r + (f)$. Therefore, since r is in the domain of φ (as it has degree less than d), $\varphi(r) = r + (f) = h + (f)$, as desired. □

- In many ways, this is an equivalent statement to the Euclidean algorithm.
  - Indeed, here, we are constructing an isomorphism of abelian groups $j : R^d \to R[X]/(f)$ given by
    $$j(a_0, a_1, a_2, \ldots, a_{d-1}) = \pi(a_0 + a_1X + a_xX^2 + \cdots + a_{d-1}X^{d-1})$$
    where π is the canonical surjection.
- $R[X]$ is also a vector space with $1, X, X^2, \ldots$ as the basis.
- We have that
  $$\{g \in R[X] : \deg(g) < d\} = \{a_0 + \cdots + a_{d-1}X^{d-1} : a_0, \ldots, a_{d-1} \in R\}$$
  - As an abelian group (ignoring multiplication), this set is group isomorphic to $(R^d, +)$.
- We now motivate a particular related construction.
- Revisiting the creation of $\mathbb{C}$ from $\mathbb{R}$.
  - We can use quotient rings to solve $X^2 + 1 = 0$.
  - In particular, the equation $X^2 + 1 = 0$ does not have a solution in $\mathbb{R}[X]$. However, it does have a solution in $\mathbb{R}[X]/(X^2 + 1)$, as we will see presently.
  - Consider the function described in the above corollary, sending $\mathbb{R} \hookrightarrow \mathbb{R}[X] \twoheadrightarrow \mathbb{R}[X]/(X^2+1)$. Let $\bar{X} := X + (X^2 + 1) \in \mathbb{R}[X]/(X^2 + 1)$ denote the image of X in $\mathbb{R}[X]/(X^2 + 1)$ under the second map. It follows that in this new ring,
    $$\begin{aligned}\bar{X}^2 + 1 &= [X + (X^2 + 1)] \cdot [X + (X^2 + 1)] + [1 + (X^2 + 1)] \\ &= [X^2 + 1] + (X^2 + 1) \\ &= 0 + (X^2 + 1) \\ &= 0\end{aligned}$$
    as desired.
  - Additionally, the elements of this ring are of the form $a_0 + a_1\bar{X}$ $(a_0, a_1 \in \mathbb{R})$ by the above corollary. As per the rules of addition and multiplication in quotient rings, our addition and multiplication in this ring are
    $$\begin{aligned}(a_0 + a_1\bar{X}) + (b_0 + b_1\bar{X}) &= (a_0 + b_0) + (a_1 + b_1)\bar{X} \\ (a_0 + a_1\bar{X}) \cdot (b_0 + b_1\bar{X}) &= (a_0b_0 - a_1b_1) + (a_0b_1 + a_1b_0)\bar{X}\end{aligned}$$
    - For addition, we expect componentwise.
    - For multiplication, we apply the distributive law, and then reduce our final element mod $X^2 + 1$ using the fact that $\bar{X}^2 = -1$ so $a_1b_1\bar{X}^2 = -a_1b_1$.
  - Thus, since they have isomorphic sets of elements and identical operations,
    $$\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$$
  - Note that $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{R}[i]$, where $i = \sqrt{-1}$. In other words, we can look at the elements of $\mathbb{R}[X]/(X^2 + 1)$ as complex numbers, or as polynomials in i. The two concepts are equivalent since any polynomial in i reduces to a complex number via the i-cycle as follows.
    $$\begin{aligned}\sum_{j=0}^{\infty} a_j i^j &= a_0 + a_1 i + a_2 i^2 + a_3 i^3 + a_4 i^4 + a_5 i^5 + \cdots \\ &= a_0 + a_1 i - a_2 - a_3 i + a_4 + a_5 i - \cdots \\ &= (a_0 - a_2 + a_4 - \cdots) + (a_1 - a_3 + a_5 - \cdots)i \\ &= \left(\sum_{j=0}^{\infty} a_{2j}\right) + \left(\sum_{j=0}^{\infty} a_{2j+1}\right) i\end{aligned}$$

- However, this construction renders $\mathbb{C}$ as just one particular special case of interest in a far more general construction.
  - Specifically, $\mathbb{C}$ is the special case that takes $f = X^2 + 1$ as the divisor.
- Indeed, we may create a ring in which the root of any polynomial $f \in R[X]$ exists.
  - For the sake of simplicity, let f be monic of degree d. Let $A = R[X]/(f)$. Then as per the corollary, $R \hookrightarrow R[X] \twoheadrightarrow A$.
  - Once again, we let $\bar{X}$ be the image of X under the second map. $f(X) \mapsto f(\bar{X}) = 0$, as desired.
  - In analogy to the last line above,
    $$R[X]/(f) \cong R[\bar{X}]$$
    for any $\bar{X}$ satisfying $f(\bar{X}) = 0$.
  - All of this can be tied together in the following convenient corollary.
- Corollary: Given $f \in R[X]$ monic of degree $d > 0$, then there exists a ring A such that R is a subring of A and there exists $\theta \in A$ such that $\mathrm{ev}_\theta(f) = f(\theta) = 0$.

  Proof. Take $A = R[X]/(f(X))$ and put $\theta = \pi(X)$. □
- Notes on the above construction.
  - It is more standard to denote the quantity θ by $\bar{X}$; we simply did not do this in the beginning so that our notation would not "imply" the desired result.
  - The construction is valid for arbitrary (e.g., not monic) $f \in R[X]$ except that $R \to R[X]/(f)$ may not be one-to-one as R is not a subring of $R[X]/(f)$ in such generality.
- Additional examples.
  1. Take $R = \mathbb{Z}$, $f(X) = 2$. Then $\mathbb{Z} \hookrightarrow \mathbb{Z}[X] \twoheadrightarrow \mathbb{Z}[X]/(2)$.
     - (2) is the set of all polynomials with even integer coefficients. Thus, any polynomial with even integer coefficients in $\mathbb{Z}[X]$ will be projected down to zero, and any polynomial containing any odd coefficients will correspond to a coset in which all polynomials with odd terms in the same places are lumped together.
     - Essentially, reducing occurs termwise and is modulo 2 based on the coefficients. For example,
       $$5 + 2X + 4X^2 + 7X^4 + (2) = 1 + 1X^4 + (2)$$
       since $4 + 2X + 4X^2 + 6X^4 \in (2)$ and
       $$5 + 2X + 4X^2 + 7X^4 = 1 + 1X^4 + 4 + 2X + 4X^2 + 6X^4$$
     - Thus, $\mathbb{Z}[X]/(2) \cong \mathbb{Z}/2\mathbb{Z}[X]$. See also Proposition 9.2.
     - What is $\bar{X}$ in this set?? It must be some integer? Or is it just X?
  2. Take $R = \mathbb{Z}$ and $f(X) = 2X + 3$. Then we have $\mathbb{Z}[X]/(2X + 3)$.
     - $X \mapsto \bar{X}$ and $2\bar{X} + 3 = 0$, so $\bar{X} = -3/2$.
     - Just like $i \notin \mathbb{R}$, $-3/2 \notin \mathbb{Z}$.
     - We still have $\mathbb{Z}[X]/(2X + 3) \cong \mathbb{Z}[-3/2]$.
       - In other words, $\mathbb{Z}[X]/(2X + 3)$ is the set of all "polynomials" in $-3/2$ with integer coefficients, which is just equal to
         $$\{a/2^n : a \in 3\mathbb{Z}\}$$
         which is the dyadic rationals with numerator equal to a multiple of 3.

    - Ideals of this form will be considered in HW4 Q4.4.
  - This construction will be integral to Spring Quarter.
- Question/exercise: Let $\alpha \in R$. Then $R[X]/R[X]\alpha \cong (R/R\alpha)[X]$. See Proposition 9.2.
- Question: Take $R = \mathbb{Z}$. Is the ring $A = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a \equiv b \pmod{N}\}$ a special case of this construction?
- Is it that dividing by a polynomial of degree 0 puts a constraint on the coefficients whereas dividing by a polynomial of degree greater than zero puts a constraint on the variable??
- **Principal ideal domain**: A commutative ring R that is an integral domain and for which every ideal is principal. *Also known as* **PID**.
- There is a useful explanation of something on Chapter 8, page 2 of Dummit and Foote (2004).
- Theorem: Let F be a field. Then $F[X]$ is a PID.

  Proof. We have proven previously that F an integral domain implies $F[X]$ is an integral domain.

  Let $I \subset F[X]$ be a nonzero ideal. Let

  $$d = \min\{\deg(g) : g \in I,\ g \neq 0\}$$

  Pick $g \in I$ such that $\deg(g) = d$. We have that $g = a_0 + \cdots + a_d X^d$, $a_d \neq 0$, $a_d^{-1} \in F$. Let $f = a_d^{-1} g \in I$ (as guaranteed by the presence of $g \in I$). Let $h \in I$. Then the EA produces q, r such that $h = qf + r$ with $\deg(r) < d$. We know that $h, f \in I$. Thus, $h - qf = I$. It follows by the definition of d that $r = 0$. Therefore, $h \in (f)$. □
- Callum will lecture on Friday.
- Feedback on the HW.
  - Most people seem to think that the HW is at a reasonable level of difficulty.
  - The third one should be more challenging.

3.2 Rings of Fractions

1/20:
- This lecture will cover material from Sections 7.5 and 15.4 of Dummit and Foote (2004).
- Defining $\mathbb{Q}$.
  - Rigorously, we define $\mathbb{Q}$ as a subset of $(\mathbb{Z} \times \mathbb{Z}) - \{(a, 0) : a \in \mathbb{Z}\}$. In particular, we let $\mathbb{Q}$ be the set of equivalence classes in $\mathbb{Z} \times \mathbb{Z}$ under the equivalence relation

    $$\frac{a}{b} = \frac{c}{d} \quad \iff \quad ad - bc = 0$$

    where a/b denotes $(a, b) \in \mathbb{Z} \times \mathbb{Z}$.
  - Addition on $\mathbb{Q}$:

    $$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}$$

    - This makes $(\mathbb{Q}, +)$ an abelian group with identity $0 = 0/c$ for any $c \neq 0$.
  - Multiplication on $\mathbb{Q}$:

    $$\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}$$

    - This makes $(\mathbb{Q}, +, \cdot)$ a ring with identity $1 = 1/1 = d/d$ for any $d \neq 0$.

- Notice the similarities between the above approach and the definition of $\mathbb{C}$ from $\mathbb{R}$ in Lecture 2.1.
- It follows from the definition that $\mathbb{Q}$ is also a field: For any $a/b \in \mathbb{Q}$, $a/b \cdot b/a = 1$.
- We can generalize this construction to any commutative ring R.
  - As in $\mathbb{Q}$, we may only be able to take the "quotient" of certain elements of R by certain other elements of R. For example, $a/0$ does not make sense in $\mathbb{Q}$. Thus, we first define a subset of R called D: D contains elements which can act as denominators. The properties of D are motivated by the properties of denominators in $\mathbb{Q}$. In particular...
  - Let $D \subset R$ be such that $1_R \in D$, $0_R \notin D$, D has no zero divisors, and D is a **multiplicative subset**.
    - We need $1_R \in D$ so that all of the elements $a \in R$ appear in the related ring of fractions as $a/1_R$.
    - We can't have $0_R \in D$ because you cannot divide by zero.
    - We can't have any zero divisors in D because then during addition or multiplication, as defined above, the sum or product could have zero in the denominator.
    - We need closure under multiplication so that the sums and products defined above are well-defined.
  - With these constraints on D, we can define the **ring of fractions**.
- **Multiplicative subset**: A subset D of a ring R that is closed under multiplication, that is, $b, d \in D$ implies $bd \in D$.
  - This is distinct from a subring because we do not require $1 \in D$, and we do not require that D is a group under addition.
  - It is also distinct from the subgroup $(D, \times) \leq (R, \times)$ since it doesn't necessarily contain 1_R or inverses.
- $\sim$: The equivalence relation on a product ring $(A \times B, +, \cdot)$ defined as follows. *Given by*

$$(a_1, b_1) \sim (a_2, b_2) \iff a_1 \cdot b_2 - a_2 \cdot b_1 = 0$$

- Exercise: Confirm that $\sim$ is an equivalence relation.
- Just as taking the quotient of a group by a normal subgroup or a ring by an ideal yields a partition of the original object where all elements in any set in the partition are related by the substructure, taking the quotient of a set by an equivalence relation yields a partition of that set into classes called *equivalence* classes.
  - Thus, when we write $(A \times B)/\sim$, we refer to the set of equivalence classes of $A \times B$ under $\sim$.
- **Ring of fractions** (of D with respect to R): The set defined as follows under the operations defined as follows, where R is a commutative ring. *Denoted by* $\boldsymbol{D^{-1}R}$. *Given by*

$$D^{-1}R = \{(x, t) : x \in R,\ t \in D\}/\sim$$

1. Addition:

$$\frac{x_1}{t_1} + \frac{x_2}{t_2} = \frac{x_1 t_2 + x_2 t_1}{t_1 t_2}$$

   - Let $0_{D^{-1}R} = 0/1$.
     - Note that because of the way $0/1$ is defined (i.e., as an equivalence class), we no longer need to say $0/1 = 0/d$ for all $d \in D$ since all $0/d$ are included in $0/1$. In fact, at this point, $0/d$ is just an alternate name for the set $0/1$.
   - It follows from the above definition that $-(x/t) = -x/t$.

2. Multiplication:
$$\frac{x_1}{t_1} \cdot \frac{x_2}{t_2} = \frac{x_1 x_2}{t_1 t_2}$$
   - Let $1_{D^{-1}R} = 1/1$.

- Notes on the ring of fractions.
  - Notice how the notation is a nice alternative to the (already taken) R/D.
  - Notation: Write x/t for the equivalence class $[(x,t)]$.
- Proposition: $D^{-1}R$ is a ring as defined above.

  Proof. There are three steps needed: (1) check that $+, \times$ are well defined; (2) check that $(D^{-1}R, +)$ is an abelian group; and (3) check that $\times$ is an associative, commutative, and distributive operation with an identity. □

- **Field of fractions** (of R): The set $D^{-1}R$ where R is an integral domain and $D = R - \{0\}$. *Also known as* **quotient field**. *Denoted by* $\mathbf{Frac}\, \boldsymbol{R}$.
  - Inverses are given by
$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$$
    for all nonzero elements $a/b \in \operatorname{Frac} R$ (i.e., all elements for which $a, b \neq 0$).
- Example: Let R be an integral domain, and let $f \in R$ not be nilpotent. Take $D = \{1, f, f^2, \dots\}$. Then $R_f = D^{-1}R$.
  - Example: If $R = \mathbb{Z}$ and $f = 2$, then $R_2 = \{a/b \in \mathbb{Q} : b = 2^n\}$. Recall that these are the dyadic rationals.
- Example: Let $R = \mathbb{Z}$ and $D = \{a \in \mathbb{Z} : 2 \nmid a\}$. Then $D^{-1}R = \{a/b \in \mathbb{Q} : 2 \nmid b\}$.
- Besides the last two examples, the only nontrivial ideal of $\mathbb{Q}$ left is (2^n).
  - Do I have this statement right??
- If R is an integral domain, then $\operatorname{Frac}(R[X])$ is the set of all rational functions with coefficients in R.
- Theorem: There is a ring $D^{-1}R$ and a ring homomorphism $\iota : R \to D^{-1}R$ such that for all $x \in D$, $\iota(x)$ is a unit of $D^{-1}R$.

  Proof. Consider the canonical injection $\iota : R \to D^{-1}R$ defined by $x \mapsto x/1$. □

- Theorem (universal property of the ring of fractions):

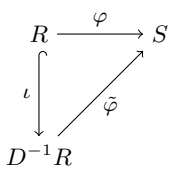

Figure 3.1: Decomposition of a ring homomorphism using $D^{-1}R$.

(1) $\iota : R \to D^{-1}R$ is an injective ring homomorphism.

(2) If $\varphi : R \to S$ is a ring homomorphism such that $\varphi(r)$ is a unit in S for all $r \in D$, then there exists a unique ring homomorphism $\tilde{\varphi} : D^{-1}R \to S$ such that $\tilde{\varphi} \circ \iota = \varphi$ (see Figure 3.1).

(3) If φ is injective, then so is $\tilde{\varphi}$.

Proof. (1) is easy.

We address (2) in two parts.

Existence: Define $\tilde{\varphi}(x/t) = \varphi(x)\varphi(t)^{-1}$.

Uniqueness: Suppose that there exists $\rho : D^{-1}R \to S$ such that $\rho \circ \iota = \varphi$. Then $\varphi(x) = (\rho \circ \iota)(x) = \rho(x/1)$. This result combined with the fact that ρ is a ring homomorphism implies that

$$1 = \rho(\tfrac{1}{1}) = \rho(\tfrac{t}{1})\rho(\tfrac{1}{t}) = \varphi(t)\rho(\tfrac{1}{t})$$

It follows since $\varphi(D) \subset S^\times$ by hypothesis that if $t \in D$, then $\rho(1/t) = \varphi(t)^{-1}$. Therefore,

$$\rho(\tfrac{x}{t}) = \rho(\tfrac{x}{1})\rho(\tfrac{1}{t}) = \varphi(x)\varphi(t)^{-1} = \tilde{\varphi}(\tfrac{x}{t})$$

We now address (3).

Suppose that φ is injective. To prove that $\tilde{\varphi}$ is injective, it will suffice to show that $\ker\tilde{\varphi} = 0$. Let $x/t \in \ker\tilde{\varphi}$ be arbitrary. Then $\tilde{\varphi}(\frac{x}{t}) = 0$. It follows by the definition of $\tilde{\varphi}$ that $\varphi(x)\varphi(t)^{-1} = 0$. Since $\varphi(t)$ is a unit by hypothesis and hence nonzero, it must be that $\varphi(x) = 0$. Additionally, as a ring homomorphism, $\varphi(0) = 0$. Combining the last two results, we have by transitivity that $\varphi(x) = \varphi(0)$. Thus, since φ is injective, $x = 0$. It follows that $x/t = 0/t$, so $\ker\tilde{\varphi} = 0$, as desired. □

3.3 Chapter 7: Introduction to Rings

From Dummit and Foote (2004).

Section 7.5: Rings of Fractions

1/30:

- Let R be a *commutative* ring throughout this section.
- Review of how zero divisors are similar to units in some ways and dissimilar in other ways.
- "The aim of this section is to prove that a commutative ring R is always a subring of a larger ring Q in which every nonzero element of R that is not a zero divisor is a unit in Q" (Dummit & Foote, 2004, p. 260).
  - If R is an integral domain, Q will be its **field of fractions** or **quotient field**.
- Review of the construction and properties of $\mathbb{Q}$.
- Why we can't include zeroes or zero divisors in the denominators.
  - Suppose b is a zero or zero divisor such that $bd = 0$.
  - If we allow b as a denominator, then
  $$d = \frac{d}{1} = \frac{bd}{d} = \frac{0}{b} = 0$$
  - Thus, there is a certain "collapsing," and we cannot expect that R appears as a natural subring of this "ring of fractions."
- Why we must have closure under multiplication for the denominators.
  - Review from class.
- "The main result of this section shows that these two restrictions are sufficient to construct a ring of fractions for R. Note that this theorem includes the construction of $\mathbb{Q}$ from $\mathbb{Z}$ as a special case" (Dummit & Foote, 2004, p. 261).

Theorem 7.15. Let R be a commutative ring. Let D be any nonempty subset of R that does not contain 0, does not contain any zero divisors, and is closed under multiplication (i.e., $ab \in D$ for all $a, b \in D$). Then there is a commutative ring Q with 1 such that Q contains R as a subring and every element of D is a unit in Q. The ring Q has the following additional properties.

1. Every element of $\mathbb{Q}$ is of the form rd^{-1} for some $r \in R$ and $d \in D$. In particular, if $D = R - \{0\}$, then Q is a field.
2. (Uniqueness of Q) The ring Q is the "smallest" ring containing R in which all elements of D become units in the following sense. Let S be any commutative ring with identity and let $\varphi : R \to S$ be any injective ring homomorphism such that $\varphi(d)$ is a unit in S for every $d \in D$. Then there is an injective homomorphism $\Phi : Q \to S$ such that $\Phi|_R = \varphi$. In other words, any ring containing an isomorphic copy of R in which all the elements of D become units must also contain an isomorphic copy of Q.

Proof. Given.

Same as in class: A general construction of Q, confirmation of its properties, and then the steps of the analogous theorem. Very well written, though, should I need additional insight in the future! □

- Theorem 15.36 generalizes Theorem 7.15 by allowing D to contain zero and/or zero divisors.
- Definition of the **ring of fractions** and **field of fractions**.
- **Subfield generated by A**: The subfield of F equal to the intersection of all subfields of F containing A, where A is some subset of a field F.
- The subfield generated by A is the smallest subfield of F containing A.
- The smallest field containing an integral domain R is its field of fractions.

  Corollary 7.16. Let R be an integral domain and let Q be the field of fractions of R. If a field F contains a subring R' isomorphic to R, then the subfield of F generated by R' is isomorphic to Q.

  Proof. Given (see Lecture 4.1). □

- Examples.
  1. $\operatorname{Frac} F \cong F$ for any field F.
  2. $\operatorname{Frac} \mathbb{Z} = \mathbb{Q}$.
     - Quadratic integer rings from Section 7.1 are brought up again.
  3. $\operatorname{Frac}(2\mathbb{Z}) = \mathbb{Q}$.
     - Notice how an identity "appears" in the field of fractions.
  4. The **rational functions**.
     - $\operatorname{Frac}(R[X])$ contains $\operatorname{Frac}(R)$.
     - $\operatorname{Frac}(R[X]) = \operatorname{Frac}(R)(X)$.
       - Example: We have that
         $$\operatorname{Frac}(\mathbb{Z}[X]) = \operatorname{Frac}(\mathbb{Q}[X]) = \mathbb{Q}(X) = \operatorname{Frac}(\mathbb{Z})(X)$$
       - We can easily see this since if $p(X)/q(X) \in \operatorname{Frac}(\mathbb{Q}[X])$, then there exists $N \in \mathbb{Z}$ such that $Np(X), Nq(X)$ both have integer coefficients (pick, for example, N to be the common denominator of all the coefficients in $p(X), q(X)$). Then $p(X)/q(X) = Np(X)/Nq(X) \in \operatorname{Frac}(\mathbb{Z}[X])$, as desired.
  5. $R_d = R[1/d] = D^{-1}R$, where $D = \{1, d, d^2, d^3, \dots\}$.
- **Rational functions** (in X over R): The field of fractions of the polynomial ring $R[X]$, where R is an integral domain and hence $R[X]$ is an integral domain. *Denoted by* $\mathbf{Frac}(\boldsymbol{R}[\boldsymbol{X}])$.
- **Field of rational functions**: The rational functions in X over a field F. *Denoted by* $\boldsymbol{F}(\boldsymbol{x})$.

Week 4

Classes of Rings

4.1 Euclidean Domains and Reducibility

1/23:

- Notes to wrap up last time to start.
- Recall the theorem from last time: There is an injective ring homomorphism $\iota : R \to D^{-1}R$ such that for any $\varphi : R \to S$ such that $\varphi(D) \subset S^\times$, there exists a unique $\tilde{\varphi} : D^{-1}R \to S$ such that $\tilde{\varphi} \circ \iota = \varphi$.
  - Callum redraws Figure 3.1.
- Something Callum misstated last time: Dyadic refers to 2-adic, not p-adic.
- Corollary: If $f \in R$ is not a zero divisor, then $R_f \cong R[X]/(fX - 1)$.
  - We can prove this using the universal property; it's on the HW.
- **Subfield of F generated by R**: The field defined as follows, where F is a field and $R \subset F$ is an integral domain. *Denoted by* $\boldsymbol{K}$. *Given by*

$$K = \bigcap_{\substack{R \subset F' \subset F \\ F' \text{ a field}}} F'$$

  - Alternative definition: The smallest field inside F that contains R.
- Proposition: Let $R \subset F$ be an integral domain, where F is a field. Then

$$K \cong \operatorname{Frac} R$$

  Proof. Background: Consider the injection $R \to F$. It sends every element of $D = R - \{0\}$ to a unit in F. Moreover, this function "factors through the fraction field" via Figure 3.1 as per the theorem. We now begin the argument in earnest.

  To prove that $K \cong \operatorname{Frac} R$, we will use a bidirectional inclusion proof. For the forward direction, observe that $R \subset \operatorname{Frac} R \subset F$. Therefore, by the definition of K, $K \subset \operatorname{Frac} R$, as desired. For the backward direction, let $x/y \in \operatorname{Frac} R$ be arbitrary. To confirm that $x/y \in K$, it will suffice to verify that $x/y \in F'$ for all $R \subset F' \subset F$. Let F' subject to said constraint be arbitrary. Since $x/y \in \operatorname{Frac} R$, $x, y \in R$. It follows since $R \subset F'$ that $x, y \in F'$. Thus, since F' is a field and hence closed under multiplicative inverses, $1/y \in F'$. Finally, since F' is closed under multiplication and $x, 1/y \in F'$, we have that $x/y \in F'$, as desired. □
- Example: Let $R = \mathbb{Z}[\sqrt{2}] = \mathbb{Z}[X]/(X^2 - 2)$. Then

$$\operatorname{Frac} R = \mathbb{Q}[\sqrt{2}] = \frac{\mathbb{Q}[X]}{(X^2 - 2)}$$

- That's it for rings of fractions. We now move onto Euclidean Domains (EDs), Principal Ideal Domains (PIDs), and Unique Factorization Domains (UFDs).
- An ED is a PID, and a PID is a UFD (hence, for example, an ED is both a PID and a UFD).
- **Norm**: A function from an integral domain R to $\mathbb{Z}_{\geq 0}$ that satisfies the following. *Denoted by* $\boldsymbol{N}$. *Constraints*

  (i) Let $a \in R$. Then $N(a) = 0$ iff $a = 0$.

  (ii) $h, f \in R$ and $f \neq 0$ implies that there exists $q, r \in R$ such that $h = qf + r$ and $N(r) < N(f)$.
- **Euclidean domain**: An integral domain on which there exists a norm. *Also known as* **ED**.
- **Strongly Euclidean domain**: An ED for which the norm N satisfies the additional constraint (iii) below. *Also known as* **SED**. *Constraint*

  (iii) $N(ab) = N(a)N(b)$ for all $a, b \in R$.
- Theorem: If R is an ED, then R is a PID.

  Proof. This proof will use an analogous argument to that used in the proof that $F[X]$ is a PID from the end Lecture 3.1. Let's begin.

  To prove that R is a PID, it will suffice show that for every ideal $I \subset R$, $I = (f)$ for some $f \in I$. Let $I \subset R$ be arbitrary. Let
  $$d = \min\{N(a) : a \in I - \{0\}\}$$
  Pick $f \in I - \{0\}$ such that $N(f) = d$. We will now argue that $I = (f)$ via a bidirectional inclusion proof. In one direction, since I is an ideal, $(f) = Rf \subset I$. In the other direction, let $h \in I$ be arbitrary. Then since $f \neq 0$ by assumption, the hypothesis that R is an ED implies that there exist $q, r \in R$ such that $h = qf + r$ and $N(r) < N(f)$. It follows since $h, qf \in I$ that $r = h - qf \in I$. But since $N(r) < N(f) = d$, $r \in I$ implies by the definition of d that necessarily $N(r) = 0$ and hence $r = 0$. Therefore, $h = qf$, as desired. □
- Note that showing that $r \in I$ this way would not be acceptable in the HW??
- Examples of EDs:
  1. $\mathbb{Z}$, $N(m) = |m|$.
     - The norm is non-unique.
  2. $F[X]$[1], $N(f) = 2^{\deg(f)}$.
     - We define the norm in this way because then the degree of the zero polynomial being $-\infty$ makes $N(0) = 2^{-\infty} = 0$.
     - Note that since $\deg(fg) = \deg(f) + \deg(g)$, $N(fg) = N(f)N(g)$ here.
  3. $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$ (d is a **square-free integer**), $N(a + b\sqrt{d}) = |(a + b\sqrt{d})(a - b\sqrt{d})| = |a^2 - b^2 d|$ for $a, b \in \mathbb{Q}$.
     - Observations (in the context of $\mathbb{Q}[\sqrt{d}]$, not $\mathbb{Z}[\sqrt{d}]$):
       - $N(a + b\sqrt{d}) = 0$ iff $(a, b) = (0, 0)$.
       - $\mathbb{Q}[\sqrt{d}]$ is SE (strongly Euclidean) since $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Q}[\sqrt{d}]$.
       - $N(\alpha) \in \mathbb{Z}$ for all $\alpha \in \mathbb{Z}[\sqrt{d}]$. This is why only $\mathbb{Z}[\sqrt{d}]$ is an ED.
     - Most famous example: $\mathbb{Z}[\sqrt{-1}]$, which are the **Gaussian integers**.
     - Also interesting are $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt{2}]$, and $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}] \cong \mathbb{Z}[X]/(X^2 + X + 1)$.
       - In the last example, the complex number in brackets is a cube root of unity equal to $\cos(120) + i\sin(120)$.

[1] Henceforth, "F" is assumed to denote a field.

  - The reason why we define the norm on $\{a+b\sqrt{d}\}$ for $a,b\in\mathbb{Q}$ instead of $a,b\in\mathbb{Z}$.
    - The number θ in $\mathbb{Z}[\theta]$ may not always be a radical or imaginary; it can be complex, too, as in the case of $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$.
    - Let $\theta=\frac{-1+\sqrt{-3}}{2}$. In this case, we have

$$\left\{\alpha+\beta\frac{-1+\sqrt{-3}}{2}\middle|\alpha,\beta\in\mathbb{Z}\right\}\cong\left\{a+b\sqrt{-3}\middle|a,b\in\mathbb{Q},\ a=\alpha-\frac{1}{2}\beta,\ b=\frac{1}{2}\beta,\ \alpha,\beta\in\mathbb{Z}\right\}$$

- **Square-free integer**: An integer that is not divisible by the square of any integer.
- **Gaussian integers**: The Euclidean domain $\mathbb{Z}[\sqrt{-1}]$.
- Exercise: Prove that $\mathbb{Z}[\sqrt{d}]$ is SE (i.e., is an SED) for $d=-1,-2,2,3$.
  - Hint: Given $h,f\in\mathbb{Z}[\sqrt{d}]$, we have $h/f\in\mathbb{Q}[\sqrt{d}]$. Choose $q\in\mathbb{Z}[\sqrt{d}]$ as close as possible to h/f. For a given d, you will find $N(q-h/f)<1$.
  - The same procedure will show that $\mathbb{Z}[(-1+\sqrt{d})/2]$ is SE for $d=-3,5$.
- **Unit**: An element $u\in R$ for which there exists $v\in R$ such that $uv=vu=1$.
- $\boldsymbol{R^\times}$: The set of all units of R.
  - $(R^\times,\times)$ is a group.
- Examples:
  1. $F^\times=F-\{0\}$.
  2. $F[X]^\times=F^\times$, i.e., is the nonzero constant polynomials.
     - This is because any higher degree polynomial cannot be taken back down in degree — multiplying polynomials adds degrees.
  3. $\mathbb{Z}^\times=\{\pm1\}$.
  4. $\mathbb{Z}[\sqrt{-1}]^\times=\{\pm1,\pm i\}$.
  5. $R[X]^\times=R^\times$ (R an integral domain).
  6. Suppose R is not an integral domain. Then we get things like $a\neq0\in R$ and $a^2=0$ (i.e., a is a zero divisor) implies that $(1-aX)(1+aX)=1-a^2X^2=1$.
     - We forbid this! It's nasty. Thus, we assume that rings of polynomials are taken over integral domains.
- **Reducible** (element): A nonzero element $a\in R$ such that $a=bc$ and $b,c\notin R^\times$, where R is an integral domain.
  - Alternative definition: An element that is the product of two things, neither of which is a unit.
- $R-\{0\}$ is a disjoint union of...
  (i) Units;
  (ii) Reducible elements;
  (iii) And irreducible elements.

Proof. Suppose for the sake of contradiction that $a\in R-\{0\}$ is both reducible and a unit. Since a is reducible, $a=bc$ where $b,c\notin R^\times$. Since a is a unit, we may define $d=a^{-1}$. Then

$$1=ad=bcd=b(cd)$$

so $b\in R^\times$, a contradiction. □

- Corollary: If $a_1 \cdots a_r \in R^\times$, then $a_i \in R^\times$ $(i = 1, \ldots, r)$.

  Proof. Same strategy as above, i.e., definition of a unit followed by associativity. □

- Reducibility/irreducibility changes based on context.
- Example:
  - Consider $F[[X]]$, where X is taken to be irreducible.
    - Here, all elements are of the form uX^n for some $u \in F$ and $n \in \mathbb{Z}_{\geq 0}$.
  - However, if we define $X = (X^{1/2})^2$, then $F[[X]] \subset F[[X^{1/2}]]$. In this larger context, X is now reducible.
  - We can continue the chain via
$$\bigcup_{n=1}^{\infty} F[[X^{\frac{1}{2^n}}]]$$
- **Factorization** (of $a \in R$): A product of certain elements of R that is equal to a, where R is a ring; in particular, the product must consist of one unit u and r irreducible elements $\pi_1, \ldots, \pi_r \in R$. *Given by*
$$a = u\pi_1\pi_2 \cdots \pi_r$$
- **Unique factorization domain**: An integral domain R such that for every nonzero element $a \in R$ which is not a unit, any two factorizations
$$a = u\pi_1\pi_2 \cdots \pi_r \qquad\qquad a = u'\pi_1'\pi_2' \cdots \pi_s'$$
of a satisfy the following conditions.
  (i) *Same length*: $r = s$.
  (ii) *Uniqueness up to* ***associates***: There exists $\sigma \in S_r$ such that $\pi_i' = \pi_{\sigma(i)}u_i$ for all $1 \leq i \leq r$, u_i being a unit.

  Also known as **UFD**.
- Wednesday: Show that a PID is a UFD.

4.2 Unique Factorization Domains

1/25:
- Goal: UFDs.
- We review some definitions from last time to start.
- **Prime** (ideal): An ideal P in a commutative ring R for which R/P is an integral domain.
  - Equivalently, $1 \notin P$ and $a, b \notin P$ imply $ab \notin P$, i.e., $R - P$ is a multiplicative set.
  - Equivalently (contrapositive): $ab \in P$ implies $a \in P$ or $b \in P$.
- Observation: Maximal ideals are prime ideals.
- From now on, R denotes an integral domain.
- **Factorization** (of a nonzero element): A product $a = u\pi_1\pi_2 \cdots \pi_r$, where $u \in R^\times$, each π_i is irreducible, and $r = 0$ is allowed.
- **Irreducible** (element): A nonzero element that is neither a unit nor reducible.
  - Think of them a bit like primes, though this is very dangerous. See Dummit and Foote (2004).

- **Equivalent** (factorizations): Two factorizations $a = u\pi_1\pi_2\cdots\pi_r$ and $a = u'\pi_1'\pi_2'\cdots\pi_s'$ for which $r = s$ and there exists $\sigma \in S_r$ and $u_1, \ldots, u_r \in R^\times$ such that $\pi_i' = u_i\pi_{\sigma(i)}$ $(i = 1, \ldots, r)$ where $u\pi_1$ is also irreducible.
- **Unique factorization domain**: An integral domain R for which every nonzero a has a factorization and any factorizations of a are equivalent to each other.
- **Prime** (element): A nonzero $\pi \in R$ for which (π) is a prime ideal.
- Exercise: Prove that if π is prime, then π is irreducible.
  - Note that π irreducible does *not* imply that π is prime in general.
- Lemma*: If every irreducible element of R is prime, then any two factorizations of any nonzero $a \in R$ are equivalent.

  Proof. We induct on the length $r \geq 0$ of factorizations.

  For the base case $r = 0$, let $a \in R$ be arbitrary. Factor it into

  $$a = u\prod_{i=1}^{r}\pi_i = u\prod_{i=1}^{0}\pi_i = u$$

  It follows that a is a unit. Therefore, there exists $b \in R$ such that $ab = 1$. Now suppose for the sake of contradiction that we also have

  $$a = u'\pi_1'\cdots\pi_s'$$

  It follows that

  $$1 = (u'\pi_1'\cdots\pi_s')b = \pi_1'(u'\pi_2'\cdots\pi_s'b)$$

  Thus, π_1' is a unit, contradicting the hypothesis that π_1' is irreducible. Therefore, $s = 0$ and $u' = u$, as desired.

  Now suppose inductively that we have proven the claim for $r - 1$; we now wish to prove it for r. Let

  $$a = u\pi_1\cdots\pi_r \qquad\qquad a = u'\pi_1'\cdots\pi_s'$$

  be two factorizations of an arbitrary $a \in R$. By the definition of a factorization, π_1 is irreducible. Thus, by hypothesis, π_1 is prime and hence (π_1) is a prime ideal. Additionally, we have that

  $$a = u\pi_1\cdots\pi_r = (u\pi_2\cdots\pi_r)\pi_1 \in R\pi_1 = (\pi_1)$$

  Thus, we must have $u'\pi_1'\cdots\pi_s' \in (\pi_1)$ as well. It follows that one of the elements in the product $u'\pi_1'\cdots\pi_s'$ is equal to $\pi_1 b$ for some $b \in R$. Suppose for the sake of contradiction that this element is u'. Then $u' = \pi_1 b$. But since u' is a unit, there exists $c \in R$ such that $1 = u'c$. It follows via substitution that

  $$1 = u'c = \pi_1 bc = \pi_1(bc)$$

  i.e., that π_1 is a unit, contradicting the hypothesis that it's irreducible. Therefore, $u' \notin (\pi_1)$. It follows that one of the $\pi_i' \in (\pi_1)$. WLOG, let $\pi_1' \in (\pi_1)$. Then $\pi_1' = u_1\pi_1$ for some $u_1 \in R$. In particular, since π_1' is irreducible, then either $u_1 \in R^\times$ or $\pi_1 \in R^\times$. But we can't have the second case since π_1 is irreducible (and hence not a unit) by assumption. Thus $u_1 \in R^\times$. It follows that

  $$\begin{aligned} a &= a \\ u\pi_1\cdots\pi_r &= u'\pi_1'\cdots\pi_s' \\ u\pi_1\cdots\pi_r &= u'u_1\pi_1\pi_2'\cdots\pi_s' \\ u\pi_2\cdots\pi_r &= u'u_1\pi_2'\cdots\pi_s' \end{aligned}$$

  where we apply the cancellation lemma in the last step, as permitted by the facts that R is an integral domain and π_1 is irreducible (hence nonzero). Thus, by the induction hypothesis, the factorizations

$u\pi_2 \cdots \pi_r$ and $u'u_1\pi_2' \cdots \pi_s'$ are equivalent. It follows that $r = s$ and there exists $\sigma \in S_{[2:r]}$ and units $u_2, \ldots, u_r \in R^\times$ such that $\pi_i' = u_i\pi_{\sigma(i)}$ $(i = 2, \ldots, r)$. Extend σ to S_r by defining $\sigma(1) = 1$. Thus, taking $\sigma \in S_r$ and $u_1, \ldots, u_r \in R^\times$, we know that $\pi_i' = u_i\pi_i$ $(i = 1, \ldots, r)$. Therefore, $u\pi_1 \cdots \pi_r$ and $u'\pi_1' \cdots \pi_s'$ are equivalent factorizations of a, as desired. □

- To prove that something is a UFD, it is all important to show that irreducible...??
- Notation: $a \mid b$ iff $b \in (a)$.
- **Greatest common divisor**: The number pertaining to $a, b \in R$ both nonzero which satisfies the following two constraints. *Denoted by* $\boldsymbol{d}$, $\mathbf{gcd}(\boldsymbol{a}, \boldsymbol{b})$, $\mathbf{g.c.d.}\,(\boldsymbol{a}, \boldsymbol{b})$. *Constraints*

  (i) $d \mid a$ and $d \mid b$.

  (ii) $d' \mid a$ and $d' \mid b$ implies $d' | d$.

- d is well-defined up to multiplication by $u \in R^\times$.
  - Example: We commonly think of $\gcd(6, 9) = 3$, but in $\mathbb{Z}$, it could also be $-3 = -1 \cdot 3$ where $-1 \in \mathbb{Z}^\times = \{\pm 1\}$.
- Essay: $d \mid a$ implies $a = bd$ and the factors of d are a subset of the factors of a. Let $a = u\pi_1 \cdots \pi_r \cdot \pi_1'\pi_2' \cdots \pi_h'$ and $b = u'\pi_1 \cdots \pi_r \cdot \pi_1''\pi_2'' \cdots \pi_g''$. For all $i \leq h$, $j \leq g$: $\pi_i \nmid \pi_j''$.
  - I.e., the factors of a, b that don't multiply out to $\gcd(a, b) = d$ are all relatively prime.
- Let $d = \pi_1 \cdots \pi_r = \gcd(a, b)R$.
- Existence of factorization in a PID.
- Example: $F[X]$.
  - Recall that $F[X]$ is a PID.
  - Let $f \in F[X]$ have $\deg(f) > 0$.
  - Then since PIDs are UFDs, $f = uf_1 \cdots f_r$ where $u \in F[X]^\times = F^\times$ and each f_i is irreducible.
  - We have that $\deg f = \deg f_1 + \cdots + \deg f_r \geq r$.
  - This is the Fundamental Theorem of Algebra!
- We now attempt a rigorous proof of the existence of prime factorizations in PIDs. Without a convenient norm from which to derive a prime factorization (as we have in EDs), we need this proof.
  - Suppose that $a \in R$ nonzero is not a unit.
  - Then $a = bc$ where $b, c \notin R^\times$.
  - If b or c has a factorization, then $a = bc$ factors further.
  - WLOG, let c have a factorization.
  - Let $c = b_1a_2$, where $b_1, a_2 \notin R^\times$. Suppose a_2 admits a factorization. Then $a_2 = b_2a_3$, where $b_2, a_3 \notin R^\times$.
  - We can go on forever: $a_n = b_na_{n+1}$ where $b_n \notin R^\times$ and a_{n+1} factors further.
  - By their definitions, $\cdots (a_n) \subset (a_{n+1}) \cdots$. Additionally, $b_n \notin R^\times$ implies $(a_n) \neq (a_{n+1})$.
  - Now consider a chain of ideals $I_1 \subset I_2 \subset I_3 \subset \cdots$. Is $\bigcup_{n=1}^\infty I_n$ an ideal? Yes, it is. Let's call it I.
  - R is a PID implies that $I = (\alpha)$.
  - Definition of an infinite union: There exists n such that $\alpha \in I_n$. Therefore, $(\alpha) \subset I_n \subsetneq I_{n+1} \subset \cdots \subset (\alpha)$. It follows that the factorization is finite.
  - See the proof in the book for clarification: Theorem 8.14 of Dummit and Foote (2004).

- Last theorem to prove.
- Theorem: R is a PID implies R is a UFD.
  - Existence, we've done directly above.
  - Equivalence: By Lemma*, we only need irreducible $\pi \in R$ to be prime.
  - a is reducible.
  - Gist: $a = bc$, $b \notin R^\times$ and $c \notin R^\times$ implies $(a) \subsetneq (b) \subsetneq R$. Thus, a is irreducible. It follows that (a) is maximal and hence (a) is prime. All these concepts are equivalent in a PID.
- Examples: $\mathbb{Z}$, $F[X]$, $F[[X]]$.
- Let $a_n = b_n a_{n+1}$. Then $(a_n) \subset (a_{n+1})$. and $b_n \notin R^\times$.
- If $(a_n) = (a_{n+1})$, then $a_{n+1} = ca_n$, $a_n = b_n \subset a_n$, $1 = b_n c$.
- Lastly, we have a theorem summarizing some of today's results.
- Theorem: Let R be an integral domain such that every nonzero $a \in R$ admits a factorization. Then TFAE.
  1. R is a UFD.
  2. Every irreducible element of R is prime.
  3. Every pair of elements of R has a gcd.

  Proof. Partially given above. □

4.3 Office Hours (Callum)

- What kind of stuff from the recent lectures do we need to use in HW3?
  - It is mostly content from before Wednesday of Week 3.
  - The Euclidean algorithm will crop up in a few places, and some more recent/advanced stuff may be needed to solve the last problem.
- Do we need to provide rationale for our answers to Q3.1?
  - Yes.
  - We can just give a general proof once in the first one.
- Is Q3.2 a rote check of the definition? Are there any other factors to worry about?
  - It is straight from the definition.
- Is Q3.3(iii) too difficult?
  - The forward inclusion $I_1 I_2 \subset I_1 \cap I_2$ always holds. The backwards one needs coprime ideals (i.e., the fact that $(m) + (n) = \mathbb{Z}$ if m, n are coprime).
- Q3.5?
  - No complications; just consecutive applications of the universal property of $R[X]$ should yield the desired result.
- Is Q3.6 discussing evaluation functions?
  - Yes, even though they're denoted ϕ there.
  - See the Corollary from Lecture 3.1 for help on this problem.

- Hint for Q3.6(ii)?
  - This is a "you either see it or you don't" problem.
  - It shouldn't take that long to do once you see it, but it could take a long time to see it.
- For Q3.7, do we just have to define an inverse ψ and check $\phi \circ \psi = \psi \circ \phi = \mathrm{id}$, or do we need to conduct a broader set of isomorphism checks, such as bijectivity, ring homomorphism ones, etc.?
  - Cite Q3.5 for proving that the inverse is a ring homomorphism. Other than that, not really — it is mainly about focusing on the inverse condition.
- What is meant by "type" in Q3.8? Does the argument have to be a monomial of the given form, or are higher order polynomials allowed, too? Do you more broadly mean evaluation-based functions?
  - Exactly the same monomial evaluation. The only degrees of freedom are a, b.
- Is $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$?
  - Yes.
  - Note: Don't use q as a dummy variable because $\mathbb{F}_q$ is something else.
- In Q3.9(ii), how do I prove that there are always two a's that go to a^2? Can I just show that $a^2 = 1^2 a^2$ or something?
  - Don't use (i) to prove (ii); just use similar reasoning.
  - I've already made the big observation by noting that its $\pm a$ that both square to the same number. Rest should be smooth sailing.
- Thoughts on Q3.10?
  - By far the hardest question.
  - Tips: Show that $X^2 - \theta^2$ is a maximal ideal in the polynomial ring. If f is irreducible, then (f) is maximal. Check that $X^2 - \theta^2$ is irreducible.
  - Like 5 problems in 1 problem. Takes a bunch of techniques. The case where the square is zero is not hard. Write down four distinct rings and then use this to prove that you can't get any other ones. Keep them all in the quotient form? One is a product of two cyclic groups; that's a product of fields. You're allowed to multiply differently when they're rings, not groups. 2 groups, but 4 rings.

4.4 Division and the Chinese Remainder Theorem

1/27:

- This whole lecture is a speech for PIDs over UFDs.
- Proposition: Let R be a PID, and let $\pi \in R$ be nonzero. Then TFAE.

  (1) π is irreducible.

  (2) (π) is a maximal ideal.

  (3) π is prime.

  Proof. (2) $\implies$ (3): Since (π) is a maximal ideal, $R/(\pi)$ is a field. Thus, it's an integral domain. Therefore, (π) is a prime ideal.

  (3) $\implies$ (1): Holds in any integral domain.

  (1) $\implies$ (2): If (π) is not maximal, then there exists an ideal I such that $(\pi) \subsetneq I \subsetneq R$. But $I = (a)$. Then $\pi = ab$. $I \neq R$ implies that $a \notin R^\times$. Additionally, $(\pi) \neq (a)$ implies $b \notin R^\times$. Therefore, π is reducible, a contradiction. $\square$

- Recall computing greatest common divisors from last lecture.
  - In particular, we know that $R - \{0\}$ (or R??) is an integral domain.
  - Thus, if $a, b \in R - \{0\}$, then $a \sim b$ if there exists $u \in R^\times$ such that $a = ub$.
    - Nori confirms that $\sim$ is an equivalence relation.
    - If $a \sim b$, we say that a is an **associate** of b.
  - Notation: $\sim \backslash R - \{0\}$ implies that we're applying the equivalence relation $\sim$ to the set $R - \{0\}$.
  - $\gcd(a, b) \in \sim \backslash R - \{0\}$.
    - This allows us to define a unique gcd; recall that gcd's are only unique up to multiplication by units, so by making all **associates** the same equivalence class, we can define a unique one.
- **Associate** (elements): Two elements $a, b \in R$ such that $a = ub$ where $u \in R^\times$. *Denoted by* $\boldsymbol{a \sim b}$.
- Lemma: If $a, b \in R$ a PID, then $\gcd(a, b)$ is equal to any generator of the ideal $Ra + Rb$.

  Proof. Since R is a PID, there exists $d \in R$ such that $Ra + Rb = Rd$. Any such d is a generator of $Ra + Rb$. To prove that $d = \gcd(a, b)$, it will suffice to show that $d \mid a$, $d \mid b$, and $d' \mid a, b$ implies $d' \mid d$. Let's begin.

  Since $Ra, Rb \subset Ra + Rb = Rd$, we know that $a, b \in (d)$. Thus, $d \mid a, b$. Now let $d' \in R$ be an arbitrary element such that $d' \mid a$ and $d' \mid b$. It follows that $a, b \in (d')$. Since $d \in Ra + Rb$, there exist $\alpha, \beta \in R$ such that $\alpha a + \beta b = d$. Thus, $d = \alpha a + \beta b \in (d')$, so $d' \mid d$, as desired. □
- Look back to $AX + AY$ from Lecture 2.2!
- We will see later (next week) that $F[X, Y]$ is a UFD and that $\gcd(X, Y) = 1$.
  - But $1 \notin (X, Y)$.
- Assume R is a UFD and $a \neq 0$.
  - A (traditional) factorization of $a = u\pi_1^{k_1}\pi_2^{k_2}\cdots\pi_r^{k_r}$. We assume as we have been that each π_i is irreducible and $i \neq j$ implies that $(\pi_i) \neq (\pi_j)$ iff $\pi_i \nsim \pi_j$.
  - What is $R/(a)$?
  - Note: If $I \subset J \subset R$, then there exist ring homomorphisms from

    $$R \to R/I \qquad R \to R/J \qquad R/I \to R/J$$

  - Consider $(a) \subset (\pi_i^{k_i})$. Then $R/(a) \to R/(\pi_i^{k_i})$. Moreover, we get a ring homomorphism

    $$R/(a) \hookrightarrow \prod_{i=1}^{r} R/(\pi_i^{k_i})$$

    - For the integers, this is an isomorphism.
    - See the Chinese remainder theorem.
  - As per before, there exists $\varphi : R \to \prod_{i=1}^r R/(\pi_i^{k_i})$.
  - What is $\ker(\varphi)$?
  - We have that $\varphi(h) = 0$ iff $\pi_i^{k_i} \mid h$ for all $i = 1, 2, \ldots, r$ iff $\prod_{i=1}^r \pi_i^{k_i} \mid h$ iff $a = u\prod_{i=1}^r \pi_i^{k_i} \mid h$ iff $h \in (a)$.
    - Nori pauses to motivate why the factors of a dividing h implies that that the product of the factors does as well.
  - $\ker(\varphi) = (a)$. Product of commutative diagrams?? *See lower right of board 2*
  - Let $I \subset J_1 \subset R$ and $I \subset J_2 \subset R$.

- Aside.
  - Let $R = F[X, Y]$.
  - Then $R/(XY) \to (R/(X)) \times (R/(Y))$ is not onto.
  - Note that $R/(X) = F[X, Y]/(X) \cong F[Y]$ and likewise for $R/(Y)$.
  - There is a function $R \to R/(XY)$.
  - $f(X, Y) \in R$ maps to $f(0, Y)$ and $f(X, 0)$. There must be a condition: $g(0) = h(0)$.
- Let $\pi_1^{k_1} = b$ and $\pi_2^{k_2} \cdots \pi_r^{k_r} = c$. Then $\gcd(b, c) = 1$. If R is a PID, then $Rb + Rc$ is the ideal generated by $\gcd(b, c)$, and hence is R.
  - It follows that there exists $\beta, \gamma \in R$ such that $\beta\pi_1^{k_1} + \gamma c = 1$.
  - This is the Chinese Remainder Theorem.
  - Consider $R \to R/(\pi_1^{k_1}) \times (R/(\pi_2^{k_2}) \times \cdots \times R/(\pi_r^{k_r}))$ sending
    $$\gamma c \mapsto (1, 0, \ldots, 0)$$
  - Multiply by an arbitrary $h \in R$. Then $h\gamma c \mapsto (h, 0, \ldots, 0)$.
  - The image contains $R/(\pi_1^{k_1}) \times 0 \times \cdots \times 0$ which contains $0 \times R/(\pi_2^{k_2}) \times 0 \times \cdots \times 0$. This is because if we have $(\alpha_1, \ldots, \alpha_r)$, then we can always write it as
    $$(\alpha_1, \ldots, \alpha_r) = (\alpha, 0, 0, \ldots, 0) + (0, \alpha_2, 0, \ldots, 0) + \cdots + (0, 0, 0, \ldots, \alpha_r)$$
- **Chinese Remainder Theorem**: Let R be a PID, and let a factor as we've discussed. Then the natural arrow $R/(a) \to \prod_{i=1}^{r} R/(\pi_i^{k_i})$ is an isomorphism of rings.
- Examples:
  - $F[X]$: $X - a$ is irreducible for all $a \in F$.
  - $\mathbb{C}[X]$: These are the only irreducibles (fundamental theorem of algebra).
  - $\mathbb{R}[X]$: $X - a$ for $a \in \mathbb{R}$ and $(X - z)(x - z)$ for $z \in \mathbb{C} - \mathbb{R}$ are all irreducible.
- Corollary of the earlier lemma: If $R_1 \subset R_2$ are both PIDs and $(a, b) \in R_1$, then "$\gcd_{R_1}(a, b) = \gcd_{R_2}(a, b)$."

  Proof. Let $R_1 a + R_1 b = R_1 d$, $d \in R_1$. Then $R_2 a + R_2 b = R_2 d$. □
- Explanation of what's in quotes: We're taking gcd's in different rings. See the commutative diagram below.

$$\begin{array}{ccc} R_1 - \{0\} & \hookrightarrow & R_2 - \{0\} \\ \downarrow & & \uparrow \\ \sim \backslash R_1 - \{0\} & \longrightarrow & \sim \backslash R_2 - \{0\} \end{array}$$

Figure 4.1: Greatest common divisor in different rings.

- We should check this.
- How do we put $F[X, Y] \subset F[X, Z]$? Put $Y = XZ$. Then $\gcd(X, Y) = 1$.
- Midterm on Monday of sixth week; HW pushed to Friday that week.
- Problem: Let F be a subfield of the field E. Assume $\gcd(f, g) = 1$ where $f, g \in F[X]$. Show that there does not exist $a \in E$ such that $f(a) = g(a) = 0$.
- Problem: Let $f \in \mathbb{Q}[X]$. Assume that $\gcd(f, f') = 1$ where f' denotes the derivative of f. Prove that if $f(a) = 0$ for some $a \in \mathbb{R}$, then f is not divisible by $(X - a)^2$ in $\mathbb{R}[X]$.

4.5 Chapter 7: Introduction to Rings

From Dummit and Foote (2004).

Section 7.6: The Chinese Remainder Theorem

2/1:

- Assume commutative rings with identity.
- **Ring direct product**: The direct product of an arbitrary collection of rings as (abelian) groups, which is made into a ring by defining multiplication componentwise. *Denoted by* $\boldsymbol{R_1 \times R_2}$.
- $\varphi : R \to R \times \cdots$ is a ring homomorphism iff the induced maps to each component are all homomorphisms.
- The units of a ring direct product are the n-tuples that have units in every entry.
- **Comaximal** (ideals): Two ideals $A, B \subset R$ such that $A + B = R$.
  - Motivation: Two numbers $n, m \in \mathbb{Z}$ being relatively prime is equivalent to $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$, where we may recall that $n\mathbb{Z}, m\mathbb{Z}$ are ideals.
- Generalizing a result about integer division to rings.

  Theorem 7.17 (Chinese Remainder Theorem)**.** Let $A_1, \ldots, A_k$ be ideals in R. The map from $R \to R/A_1 \times \cdots \times R/A_k$ defined by
  $$r \mapsto (r + A_1, \ldots, r + A_k)$$
  is a ring homomorphism with kernel $A_1 \cap \cdots \cap A_k$. If for each $i, j \in \{1, \ldots, k\}$ with $i \neq j$, the ideals A_i, A_j are comaximal, then this map is surjective and $A_1 \cap \cdots \cap A_k = A_1 \cdots A_k$, so
  $$R/(A_1 \cdots A_k) = R/(A_1 \cap \cdots \cap A_k) \cong R/A_1 \times \cdots \times R/A_k$$

  Proof. Given. See HW3 Q3.3. □
- History of the Chinese Remainder Theorem.
  - Derives its name from the special case that when n, m are relatively prime integers,
    $$\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$$
  - In number theoretic terms: This "relates to simultaneously solving two congruences modulo relatively prime integers (and states that such congruences can always be solved, and uniquely)" (Dummit & Foote, 2004, p. 266).
  - Such problems were originally considered by the ancient Chinese.
- Using the Chinese Remainder Theorem to prove the Euler φ-function.

  Corollary 7.18. Let n be a positive integer and let $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be its factorization into powers of distinct primes. Then
  $$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})$$
  as rings, so in particular, we have the following isomorphism of multiplicative groups.
  $$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times$$
  Thus,
  $$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$$

  Proof. Since the rings above are isomorphic as rings, their groups of units must be isomorphic as well. Comparing orders on the two sides of the latter isomorphism gives the final result. □

4.6 Chapter 8: Euclidean Domains, Principal Ideal Domains, and Unique Factorization Domains

From Dummit and Foote (2004).

Goals for the Chapter

1/30:

- Focus: Study classes of rings with more algebraic structure than generic rings.
- **Euclidean Domain**: A ring with a division algorithm. *Also known as* **ED**.
- **Principal Ideal Domain**: A ring in which every ideal is principal. *Also known as* **PID**.
- **Unique Factorization Domain**: A ring in which all elements have factorizations into primes. *Also known as* **UFD**.
- Examples: $\mathbb{Z}$ and $F[X]$ (F a field).
- This chapter: Recover all theorems concerning the integers $\mathbb{Z}$ stated in Chapter 0 as special cases of results valid for more general rings.
- Next chapter: Apply these results to the special case where $R = F[X]$.
- Assumption for this chapter: All rings R are commutative.

Section 8.1: Euclidean Domains

- Definitions of a **norm** and **Euclidean Domain**.
- Notes on norms.
  - Essentially a measure of "size" in R.
  - The defined notion is fairly week, and an integral domain R may possess several different norms.
- **Positive norm**: A norm N such that $N(a) > 0$ for all $a \neq 0$.
- EDs are said to possess a **Division Algorithm**.
- Converting between the book's definition of an ED and the in-class one.
  - Take the N of the book, define $N'(x) = N(x) + 1$ for all nonzero $x \in R$ and $N'(0) = 0$. Then N' satisfies the in-class requirements.
- **Quotient**: The element q in the definition of a norm/ED. *Denoted by* $\boldsymbol{q}$.
- **Remainder**: The element r in the definition of a norm/ED. *Denoted by* $\boldsymbol{r}$.

2/1:

- Division Algorithms allow a **Euclidean Algorithm** for two elements $a, b \in R$ to find the greatest common divisor.
  - Note that these "divisions" are actually divisions in $\operatorname{Frac} R$, for example.
  - Also, note that the Euclidean algorithm terminates since $N(b) > N(r_0) > \cdots > N(r_n)$ is a decreasing sequence of nonnegative integers and thus cannot continue indefinitely.
  - We have no guarantee (yet) that the quotient and remainder are unique.
- Examples.
  1. Fields.
     - Any norm satisfies the defining condition of the Division Algorithm because we always have $a = qb + 0$ for any $a, b \in F$.

2. Integers $\mathbb{Z}$, $N(m) = |m|$.
   - From class.
   - Dummit and Foote (2004) proves rigorously, from a ring theory perspective, that long division is a thing.
   - The quotient and remainder are not unique (unless we require the remainder is nonnegative).
     - Example: $5 = 2 \cdot 2 + 1 = 3 \cdot 2 - 1$.
3. $F[X]$ with $N(f) = \deg(f)$.
   - That long division is a thing is proved similarly to for $\mathbb{Z}$ (see Chapter 9).
   - For polynomials, the quotient and remainder are unique.
   - We will prove later that $R[X]$ is an ED iff R is a field. Essentially, this is because we must be able to divide arbitrary nonzero coefficients.
4. Quadratic integer rings are not EDs in general.
   - Take the absolute value of the field norm to get a potential norm, but these rarely work.
   - Gaussian integers do work, though, under this absolute value field norm.
   - The rest of the proof that $\mathbb{Z}[i]$ is an ED goes beyond the scope of class.
5. **Discrete valuation rings**.
   - Take $N = \nu$ and $N(0) = 0$.

- **Discrete valuation** (on K): A function from $K^\times \to \mathbb{Z}$, where K is a field, satisfying the following constraints. *Denoted by* $\boldsymbol{\nu}$. *Constraints*

  (i) $\nu(ab) = \nu(a) + \nu(b)$, i.e., $\nu : (K^\times, \cdot) \to (\mathbb{Z}, +)$ is a group homomorphism.

  (ii) ν is surjective.

  (iii) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$ for all $x, y \in K^\times$ with $x + y \neq 0$.

- **Valuation ring** (of ν): The subring of K defined as follows. *Given by*

$$\{x \in K^\times : \nu(x) \geq 0\} \cup \{0\}$$

- **Discrete valuation ring**: An integral domain R for which there exists a valuation ν on $\operatorname{Frac} R$ such that R is the valuation ring of ν.

- Example: The ring R containing all rationals whose denominators are relatively prime to some fixed $p \in \mathbb{Z}$ is a discrete valuation ring of $\mathbb{Q}$.

- A Division Algorithm makes every ideal of an ED principal.

  Proposition 8.1. Every ideal in an ED is principal. More precisely, if I is any nonzero ideal in the ED R, then $I = (d)$, where d is any nonzero element of I of minimum norm.

  Proof. Given (see Lecture 4.1). □

- Since $\mathbb{Z}$ is an ED, Proposition 8.1 implies that every ideal of $\mathbb{Z}$ is principal.
  - Recall that we have previously proven this in Section 7.3 and 2.3.

- Examples.
  1. Consider $\mathbb{Z}[X]$.
     - Since $(2, X)$ is not principal (see Section 7.4), $\mathbb{Z}[X]$ is not an ED.
  2. The quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$ is not a PID.
     - Consider the ideal $I = (3, 2 + \sqrt{-5})$. Suppose it equals $(a + b\sqrt{-5})$ for some $a, b \in \mathbb{Z}$ and then arrive at contradictions in every case you consider.

- Euclidean Algorithms guarantee a greatest common divisor in any ED.
- **Multiple** (of b): An element $a \in R$ such that $a = bx$ for some $x \in R$.
- **Divisor** (of a): An element $b \in R$ such that $a = bx$ for some $x \in R$. *Also known as* $\boldsymbol{b}$ **divides** $\boldsymbol{a}$.
- Definition of the **greatest common divisor** of a, b.
- Note:
$$b \mid a \iff a \in (b) \iff (a) \subset (b)$$
  - More on discussing gcd's in terms of ideals (repeat from class).
- A *sufficient* condition for the existence of a gcd.

  Proposition 8.2. If a, b are nonzero elements in the commutative ring R such that the ideal generated by a, b is a principal ideal (d), then d is the greatest common divisor of a, b.

- Note that the condition is not *necessary*: For example, in $\mathbb{Z}[X]$, $(2, x)$ is nonprincipal even though 1 is a valid gcd.
- **Bezout Domain**: An integral domain in which every ideal generated by two elements is principal.
  - Per the exercises, there are Bezout Domains that contain nonprincipal (necessarily infinitely generated) ideals.
- gcd uniqueness.

  Proposition 8.3. Let R be an integral domain. If two elements d, d' of R generate the same principal ideal, i.e., $(d) = (d')$, then $d' = ud$ for some unit $u \in R$. In particular, if d, d' are both greatest common divisors of a, b, then $d' = ud$ for some unit u.

  Proof. Not very important since its only relation to class content is via the lemma from Lecture 4.3 that $Ra + Rb = (\gcd(a, b))$. However, included because it's very slick. We prove each statement separately.

  Suppose $(d) = (d')$. We divide into two cases (d or d' is 0, and neither is zero). Suppose first that d or d' is 0. WLOG, let $d = 0$. Then $d' \in (0) = \{0\}$, so $d' = 0$. Therefore, since $0 = 1 \cdot 0$, $d' = ud$ for a unit (specifically the identity, for example) in R. Now suppose that $d, d' \neq 0$. Since $d \in (d')$, $d = xd'$ for some $x \in R$. Similarly, $d' = yd$ for some $y \in R$. It follows that

  $$\begin{aligned} d &= xyd \\ d(1 - xy) &= 0 \end{aligned}$$

  Since R is an integral domain, $d = 0$ or $1 - xy = 0$. But $d \neq 0$ by hypothesis, so

  $$\begin{aligned} 1 - xy &= 0 \\ 1 &= xy \end{aligned}$$

  Therefore, x, y are both units and we have the desired result.

  If d, d' are both gcd's of a, b, then $(d) = (d')$. Thus, apply the first statement to obtain the desired result. □

- Very important property of EDs: gcd's always exist and can be computed algorithmically.

  Theorem 8.4. Let R be an ED, and let $a, b \in R$ be nonzero. Let $d = r_n$ be the last nonzero remainder in the Euclidean algorithm for a, b. Then

  1. $d = \gcd(a, b)$.

2. The principal ideal $(d) = (a, b)$. In particular, d can be written as an R-linear combination of a, b, i.e., there exist $x, y \in R$ such that
$$d = ax + by$$

Proof. Given (see the Lemma from Lecture 4.3). □

- The Euclidean Algorithm is **logarithmic** in the size of the integers.
  - It can be proven that "the number of steps required to determine the greatest common divisor of two integers a and b is at worst 5 times the number of digits of the smaller of the two numbers" (Dummit & Foote, 2004, p. 276).
- Some more stuff on uniqueness and Diophantine equations.
- $\widetilde{\boldsymbol{R}}$: The collection of units of R together with 0. *Given by*
$$\widetilde{R} = R^\times \cup \{0\}$$
- **Universal side divisor**: An element $u \in R - \widetilde{R}$ such that for every $x \in R$, there is some $z \in \widetilde{R}$ such that u divides $x - z$ in R.
  - Implication: There is a type of division algorithm for every $x \in R$ by u; indeed, if $u \mid (x - z)$, then there exists $q \in R$ such that $x - z = qu$ or
$$x = qu + z$$
- The existence of universal side divisors is a weakening of the Euclidean condition (i.e. here, we only postulate that we can divide by *some* elements, not *all* elements).

  Proposition 8.5. Let R be an integral domain that is not a field. If R is a Euclidean Domain, then there are universal side divisors in R.

  Proof. Given. □
- Example: Proving $\mathbb{Z}[(1 + \sqrt{-19})/2]$ is not an ED using Proposition 8.5.

Section 8.2: Principal Ideal Domains

2/3:
- Definition of a **PID**.
- Since EDs are PIDs, all results proved herein hold for EDs, too.
- Examples.
  1. $\mathbb{Z}$ is a PID; $\mathbb{Z}[X]$ is not (think $(2, X)$).
  2. Quadratic integer rings.
- Not every PID is an ED.
- Dummit and Foote (2004) believes that PIDs are a natural class of rings in which to study ideals.
- Both EDs and PIDs have gcd's; only EDs have an algorithm for computing them, though.
  - Thus, gcd-adjacent results are often proven in PIDs, but specific examples are typically computed using a Euclidean Algorithm if available.
- Facts about gcd's.

Proposition 8.6. Let R be a PID and let a, b be nonzero elements of R. Let d be a generator for the principal ideal generated by a and b. Then...

1. d is a greatest common divisor of a and b;
2. d can be written as an ***R*-linear combination** of a and b.
3. d is unique up to multiplication by a unit of R.

Proof. See Propositions 8.2-8.3, which this proposition just rehashes. □

- Per Corollary 7.14, every maximal ideal is a prime ideal. The converse also holds in PIDs.

  Proposition 8.7. Every nonzero prime ideal in a PID is a maximal ideal.

  Proof. See Lecture 4.3. □

- Recall that F a field implies that $F[X]$ is an ED. The converse also holds in PIDs.

  Corollary 8.8. If R is any commutative ring such that the polynomial ring $R[X]$ is a PID (or an ED), then R is necessarily a field.

  Proof. Given. □

- We wrap up by proving that not every PID is an ED. We also relate the principal ideal property to another weakening of the Euclidean condition.
- **Dedekind-Hasse norm**: A positive norm N such that for every nonzero $a, b \in R$, either $a \in (b)$ or there exists a nonzero element $x \in (a, b)$ such that $N(x) < N(b)$.
  - Alternate definition: Either $b \mid a \in R$ or there exist $s, t \in R$ such that $0 < N(sa - tb) < N(b)$.
  - Dedekind-Hasse norms and all related content will be omitted from this course.
- R is Euclidean with respect to N if it is always possible to satisfy the Dedekind-Hasse condition with $s = 1$..
  - This means that other values of s represent a related but weaker condition than the Euclidean one; this is the weakening alluded to above.
- PIDs and Dedekind-Hasse normed spaces are equivalent.

  Proposition 8.9. The integral domain R is a PID iff R has a Dedekind-Hasse norm.

  Proof. Given. □

- Note: That a ring satisfying the Dedekind-Hasse condition is a PID has been known since 1928. That a PID necessarily satisfies the Dedekind-Hasse condition was not discovered until 1997.
- Example: Proof that $\mathbb{Z}[(1 + \sqrt{-19})/2]$ is a PID but not an ED.

Section 8.3: Unique Factorization Domains

2/5:

- In addition to the Euclidean Algorithm, gcd's can be computed via factorization into primes and a simple comparison.
- The notion of factorization can be extended to a larger class of rings called UFDs.
- Goal of this section: Prove that every PID is a UFD; thus, all results in this section will hold for EDs and PIDs, too.
- **Irreducible** (element): A nonzero element $r \in R$ that is not a unit and such that whenever $r = ab$ with $a, b \in R$, at least one of a or b must be a unit in R.
- **Reducible** (element): An element that is not reducible.
  - Recall from class that even though it's not explicitly stated in the definition, we can prove that reducible elements are not units.
- **Prime** (element): A nonzero element $p \in R$ that is not a unit and such that whenever $p \mid ab$ for any $a, b \in R$, then either $p \mid a$ or $p \mid b$.
  - The definition from class is also given.
- Definition of **associate** elements.
- Prime implies irreducible.

  Proposition 8.10. In an integral domain, a prime element is always irreducible.

  Proof. Let (p) be an arbitrary prime ideal in R an integral domain. Suppose $p = ab$. Then $ab \in (p)$, so WLOG $a \in (p)$. It follows that $a = pr$ for some $r \in R$. Thus, $p = ab = prb$, so by the cancellation lemma (which applies under the given hypotheses), $rb = 1$. Therefore, b is a unit, so p is irreducible, as desired. □

- Irreducible $\not\Rightarrow$ prime in general.
  - Example using quadratic integer rings given.
- Prime $\iff$ irreducible in a PID.

  Proposition 8.11. In a PID, a nonzero element is prime iff it is irreducible.

  Proof. Given (see Lecture 4.3). □

- Example.
  1. Quadratic integer rings.
- Example:
  - The irreducible of $\mathbb{Z}$ are the prime numbers (and their negatives).
  - Two integers $a, b \in \mathbb{Z}$ are associates iff $a = \pm b$.
- Dummit and Foote (2004) discusses factorization in $\mathbb{Z}$ in the language of rings (e.g., "units," "irreducible," "unique," etc.) to motivate UFDs.
  - Very insightful.
- **Prime factorization**: The expression of an element in $\mathbb{N}$ as a product of other elements in $\mathbb{Z}$, all of which are positive and prime.

- Definition of a **UFD**.
- Examples.
  1. All fields F are trivially UFDs.
     - All elements are units, so there exist no elements for which we can verify the constraints, so the condition is vacuously true.
  2. PIDs are UFDs.
     - E.g., $\mathbb{Z}$, $F[X]$ are UFDs.
  3. $R[X]$, where R is a UFD.
     - See Theorem 9.7.
     - This contrasts with EDs and PIDs, where R being an ED (resp. PID) does not make $R[X]$ an ED (resp. PID).
     - It follows that $\mathbb{Z}[X]$ is a UFD.
  4. $\mathbb{Z}[2i]$: Integral domain that is not a UFD.
     - See Exercise 7.1.23.
     - Argument included.
  5. $\mathbb{Z}[\sqrt{-5}]$: Another integral domain that is not a UFD.
     - Argument included.
- Proposition 8.11 for UFDs.

  Proposition 8.12. In a UFD, a nonzero element is prime iff it is irreducible.

  Proof. Given (not covered in class).

  Note that this proposition plus the previously alluded to result that PID $\implies$ UFD do *not* suffice to prove Proposition 8.11. This is because we will need Proposition 8.11 to prove that PID $\implies$ UFD, and we must avoid circular reasoning. □
- Greatest common divisors exist in UFDs.

  Proposition 8.13. Let a, b be two nonzero elements of a UFD R and suppose that

  $$a = up_1^{e_1} \cdots p_n^{e_n} \qquad\qquad b = vp_1^{f_1} \cdots p_n^{f_n}$$

  are prime factorizations for a and b, where u, v are units, the primes $p_1, \ldots, p_n$ are *distinct*, and the exponents $e_i, f_i \geq 0$ $(i = 1, \ldots, n)$. Then the element

  $$d = p_1^{\min(e_1, f_1)} \cdots p_n^{\min(e_n, f_n)}$$

  (where $d = 1$ if all the exponents are 0) is a gcd of a, b.

  Proof. Given (not directly covered in class; related to Statement (*) from Lecture 5.1). According to the Week 4 summary, it is important. The proof in the book is a bit hand-wavey, though.

  We first must prove that $d \mid a, b$. This follows immediately from the fact the the exponents of each prime in d are no larger than the corresponding ones in a, b.

  We now must prove that if $c \mid a, b$, then $c \mid d$. Since R is a UFD, factor c into $q_1^{g_1} \cdots q_m^{g_m}$. Consider an arbitrary q_i. Since it divides c, it must divide a, b. In particular, since it and all of the p_j are irreducible by Proposition 8.12, it must divide some p_j to yield a unit. Thus, q_i and p_j are the same up to associates. Consequently, all q's are equal to p's up to associates. We get a similar condition on the exponents to that in d, implying that $c \mid d$, as desired. □

- Example.

  1. An application of Proposition 8.13.

- We now prove the main result.

  Theorem 8.14. Every PID is a UFD. In particular, every ED is a UFD.

  Proof. Let R be a PID, and let r be an arbitrary nonzero element of R which is not a unit. To prove that R is a UFD, it will suffice to show that r can be written as a finite product of irreducible elements of R and that this decomposition is unique up to associates.

  Existence: We proceed analogously to the prime factorization algorithm for integers, meaning that we will divide into cases, subcases, subsubcases, etc. as needed depending on whether or not all factors are irreducible at each step and then use the "finiteness" of r to prove that the decomposition can only go on for so long. To see what this means, let's begin. If r is irreducible, then we are done. Otherwise, r is reducible, and hence $r = r_1 r_2$ where $r_1, r_2 \notin R^\times$. If r_1, r_2 are both irreducible, then (again) we are done. Otherwise, at least one of the two elements (say r_1) is reducible and hence can be written $r_1 = r_{11} r_{12}$ for nonunit elements r_{11}, r_{12}. We can continue on in this manner.

  We now verify that this process terminates. Precisely, we verify that we necessarily reach a point where all of the elements obtained as factors of r are irreducible. Let's begin. Suppose for the sake of contradiction that the process never terminates. Then we obtain a *proper* inclusion of ideals

  $$(r) \subsetneq (r_1) \subsetneq (r_{11}) \subsetneq \cdots \subsetneq R$$

  where the labeling is justified WLOG[2] Note that the above can also be called an infinite ascending chain of ideals. Also note that the first inclusion is proper because r_2 is not a unit, the second is proper because r_{12} is not a unit, on and on until the last inclusion is proper because $r_{1\cdots1}$ is not a unit. Lastly, note that we need the Axiom of Choice (why??) to justify the existence of such an infinite chain.

  To verify that the proper inclusion terminates, it will suffice to demonstrate that any ascending chain $I_1 \subsetneq \cdots \subsetneq R$ of ideals *in a PID* eventually becomes stationary. Precisely, we wish to find a positive integer n such that $I_k = I_n$ for all $k \geq n$. Let's begin. Let

  $$I = \bigcup_{i=1}^{\infty} I_i$$

  We can prove (easily from the definition) that I is an ideal. Thus, since R is a PID, we may write $I = (a)$ for some $a \in R$. It follows by the definition of I that $a \in I_n$ for some $n \geq 1$. By definition, $I_n \subset I$; additionally, $I = (a) \subset I_n$ since I_n is an ideal. Consequently, $I = I_n$ and the chain becomes stationary at I_n.

  Returning to the original case, the above result implies a contradiction. Thus, the original chain of ideals terminates. Therefore, a factorization of r into irreducibles is finite and, importantly, *exists*.

  Uniqueness: Since R is a PID, Proposition 8.11 implies that all irreducible elements are prime. Therefore, by Lemma* from Lecture 4.2, any two factorizations of r are equivalent, as desired. Note that Dummit and Foote (2004) proves their own version of Lemma* as part of the argument.

  The second statement follows from the first and Proposition 8.1. □

- In the proof of Theorem 8.14, we showed that any ascending chain of ideals in a PID eventually becomes stationary.

  – In Chapter 12, we will prove a more general result: An ascending chain of ideals becomes stationary in any commutative ring where all the ideals are *finitely generated*.

[2] If r_1 is irreducible and r_2 is reducible, flip the names.

- Theorem 8.14 implies another, very important result.

  Corollary 8.15 (Fundamental Theorem of Arithmetic)**.** The integers $\mathbb{Z}$ are a UFD.

  Proof. They're an ED, and hence a UFD by Theorem 8.14. □

- Relation to Dedekind-Hasse norms.

  Corollary 8.16. Let R be a PID. Then there exists a multiplicative Dedekind-Hasse norm on R.

  Proof. Given. □

- We now switch to the specific example of factorization in the Gaussian integers.
  - This will be covered in the class at a later date.
- Dummit and Foote (2004) proves a number of interesting theorems not covered in any depth in class.
- Dummit and Foote (2004) concludes the chapter with a short summary.
  - Restatement of the central result:

    $$\text{fields} \subsetneq \text{EDs} \subsetneq \text{PIDs} \subsetneq \text{UFDs} \subsetneq \text{integral domains}$$

  - Review of examples that prove *proper* inclusion:
    - $\mathbb{Z}$ is an ED, not a field.
    - $\mathbb{Z}[(1+\sqrt{-19})/2]$ is a PID, not an ED.
    - $\mathbb{Z}[X]$ is a UFD (see Theorem 9.7), not a PID.
    - $\mathbb{Z}[\sqrt{-5}]$ is an integral domain, not a UFD.

Week 5

Characterizing Polynomials

5.1 Prime Factorizations

1/30:

- Midterm next Monday.
  - There's a list of topics on Canvas.
  - Don't worry about quadratic fields (or any of the other examples in Chapter 7 of Dummit and Foote (2004)). These are interesting, but will be saved for the absolute end of the course.
  - After the midterm, Nori will start on modules.
  - We've been talking about fields, which are contained in EDs, which are contained in PIDs. There probably will not be anything on EDs. Use the weakest definition for ED (the ones in class and the book differ). Which is this??
  - PIDs are contained in UFDs, which are contained in integral domains, which are contained in commutative rings.
- PIDs are nice!
  - For instance, $\gcd(a, b)$ can be computed in them without factoring a, b.
  - This is accomplished with the Euclidean Algorithm.
    - Review page 2 of Chapter 8, as referenced in a previous class, for more context.
- In PIDs, you can factor $a = qb + r$, but q, r may not be specific; in EDs (under a nice norm), these q, r are unique.
  - Is this correct??
  - It can be proven that if R is an ED, $a = qb + r$ for $a, b \in R - \{0\}$ and $q, r \in R$ with $N(r) < N(b)$, then r, q are unique iff $N(a + b) \leq \max\{N(a), N(b)\}$.
  - For instance, we have this for $\mathbb{Z}$ under $|n|$ and for $R[X]$ under $2^{\deg(p)}$.
- Theorem: R is a UFD implies $R[X]$ is a UFD.
- Corollary: R is a UFD implies $R[X_1, \ldots, X_n]$ is a UFD.

  Proof. Use induction. □
- Corollary: $R[X]$ is a field implies R is a PID implies $R[X_1, \ldots, X_n]$ is a UFD.
  - Something about $\mathbb{Z}$, $F[[X]]$ where F is a field??
  - These are examples of PIDs.

- Example: What are the irreducibles of $\mathbb{Z}[X]$?
  - Prime numbers.
  - Let $g \in \mathbb{Q}[X]$. Assume g is monic. Then $g(X) = X^d + a_1X^{d-1} + \cdots + a_d$ for all $a_i \in \mathbb{Q}$. There exists $n \in \mathbb{N}$ such that $ng(X) \in \mathbb{Z}[X]$. Let n be the least natural number for which this is true. It follows by our hypothesis that n is the smallest such n that the coefficients of ng are relatively prime. Conclusion: $ng(X)$ is irreducible in $\mathbb{Z}[X]$.
- Takeaway: There are two types of irreducibles (those from $\mathbb{Z}$ and the new ones).
  - This statement has a clear parallel for every UFD.
- Let R be a UFD, and let $\mathcal{P}(R) \subset R - \{0\}$ be such that...
  (i) Every $\pi \in \mathcal{P}(R)$ is irreducible.
  (ii) For all $\alpha \in \mathbb{R} - \{0\}$, α irreducible, there exists a unique $\pi \in \mathcal{P}(R)$ such that $(\alpha) = (\pi)$.
- Statement (*): Every nonzero element $\alpha \in R$ is uniquely expressible as

$$\alpha = u \prod_{\pi \in \mathcal{P}(R)} \pi^{k(\pi)}$$

  where $u \in R^\times$ and for all π, $k(\pi) \in \mathbb{Z}_{\geq 0}$ and $|\{\pi \in \mathcal{P}(R) : k(\pi) > 0\}|$ is finite.

  Proof. R is a UFD implies (*). □
- Conversely, if $\mathcal{P}(R)$ is a subset of an integral domain R such that (*) holds, then R is a UFD.

  Proof. Note that $\pi \in \mathcal{P}(R)$ implies π is irreducible.

  Argument for something?? Let $\pi = ab$. Suppose $a = \pi^{m_0}\pi^{m_1} \cdots \pi_h^{m_h} u$ and $b = \pi^{n_0}\pi_1^{n_1} \cdots \pi_h^{n_h}$. Then $\pi = ab = \pi^{m_0+n_0}\pi^{m_1+n_1} \cdots$. But then because of unique factorization, we cannot have $\pi_1^{x_1} \cdots \pi_h^{x_h}$. □
- **Content** (of $f \in R[X]$): The greatest common divisor of the coefficients of a nonzero $f = a_0 + a_1X + a_2X^2 + \cdots$ in $R[X]$. *Denoted by* $\boldsymbol{c(f)}$. *Given by*

$$c(f) = \gcd(a_0, a_1, a_2, \dots)$$

- Let $c(f) = \prod_{\pi \in \mathcal{P}(R)} \pi^{k(\pi)}$.
- Gauss lemma: $f, g \in R[X]$ both nonzero implies that $c(fg) = c(f)c(g)$.

  Proof. For our purposes, it will suffice to prove the case where $c(f) = c(g) = 1$. This is because our ultimate purpose in proving this lemma is to show that a polynomial in $R[X]$ that is not irreducible is reducible specifically in $R[X]$, i.e., we need not resort to higher container rings such as $\operatorname{Frac} R$ in which we could reduce $p \in R[X]$. Let's begin.

  Let $\pi \in R$ be irreducible (hence prime). Consider the canonical surjection $R \to R/(\pi)$. It gives rise to a ring homomorphism $\varphi : R[X] \to R/(\pi)[X]$ defined by

$$\varphi(a_0 + a_1X + \cdots + a_dX^d) = \bar{a}_0 + \bar{a}_1X + \cdots + \bar{a}_dX^d$$

  In words, the ring homomorphism takes any input polynomial and reduces all of its coefficients modulo p. Moving on, $c(f) = 1$ implies that there exists i such that $\bar{a}_i \neq 0$ (if $c(f) = \pi$, for instance, then all $\bar{a}_i = 0$). Therefore, $\varphi(f) \neq 0$. Similarly, $c(g) = 1$ implies that $\varphi(g) \neq 0$. It follows since $R/(\pi)$ is an integral domain and thus contains no zero divisors that $\varphi(fg) = \varphi(f)\varphi(g) \neq 0$. Consequently, $\pi \nmid c(fg)$ (again, if $\pi \mid c(fg)$, then all coefficients would be divisible by π, hence would be equivalent to 0 mod π, hence $\varphi(fg)$ would equal 0). Clearly, this argument holds for any $\pi \in R$ irreducible. Thus, since $c(fg)$ is not divisible by any element of R, we must have that $c(fg) = 1$. □

- This proof can be done by brute force without quotient rings, and elegantly with quotient rings. Dummit and Foote (2004) does both and we should check this out. The above is Nori's cover of just the latter, elegant argument.
- Let K be the fraction field of R. We know that $K[X]$ is a PID (hence a UFD, etc.). The primes are the irreducible monic polynomials. Let $g = a_0 + a_1X + \cdots + a_{d-1}X^{d-1} + X^d \in K[X]$ be monic. Then there exists a nonzero $\alpha \in R$ such that $R[X] \subset K[X]$. It follows that $a_i = \alpha_i/\beta_i$ for some $\alpha_i, \beta_i \in R$ with $\beta_i \neq 0$ since $K = \operatorname{Frac} R$.
- Claim 1: There exists a unique $\beta \in R$, $\beta = \prod_{\pi \in \mathcal{P}(R)} \pi^{k(\pi)}$, such that $\beta g \in R[X]$ and $c(\beta g) = 1$.

  Proof. Denote βg by $\tilde{g}$. Then the claim is that $\tilde{g} \in R[X]$ has content 1. Thus,

  $$\frac{\tilde{g}}{\ell(\tilde{g})} = g$$

  □
- Claim 2: $g \mapsto \tilde{g}$ is a monic polynomial in $K[X]$. Then $\tilde{g} \in R[X]$ with content 1 and

  $$\widetilde{gh} = \tilde{g} \cdot \tilde{h}$$

  Proof. Use the Gauss lemma. □
- Statement (*) holds as a result.
- $\mathcal{P}(R[X]) = \mathcal{P}(R) \sqcup \{\tilde{g} : g \in K[X] \text{ is monic and irreducible}\}$.
- Claim 3: (*) holds for $\mathcal{P}(R[X])$.

  Proof. Scratch: Let $f \in R[X]$ be nonzero. Then $f/\ell(f) \in K[X]$ for each g_i monic and irreducible. $\widetilde{\frac{f}{\ell(f)}} = \tilde{g}_1^{k_1} \cdots \tilde{g}_r^{k_r}$. We have $f, \tilde{g}_1^{k_1} \cdots \tilde{g}_r^{k_r} \in R[X]$. $f = \beta(\tilde{g}_1^{k_1} \cdots \tilde{g}_r^{k_r})$. $\beta \in R$. □
- Two remaining lectures on rings: Factoring polynomials in $\mathbb{Z}[X]$ and $\mathbb{R}[X]$.

5.2 Office Hours (Nori)

- Problem 4.1?
  - See picture.
- Lecture 2.2: "We need bijectivity because continuous functions don't necessarily have continuous inverses?"
  - We can use "$f : R_1 \to R_2$ is a ring homomorphism plus bijection" as the definition of isomorphism.
  - An equivalent definition is, "there exists a ring homomorphism $g : R_2 \to R_1$ such that $g \circ f = \mathrm{id}_{R_1}$ and $f \circ g = \mathrm{id}_{R_2}$."
  - Even though the first is simpler, the reason people use the second is because in some contexts, there *is* a difference between the definitions (such as with homeomorphisms, whose inverses need to be continuous [think proper]).
- Lecture 2.2: We have only defined the finite sum of ideals, not an infinite sum, right?
  - We defined an infinite sum, too.
  - In particular, $\sum_{i \in I} M_i = \bigcup_{F \subset IF \text{ is finite}}$.

  - Note that in a more general sense, you can have infinitely generated ideals. For example, infinite polynomials.

- Lecture 2.2: $IJ = I \cap J$ conditions.
  - $IJ \subset I \cap J$ in commutative rings.
  - Counterexample: $R = \mathbb{Z}$ and $I = (d)$ and $J = (d)$. Then $IJ = (d^2) \neq (d) = I \cap J$.
  - Equality is meaningful.

- To what extent are we covering Chapter 9, and to what extent will reading it help my understanding of the course content?
  - Just the result that $F[X]$ is a PID (implies UFD).
  - All we need from Chapter 8 for the midterm is ED implies PID, all we need from Chapter 9 for the midterm is PID implies UFD.
  - Main examples of PIDs are $\mathbb{Z}$, $F[X]$, and $F[[X]]$.

- Have we done anything outside Chapters 7-9, or if I understand them, am I good to go?
  - The Euclidean algorithm for monic polynomials may not be in Chapter 8.

- Lecture 3.1: Everything from creating $\mathbb{C}$ from $\mathbb{R}$, down.
  - We use monic polynomials just so that we can apply the Euclidean algorithm (EA).
  - We want to find ring homomorphisms $\varphi : R[X] \to A$ such that $\varphi(X^2 + 1) = 0$. How do I get hold of a φ and an A? There's exactly one way to do it. We use the universal property of a polynomial ring.
  - We want $X^2 + 1 \in \ker \psi$, so we define $R[X]/(X^2 + 1)$.
  - $R[X]/(X^2+1)$ generalizes the construction of the complex numbers. Creating a new ring in which $X^2 + 1 = 0$ has a solution.
  - Suppose R is a ring such that $f(X) \in R[X]$ doesn't have a solution. Then it does have a solution in $R[X]/(f(X))$.
  - We recover $\mathbb{C}$ as a special case of this more general construction, specifically the case where $f(X) = X^2 + 1$.

- Lecture 3.2: Do I have it right that the only nontrivial ideals of $\mathbb{Q}$ are the dyadic numbers, $\mathbb{Z}_{(2)}$, and (2^n)? Why is this? What about the triadics, for instance?
  - In $\mathbb{Z}_{(2)}$, the only ideals are of the form (2^n) for some n.

- Lecture 3.2: What is the significance of the final theorem?
  - That all rings with the D-to-units property bear a certain similarity to the ring of fractions.

- Section 7.5: Difference between the rational functions and the field of rational functions?

- Lecture 4.1: What all is going on with $F[[X^{1/2^n}]]$?
  - The idea is the irreducible elements of one ring can become reducible in the context of other rings. This is just a specific example; note how X is the only irreducible element in the first ring, but it reduces to $X = (X^{1/2})^2$ in the next ring, and so on.

- Lecture 4.3: Speech for PIDs over UFDs?

- Lecture 4.3: $R - \{0\}$ or R is an integral domain.
  - Takeaway: You don't need to factor a, b to get their gcd; indeed, you can just find a single generator of (a, b).

- Lecture 4.3: Products of commutative diagrams?
- Lecture 5.1: What is the weakest definition for an ED?
  - The *book* teaches the weakest one.
  - *We're* only interested in Euclidean domains with positive norms.
- Lecture 5.1: Uniqueness condition in the Euclidean algorithm.
- Lecture 5.1: The thing about $\mathbb{Z}$ and $F[[X]]$.
  - These are the only rings we've talked about that are PIDs. Gaussian integers are, too, but we haven't proved that yet.
- Lecture 5.1: Argument for something — is this part of the proof of the converse statement?
- Lecture 5.1: Correct notation?
- What is the set $\mathbb{Z}[X,Y,Z,W]_{XW-YZ}$ in Q4.6b?
  - Like R_f.
- What is the purpose of the commutative diagram in Q4.7?
- Where does d come into play in Q4.10?
  - We're gonna prove that the cardinality of the set is less than or equal to d. About the number of roots of a polynomial of a certain degree, like how $X^3 + \cdots$ can't have more then 3 roots. The most relevant property is that $\mathbb{R}$ is an integral domain.

5.3 Factorization Techniques

2/1:
- Notes on HW4 Q4.1.
  - A lot of people have asked questions about this.
  - The point is to get used to universal properties.
  - Universal properties are important because...
    - They will come up time and time again;
    - They will be especially important if/when we get to tensor products;
    - Two objects that satisfy the same universal property are isomorphic.
- We've introduced a lot of theory at this point, but everything is getting used more and more.
- Today: Factoring polynomials. We will look at two methods to do so.
- Assumption for this lecture: Let $f = a_0X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$ have $c(f) = 1$.
- Factorization prep.
  - Today's ring of interest: $\mathbb{Z}[X]$.
  - We want to test reducibility. Recall from Lecture 5.1 that...
    - If $\deg(f) > 0$, then f is irreducible in $\mathbb{Z}[X]$ iff $c(f) = 1$ and f is irreducible in $\mathbb{Q}[X]$.
    - Why we need the latter condition even though I don't think it was mentioned last lecture (motivation via examples).
      - ➢ Consider $X^2 - 1/4 \in \mathbb{Q}[X]$. This polynomial reduces to $(X - 1/2)(X + 1/2)$. Thus, taking $n = 4$, $4X^2 - 1$ is still reducible in $\mathbb{Z}[X]$ as it equals $(2X - 1)(2X + 1)$.

➢ Consider $X^2 - 1/3 \in \mathbb{Q}[X]$. This polynomial reduces to $(X - 1/\sqrt{3})(1 + 1/\sqrt{3})$ in $\mathbb{R}[X]$, but is irreducible in $\mathbb{Q}[X]$. Thus, taking $n = 3$, $3X^2 - 1$ is still irreducible in $\mathbb{Z}[X]$.

➢ This is the logic underlying Proposition 9.5.

■ If $\deg(f) = 0$, then f is irreducible in $\mathbb{Z}[X]$ iff f is a prime integer.

– Recall that $\ell(f)$ denotes the leading coefficient.

– If f is irreducible in $\mathbb{Q}[X]$, then so is $f/\ell(f)$, but now $f/\ell(f)$ is monic.

– Consider $f \mapsto f/\ell(f)$. It sends

$$\{f \in \mathbb{Z}[X] : f \text{ is irreducible and } \deg(f) > 0\} \to \{\text{monic irreducible polynomials in } \mathbb{Q}[X]\}$$

– The above is not a bijection as is, but if we treat $\pm f$ as the same, then it is. In other words,

$$\pm\backslash\{f \in \mathbb{Z}[X] : f \text{ is irreducible and } \deg(f) > 0\} \cong \{\text{monic irreducible polynomials in } \mathbb{Q}[X]\}$$

where the isomorphism is defined as above.

- Factorization by monomials.

– How many $g(X) = aX + b$ are there in $\mathbb{Z}[X]$ that divide f?

– If $aX + b \mid f$, then $a \mid a_0$ and $b \mid a_n$.

– We know that $a_0 > 0$ by the definition of the X^n term as the leading term. It may be either way with a_n.

■ For the sake of continuing, we will assume that $a_n \neq 0$. Why?? Perhaps because then we would have $b = 0$ in one monomial and 0 doesn't divide anything?

■ We also assume that $\gcd(a, b) = 1$.

– Because of the above constraint, we know that

$$\{g \in \mathbb{Z}[X] : \deg g = 1,\ g \mid f\} \subset \text{known finite set}$$

where the latter set consists of all monomials g with $a \mid a_0$ and $b \mid a_n$.

– $aX + b \mid f$ in $\mathbb{Z}[X]$ iff $aX + b \mid f$ in $\mathbb{Q}[X]$ iff $f(-b/a) = 0$.

– Note: If $\deg(f) \leq 3$ and f is reducible, then there exists $g \in \mathbb{Z}[X]$ such that $\deg(g) = 1$ and $g \mid f$.

■ Let $f = gh$. We know that $3 \geq \deg(f) = \deg(g) + \deg(h)$. Since $c(f) = 1$ by hypothesis, $\deg(g) \neq 0 \neq \deg(h)$. Thus, $1 \leq \deg(g) \leq 3 - \deg(h) \leq 2$ and a similar statement holds for $\deg(h)$. If $\deg(g) = 1$, then we are done. If $\deg(g) = 2$, then $\deg(h) = 1$, and we are done.

■ When we get to $\deg(f) = 4$, the above argument obviously won't work (it would be perfectly acceptable to have $\deg(g) = \deg(h) = 2$ here, for instance).

- We now move on to actual factorization techniques.

- Method 1: **Kronecker's method**.

– This method should be covered in the book somewhere.

- Let f have the same n-degree form as above.

- Let $1 \leq d \leq n$. Does there exist $g \in \mathbb{Z}[X]$ with $c(g) = 1$ and $\deg(g) = d$ such that $g \mid f$?

- Select $d + 1$ distinct integers $c_0, \ldots, c_d$.

- Easy lemma: Let $c_0, \ldots, c_d \in F$ be distinct, and let

$$P_d = \{g \in F[X] : \deg(g) \leq d\}$$

be a a $(d + 1)$-dimensional vector space. Then $T : P_d \to F^{d+1}$ given by

$$T(g) = (g(c_0), \ldots, g(c_d))$$

is an isomorphism of F-vector spaces.

Proof. P_d and F^{d+1} both have the same dimension. Thus, to prove bijectivity of this linear transformation, it will suffice to prove injectivity. To do so, we will show that $\ker(T) = \{0\}$. Let $g \in \ker(T)$ be arbitrary. Then

$$T(g) = 0$$
$$(g(c_0), \ldots, g(c_d)) = (0, \ldots, 0)$$

Thus, g has $d+1$ distinct roots $c_0, \ldots, c_d$. It follows that $g \in ((X - c_0) \ldots (X - c_d))$, meaning that $g = 0$ or $\deg(g) \geq d+1$. However, $g \in P_d$ by hypothesis as well, meaning $\deg(g) \leq d$. Therefore, $g = 0$, as desired. □

- There is an alternative proof of this result that doesn't deal with any existence business but just gives you a formula for computing T.
- Corollary: Given $e_0, \ldots, e_d \in F$ arbitrary, there exists a unique $g \in P_d$ such that $g(c_i) = e_i$ $(i = 0, \ldots, d)$.
  - Note that this is less a corollary and more a restatement of the lemma: A "unique" element of the domain speaks to bijectivity.
- If such a g exists, then $f = gh$ for some $h \in \mathbb{Z}[X]$. It follows that it is uniquely determined by its the values $g(c_0), \ldots, g(c_d)$. But $g(c_i) \mid f(c_i)$ for all $i = 0, \ldots, d$. Note that if $f(c_i) = 0$, then $X - c_i \mid f$ in $\mathbb{Z}[X]$.
- Now consider $S_i = \{u_i \in \mathbb{Z} : u_i \mid f(c_i)\}$. Then $S_0 \times \cdots \times S_d \subset \mathbb{Q}^{d+1}$.
- Take $F = \mathbb{Q}$. Then $T : P_d \to \mathbb{Q}^{d+1} \supset S_0 \times \cdots \times S_d$ where T is an isomorphism.
- It follows that $g \in T^{-1}(S_0 \times \cdots \times S_d) \cap \mathbb{Z}[X] \cap \{g : c(g) = 1\}$. Thus, g is an element of a finite set that is somewhat "known."
- Check whether or not $g \mid f$ (use the Euclidean Algorithm for monic polynomials).
- Then $f(X) = (X - c_0) \cdots (X - c_n) + b$
- Method 2.
  - Basic philosophy: Given a monic polynomial over $\mathbb{C}$ and for which you know all of the coefficients, said coefficients yield an upper bound on the value of every root.
- Lemma: Let $f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{C}[X]$ have $a_0 \neq 0$. Define the number

$$C = \max\left\{\left|\frac{a_1}{a_0}\right|, \left|\frac{a_2}{a_0}\right|^{1/2}, \ldots, \left|\frac{a_n}{a_0}\right|^{1/n}\right\}$$

The elements in the max set are the coefficients of $1/\ell(f)$. If $z \in \mathbb{C}$ and $f(z) = 0$, then $|z| \leq 2C$. Moreover,

$$\frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^n} = 1$$

Proof. If $C = 0$, you're done. Thus, we assume that $C \neq 0$.

WLOG, take $a_0 = 1$ so that f is monic (if $a_0 \neq 1$, divide through by a_0). It follows that

$$\begin{aligned} 0 &= 1z^n + a_1 z^{n-1} + \cdots + a_n \\ -z^n &= a_1 z^{n-1} + \cdots + a_n \\ -1 &= a_1 \frac{1}{z} + a_2 \frac{1}{z^2} + \cdots + a_n \frac{1}{z^n} \\ &= \left(\frac{a_1}{C}\right)\left(\frac{C}{z}\right) + \left(\frac{a_2}{C^2}\right)\left(\frac{C}{z}\right)^2 + \cdots + \left(\frac{a_n}{C^n}\right)\left(\frac{C}{z}\right)^n \end{aligned}$$

By the definition of C, we have that

$$|a_r|^{1/r} \leq C$$

Thus, $|a_r| \leq C^r$ and hence $|a_r/C^r| \leq 1$. We now can relate back to the above.

If $|C/z| \leq 1/2$, this contradicts the triangle inequality (why??), so we must have $|C/z| > 1/2$ or $|z/C| < 2$ so $|z| < 2C$.

We now want $g \in \mathbb{Z}[X]$ with $c(g) = 1$, $\deg(g) = d$, and $g \mid f$ in $\mathbb{Z}[X], \mathbb{Q}[X], \mathbb{C}[X]$. We have $g = b_0X^d + b_1X^{d-1} + \cdots + b_d$ ($b_i \in \mathbb{Z}$). Thus, $g/b_0 = (X - z_1)\cdots(X - z_d)$ with $f(z_1) = \cdots = f(z_d) = 0$. Then we have the following by expanding.

$$= X^d - \left(\sum_{i=1}^{d} z_i\right) X^{d-1} + \left(\sum_{1 \leq i \leq j \leq d} z_i z_j\right) X^{d-2} + \cdots$$

The second term is equal to b_1/b_0; the third is b_2/b_0; etc. We thus have an upper bound

$$|b_r/b_0| \leq (2C)^r \binom{d}{r}$$

Note that $\ell(g) \mid \ell(f)$. The search for the coefficients is now limited to a finite space, and we are done. $a_0b_r/b_0 \in \mathbb{Z}$ and we have an upper bound on its absolute value, specifically the following which, at this point, we can turn over the problem to someone with a computer to solve.

$$|a_0b_r/b_0| \leq (2C)^r \binom{d}{r}(a_0)$$

□

- A great technique for reducing polynomials modulo a prime number.
  - Consider $0^2, 1^2, 2^2, 3^2, 4^2 \pmod 5$. This is $\{0, \pm 1\}$. It follows that $m \equiv \pm 2 \pmod 5$. $X^2 - m \in \mathbb{Z}[X]$ is irreducible, but $(X^2 - m) = (X - h)(X + h)$ implies that $X^2 - h^2 \equiv m \pmod 5$.

5.4 Office Hours (Callum)

- Lecture 3.2: Is the final theorem the "Universal Property of the Ring of Fractions?"
- I^e means extending I. If $f : A \to B$ where $I \subset A$, then $I^e = (f(I)) \subset B$ ($f(I)$ is not an ideal in B unless f is surjective). Similarly, the contraction J^c of some $J \subset B$ is $J^c = f^{-1}(J)$ (this is already an ideal).
- I asked misc. questions about the HW4 problems as I went through them.

5.5 Prime Ideals of Complex Polynomials

2/3:

- Last lecture on rings for a while.
- Monday begins modules.
- Today: Applications of the Gauss lemma.
- Questions to answer today.
  1. Prime ideals of $\mathbb{C}[X, Y]$.
  2. Branched coverage.
  3. Relation between topology and algebra.

- Prerequisites for today: The following lemma.
- Lemma: Let R be a UFD and $K = \operatorname{Frac} R$. Then there exists a bijection

$$R^\times \backslash \{f \in R[Y] : \deg_Y(f) > 0,\ c(f) = 1\} \cong K^\times \backslash \{f \in K[Y] : \deg_Y(f) > 0\}$$

  defined by $f \mapsto f$.

  - This bijection sends irreducibles to irreducibles.
  - We should have proven this on Monday.
- Example: $R = \mathbb{C}[X]$ and $K = \mathbb{C}(X)$.
- What are the prime ideals P in $\mathbb{C}[X, Y]$?
  - $\{0\}$.
  - (f) where f is irreducible.
  - Are there any others?
- We presently build up to answering this question.
  - Let $P \in \mathbb{C}[X, Y]$ be a nonzero prime ideal. Pick a nonzero $f \in P$. Let $f = f_1 \cdots f_r$, where each f_i is irreducible.
  - Since P is a prime, it follows that one of the f_i must be an element of P.
  - Additionally, $(f_i) \subset P$. Then assuming that $(f_i) \neq P$, there exists $g_i \in P$ such that $g_i \notin (f_i)$. Repeat the same argument for each f_j.
  - Then we get $(f_j, g_j) \subset P$. f_j, g_j are irreducible and $g \notin (f)$.
  - Case 0: If $f \in R = \mathbb{C}[X]$ and f is irreducible, then $(f) = (X - a)$. Recall that $\mathbb{C}[X, Y]/(X - a) \cong \mathbb{C}[Y]$ (the isomorphism is given by $f(X, Y) = f(a, Y)$). More generally, we have that $\mathbb{C}[X, Y]/P \cong \mathbb{C}[Y]/\phi(P)$ since $P \supsetneq (X - a)$ and hence $\phi(P) \neq 0$.
  - It follows that there exists a $b \in \mathbb{C}$ such that $\phi(P) = (Y - b)$. Thus, $P = (X - a, Y - b)$.
- **Nonzero** (ideal): An ideal I for which there exists a nonzero $f \in I$.
- We now state the theorem.
- Theorem: Every prime ideal of $\mathbb{C}[X, Y]$ is either...

  (i) $\{0\}$.

  (ii) (f) where f is irreducible.

  (iii) $(X - a, Y - b)$ for all $(a, b) \in \mathbb{C}^2$.

  The ideals (iii) are the maximal ideals. We define $\phi : \mathbb{C}[X, Y] \to \mathbb{C}$ by $\phi(f) = f(a, b)$; then $\ker \phi = (X - a, Y - b)$.

  Proof. Rest of the proof: Let $f, g \in P$ be such that $f, g \notin \mathbb{C}[X]$. It follows from the Gauss lemma that f, g are irreducible in $\mathbb{C}(X)[Y]$ and the gcd in $\mathbb{C}(X)[Y]$ is $(f, g) = 1$. It follows that there exist $A, B \in \mathbb{C}(X)[Y]$ such that $1 = Af + By$. Form of A, B: We have

$$A = \alpha_d Y^d + \cdots + \alpha_0$$

  where each $\alpha_i = u_i(X)/v_i(X)$ for $u_i, v_i \in \mathbb{C}[X]$. Similarly, $B = \beta_e Y^e + \cdots + \beta_0$ with a similar condition on the β_i. Let $h = \prod_i v_i \cdot \prod_j \omega_j$. Then h is nonzero and an element of $\mathbb{C}[X]$. It follows that $hA = A'$ and $hB = B'$ are elements of $\mathbb{C}[X, Y]$. It follows that $A'f + B'g = h$ where $A', B' \in \mathbb{C}[X, Y]$. Thus, $h \in (f, g) \subset P$. Thus, $h = \prod_{i=1}^{e}(X - a_i)$ and $X - a \in P$ for some $a \in \mathbb{C}$. And thus we have reduced to case 0. □

- Hilbert null statement The only maximum ideals of $\mathbb{C}[X_1, \ldots, X_n]$ are $(X_1 - a_1, \ldots, X_n - a_n)$ where $(a_1, \ldots, a_n) \in \mathbb{C}^n$.
  - This is outside this course.
- Exercise: Continue the proof to show that the collection $\{(a, b) \in \mathbb{C}^2 : f(a, b) = g(a, b) = 0\}$ is finite if both f, g are distinct and irreducible in the usual sense, i.e., $(f) \neq (g)$.
- The set

$$\{(a, b) \in \mathbb{C}^2 : (f \cdot g)(a, b) = 0\} = \{(a, b) \in \mathbb{C}^2 : f(a, b) = 0\} \cup \{(a, b) \in \mathbb{C}^2 : g(a, b) = 0\}$$

  minus a finite set is disconnected. *picture; draw diagram of Cartesian plane with missing origin!!*
- Example: Let $f = X$ and $g = Y$. Then $\{(a, b) \in \mathbb{C}^2 : ab = 0\}$ is the X, Y axes and it is disconnected if we remove a finite set of points (e.g., 0). Same in more general, curvy spaces.
- Consider one irreducible polynomial $f(X, Y) = a_0(X)Y^d + \cdots + a_d(X)$. where the $a_i \in \mathbb{C}[X]$ and $a_0(X) \neq 0$.
  - Freeze $X = c$.
  - Denote $f(c, Y)$ by $f_c(Y)$.
  - Take the intersection of $X = c$ and the polynomial in Y.
  - There is a finite set of distinct points. How do we know that there are at most d?
  - Now assume f is irreducible and in $\mathbb{C}[X][Y]$. Then f is irreducible in $\mathbb{C}(X)[Y]$.
  - Comparing f_c and $\partial f_c/\partial y = (\partial f/\partial y)_c$. The Y-degree of $\partial f/\partial y$ is $d - 1$. Since f is irreducible,

$$\gcd_{\mathbb{C}(X)[Y]}(f, \partial f/\partial y) = 1$$

  - Same game gives $A', B' \in \mathbb{C}[X, Y]$ and a nonzero $h \in \mathbb{C}[X]$ such that

$$A'(X, Y)f(X, Y) + B'(X, Y)\frac{\partial f}{\partial Y} = h(X)$$

- Now consider $\{c \in \mathbb{C} : a_0(c) \neq 0 \text{ and } h(c) \neq 0\}$.
- What we have shown is that if you omit a finite set of vertical lines, you understand the zeroes pretty well. This is called a **branched covering**.
- Complex analysis takes it from here.
- Theorem: If $f \in \mathbb{C}[X, Y]$ is square-free and not a constant, then $\{(a, b) \in \mathbb{C}^2 : f(a, b) = 0\}$ minus any finite set is connected iff f is irreducible.

5.6 Office Hours (Ray)

- For Q4.5a, do specify nonoverlapping ideals $(n)^e$.
- Q3.10?
  - The actually most important thing is working with the characteristic. We don't need a ton of detail on p, p^2. 1-2 sentences will suffice, just to show that we understand it follows from the additive group structure and Lagrange's theorem. p^2 case: $\mathbb{Z}/p^2 \cong R$. Multiplication is defined modulo p^2.

- The rest is the other case. As an additive group, we have it as a decomposition into the direct sum of two vector spaces $\mathbb{F}_p \langle 1 \rangle \oplus \mathbb{F}_p \langle \theta \rangle$. Now we just need to pin down $\theta^2 = \alpha\theta + \beta$. If $p \neq 2$, then division exists, so $\theta' = \theta - \alpha/2$. Then $\theta'^2 = \gamma \in \mathbb{F}_p$. If you bash it out, then the linear $\alpha/2$ term cancels. We want to say that there's only three different γs. We can change γ by scalars. γ matters up to $(\mathbb{F}_p^\times)^2$. Case 1: $\gamma = 0$. Second case: γ is a square (so pick $\gamma = 1$). Third case: γ is nonzero and not a square. Because any square is the same, there's only one case there. Three cases correspond to $\mathbb{F}_p[X]/X^2$, $(\mathbb{F}_p^\times)^2$, and $\mathbb{F}_{p^2}$. $X^2 - c$ is irreducible in this last case. So take $\mathbb{F}_p[X]/(X^2 - c)$. Irreducible in a PID implies prime implies maximal implies $\mathbb{F}_p[X]/(X^2 - c)$ is a field.
- A small number of people did it a cleaner way: We know we have a map from $\mathbb{F}_p[X] \to R$ by the universal property that sends $X \mapsto \theta$ and $\theta \notin i(\mathbb{F}_p)$. By the FIT, $\mathbb{F}_p[X]/(\ker\phi) \cong R$. For size reasons, $\ker\phi$ must be a quadratic. There are three cases then for a quadratic $X^2 + aX + b$: Irreducible, reducible to a product of two distinct factors, reducible to a square. These are analogous to the other cases in the other method. This is a nicer way of doing it since there's often a feeling in algebra like it's just definition upon definition, but this allows us to use some of the "algebra" we remember from high school!
- Let R be a ring with cardinality p^2 (we know that at least one exists: $\mathbb{Z}/p^2\mathbb{Z}$ under addition and multiplication mod p^2). Let $j : \mathbb{Z} \to R$ be a ring homomorphism. Then $j(0) = 0_R$ and $j(1) = 1_R$. It follows that $j(n) = n_R$. By the pidgeonhole principle, $j(p^2) = j(a)$ for some $a \in [0, p^2 - 1]$. Thus, the only values of $\mathbb{Z}$ we really need to worry about are where $[0, p^2 - 1]$ get sent since everything else is determined by these values. One option would be to send them all to distinct elements.
- As proven last quarter, there are only two abelian groups of cardinality p^2: $\mathbb{Z}/p^2\mathbb{Z}$ and $(\mathbb{Z}/p\mathbb{Z})^2$.

5.7 Chapter 9: Polynomial Rings

From Dummit and Foote (2004).

Section 9.1: Definitions and Basic Properties

2/5:

- Review of the definitions of **polynomial rings**, **formal sums**, **degrees**, **leading terms**, **leading coefficients**, **monic** polynomials, and polynomial **addition** and **multiplication**.
- Restatement of Proposition 7.4.

  Proposition 9.1. Let R be an integral domain and let $p(X), q(X)$ be nonzero elements of $R[X]$. Then

  1. $\deg p(X)q(X) = \deg p(X) + \deg q(X)$;
  2. The units of $R[X]$ are just the units of R;
  3. $R[X]$ is an integral domain.

- Recall that the quotient field of $R[X]$ is the field of rational functions in X with coefficients in R.
- Relating the ideals of R and $R[X]$.

  Proposition 9.2. Let I be an ideal of the ring R, and let $(I) = I[X]$ denote the ideal of $R[X]$ generated by I (the set of polynomials with coefficients in I). Then

  $$R[X]/(I) \cong (R/I)[X]$$

  In particular, if I is a prime ideal of R, then (I) is a prime ideal of $R[X]$.

  Proof. Given. □

- $I \subset R$ maximal $\not\Rightarrow$ $(I) \subset R[X]$ maximal.

- However, $I \subset R$ maximal $\Rightarrow (I, X) \subset R[X]$ maximal.
- Example.
  1. $R = \mathbb{Z}$ and $I = n\mathbb{Z}$.
     - The "reduction homomorphism" is given by reducing the coefficients of polynomials in $\mathbb{Z}[X]$ modulo n.
     - If n is composite, then $\mathbb{Z}[X]/(n\mathbb{Z}) = \mathbb{Z}[X]/n\mathbb{Z}[X]$ is not an integral domain.
     - If p is prime, then $\mathbb{Z}[X]/(p\mathbb{Z})$ is an integral domain — and in fact an ED as well.
     - Additionally, $p\mathbb{Z}[X] \subset \mathbb{Z}[X]$ is a prime ideal.
- We now introduce polynomial rings in several variables.
- **Polynomial ring** (in the variables $X_1, \ldots, X_n$ with coefficients in R): The ring defined inductively as follows. *Denoted by* $\boldsymbol{R[X_1, \ldots, X_n]}$. *Given by*

$$R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n]$$

  - Interpretation: Polynomials in n variables with coefficients in R are just "polynomials in *one* variable but now with coefficients that are themselves *polynomials in* $n-1$ *variables*" (Dummit & Foote, 2004, pp. 296–97).
  - Such a polynomial is a finite sum of nonzero **monomial terms**.
- **Monomial term**: A term of the following form, where $a \in R$ is the **coefficient** of the term and the $d_i \in \mathbb{Z}_{\geq 0}$. *Also known as* **term**. *Given by*

$$aX_1^{d_1} \cdots X_n^{d_n}$$

- **Monomial**: A monic term of the above form. *Given by*

$$X_1^{d_1} \cdots X_n^{d_n}$$

- **Monomial part** (of a term): The part $X_1^{d_1} \cdots X_n^{d_n}$ of a term $aX_1^{d_1} \cdots X_n^{d_n}$.
- **Degree** (in X_i of a term): The exponent d_i.
- **Degree** (of a term): The quantity defined as follows. *Denoted by* $\boldsymbol{d}$. *Given by*

$$d = d_1 + \cdots + d_n$$

- **Multidegree** (of a term): The ordered n-tuple of the following form, where the term corresponds to a nonzero polynomial in n variables. *Given by*

$$(d_1, \ldots, d_n)$$

- **Degree** (of a nonzero polynomial): The largest degree of any of its terms.
- **Homogeneous** (polynomial): A polynomial in which all terms have the same degree. *Also known as* **form**.
- **Homogeneous component** (of f of degree k): The sum of all the monomial terms in f of degree k, where f is a nonzero polynomial in n variables. *Denoted by* $\boldsymbol{f_k}$.
- To define a polynomial ring in an arbitrary number of variables with coefficients in R, we can take the union of all the polynomial rings in a finite number of variables.
  - Dummit and Foote (2004) also discusses another way to define such a ring using homogeneous components.
- Dummit and Foote (2004) gives an example in which all of the terms above are used.
- Each statement in Proposition 9.1 is true for polynomial rings with an arbitrary number of variables.
  - To see this, just induct.

Section 9.2: Polynomial Rings Over Fields I

- Herein, we focus on polynomial rings of the form $F[X]$, where F denotes a field.
- Dummit and Foote (2004) choose a different norm on $F[X]$ than Nori; they choose $N(p) = \deg(p)$ and $N(0) = 0$.
- Polynomial division.

  Theorem 9.3. Let F be a field. The polynomial ring $F[X]$ is a Euclidean Domain. Specifically, if $a(X)$ and $b(X)$ are two polynomials in $F[X]$ with $b(X)$ nonzero, then there are *unique* $q(X), R(X) \in F[X]$ such that
  $$a(X) = q(X)b(X) + r(X)$$
  with $r(X) = 0$ or $\deg r < \deg b$.

  Proof. Given (see Lecture 3.1).

  Differences between the two version: The in-class one does not assume that the coefficients lie in a field, and thus divisors are taken to be monic therein. Otherwise, the arguments are identical. □

- Further relating $F[X]$ to the terms from Chapter 8.

  Corollary 9.4. If F is a field, then $F[X]$ is a PID and a UFD.

  Proof. Follows from Theorem 9.3, Proposition 8.1, and Theorem 8.14. □

- Examples.
  1. $\mathbb{Z}[X]$ is not a PID.
     - Recall $(2, X)$.
  2. $\mathbb{Q}[X]$ is a PID.
     - Here, $(2, X) = (1) = \mathbb{Q}[X]$.
  3. $\mathbb{Z}/p\mathbb{Z}[X]$ is a PID.
     - Takeaway: The quotient of a ring that is *not* a PID *may* be a PID, itself.
     - Example: $(2, X)$ becomes (X) when $p = 2$, and (1) when $p \neq 2$.
  4. $\mathbb{Q}[X, Y]$ is not a PID.
     - $\mathbb{Q}[X, Y] = \mathbb{Q}[X][Y]$, and $\mathbb{Q}[X]$ is not a field.
     - (X, Y) is not principal.
- The quotient and remainder of Theorem 9.3 are independent of field extensions.
  - Suppose $F \subset E$ are both fields. Divide a by q in both $F[X]$ and $E[X]$. Applying the uniqueness condition in $E[X]$, we get that there is only one factorization in $E[X]$, which must be the same as the one in $F[X] \subset E[X]$.
  - It follows that $\gcd(a, b)$ is the same in both $F[X], E[X]$, since the gcd is obtained from the Euclidean Algorithm.

Section 9.3: Polynomial Rings That Are Unique Factorization Domains

- Allowing fractional coefficients makes calculations in $R[X]$ much nicer.
  - We know that $R \subset \operatorname{Frac} R = F$ for any integral domain R.
  - It follows by Theorem 9.3 that $F[X]$ is an ED, hence a PID and a UFD.
  - Thus, it is very nice to perform calculations on $R[X]$ in its containing ring $F[X]$.
  - We spend this section specifying how computations (e.g., factorizations of polynomials) in $F[X]$ can give information about $R[X]$.
- R a UFD is a *necessary* condition for $R[X]$ to be a UFD.
  - Suppose that $R[X]$ is a UFD.
  - Then any $r \in R \subset R[X]$ has a unique factorization in terms of the irreducibles of $R[X]$, specifically those of degree 0 (i.e., in R) since $\deg(r) = 0$. Thus, r has a unique factorization, and R must be a UFD.
- We now build up to proving that R being a UFD is also a *sufficient* condition for $R[X]$ to be a UFD.
  - Sketch: To do so, we'll factor in $F[X]$ and then "clear denominators."
- We begin by comparing the factorization of a polynomial in $F[X]$ to a factorization in $R[X]$.

  Proposition 9.5 (Gauss' Lemma)**.** Let R be a UFD with $\operatorname{Frac} R = F$, and let $p \in R[X]$. If p is reducible in $F[X]$, then p is reducible in $R[X]$. More precisely, if $p = AB$ for some nonconstant polynomials $A, B \in F[X]$, then there are nonzero elements $r, s \in F$ such that $rA = a$ and $sB = b$ both lie in $R[X]$ and $p = ab$ is a factorization in $R[X]$.

  Proof. The coefficients of A, B lie in F. Let d be a common denominator[1] of these coefficients. Then

  $$dp = a'b'$$

  where $a', b' \in R[X]$. If $d \in R^\times$, then the proposition is true with $a = d^{-1}a'$ and $b = b'$. If $d \notin R^\times$, then we continue.

  Since $d \notin R^\times$, we may write $d = p_1 \cdots p_n$ as a product of irreducibles in R. By Proposition 8.12, p_1 irreducible implies p_1 prime. Thus, by Proposition 9.2, $p_1R[X]$ is prime in $R[X]$. Consequently, by Proposition 7.13, $(R/p_1R)[X] \cong R[X]/p_1R[X]$ is an integral domain. Reducing the equation modulo p_1 yields

  $$0 = \overline{a'} \cdot \overline{b'}$$

  Moreover, since $(R/p_1R)[X]$ is an integral domain, at least one of $\overline{a'}, \overline{b'}$ is zero. Suppose that $\overline{a'} = 0$. Then the coefficients of a' are congruent to 0 modulo p_1, i.e., are divisible by p_1 so that $\frac{1}{p_1}a'$ has coefficients in R. Since $p_1 \mid d$ by definition as well, we can divide p_1 from both sides of $dp = a'b'$ to obtain an equation in which every term still has coefficients in R. Iterating the process allows us to cancel out all of the factors of d, leaving an equation $p = ab$ with $a, b \in R[X]$ and a, b being F-multiples of A, B, respectively, as desired. □

- Relation to the Gauss Lemma, as presented in Lecture 5.1.
  - If the gcd of the coefficients of fg is 1, then $fg \in R[X]$. Nori's Gauss Lemma proves that the coefficients of fg being in $R[X]$ imply that the coefficients of both f, g are only divisible by 1, i.e., are in $R[X]$ as well.
  - Essentially, Nori's Gauss lemma skips the whole business with fraction fields and just goes straight from polynomials in $R[X]$ to reducibility in $R[X]$.

[1] We may choose the *greatest* common denominator, but we don't need to in this case.

  - Nori's version probably is better and more powerful.
  - Perhaps it's a bit like Proposition 9.5 rolls Nori's version, Claim 1, and Claim 2 from class all into one statement.

- Example:
  - Let $R = \mathbb{Q}$, $F = \mathbb{Q}$.
  - Consider $p(X) = 2X^2 + 7X + 3 \in \mathbb{Z}[X]$.
  - We know that p is reducible in $\mathbb{Q}[X]$. In particular, we have that
$$p(X) = (X + \tfrac{1}{2})(2X + 6)$$
  - Choose 2 as a common denominator. Then we have
$$2p(X) = (2X + 1)(2X + 6)$$
which is a factorization of $2p$ in $\mathbb{Z}[X]$.
  - The prime factorization of d is just 2. Reducing the coefficients above modulo 2, we get
$$0 = (0X + 1)(0X + 0) = 1 \cdot 0$$
  - Evidently, $2X + 6$ has coefficients which are divisible by 2, so we may take $\frac{1}{2}(2X + 6)$ to get
$$p(X) = (2X + 1)(X + 3)$$

- The only difference between the irreducible elements in $R[X]$ and $F[X]$: That all elements of R become units in the UFD $F[X]$, so (for example) $7X = 7 \cdot X$ in $\mathbb{Z}[X]$, but $7X$ is irreducible in $\mathbb{Q}[X]$.

  Corollary 9.6. Let R be a UFD, left $F = \operatorname{Frac} R$, and let $p \in R[X]$. Suppose that the gcd of the coefficients of p is 1. Then p is irreducible in $R[X]$ iff it is irreducible in $F[X]$. In particular, if p is a monic polynomial that is irreducible in $R[X]$, then p is irreducible in $F[X]$.

  Proof. We prove this claim via double contrapositives.

  Suppose first that p is reducible in $F[X]$. Then by Gauss' Lemma, p is reducible in $R[X]$.

  Now suppose that p is reducible in $R[X]$. Then $p = ab$ for some $a, b \in R[X]$. Moreover, neither a nor b is constant as if (say a) were, then the assumption that the gcd of its coefficients is 1 would imply that $a = 1$, itself, i.e., a is a unit, contradicting the statement that ab is a factorization of p. This same factorization proves that p is reducible in F. □

- We can now prove the result we've been building up toward.

  Theorem 9.7. R is a UFD iff $R[X]$ is a UFD.

  Proof. Given. □

- Extending Theorem 9.7 to multivariable polynomials.

  Corollary 9.8. If R is a UFD, then a polynomial ring in an arbitrary number of variables with coefficients in R is also a UFD.

  Proof. Given. □

- Examples.
  1. $\mathbb{Z}[X]$ and $\mathbb{Z}[X, Y]$ are UFDs.

  - As mentioned earlier, $\mathbb{Z}[X]$ is a UFD that is not a PID.
2. $\mathbb{Q}[X]$, $\mathbb{Q}[X, Y]$, etc. are UFDs.

- "A nonconstant monic polynomial... is irreducible if and only if it cannot be factored as a product of two monic polynomials of smaller degree" (Dummit & Foote, 2004, p. 306).
- Polynomials that are irreducible in $R[X]$ for R an arbitrary *integral domain* are not necessarily irreducible in $(\operatorname{Frac} R)[X]$.
  - Dummit and Foote (2004) justifies this using an example with quadratic integer rings.

Section 9.4: Irreducibility Criteria

- **Irreducibility criterion**: An easy mechanism for determining when some types of polynomials are irreducible.
  - Simplify the typically laborious process of checking for factors.
- **Linear** (factor): A factor of degree 1.
- **Root** (in F of $p \in F[X]$): An $\alpha \in F$ with $p(\alpha) = 0$.
- When is there a linear factor?

  Proposition 9.9. Let F be a field and let $p \in F[X]$. Then p has a factor of degree one iff p has a root in F.

  Proof. Given (related to the example following the in-class proof of the Euclidean algorithm for monic polynomials in Lecture 3.1). □

- Reducibility in polynomials of small degree.

  Proposition 9.10. A polynomial of degree two or three over a field F is reducible iff it has a root in F.

  Proof. Given (see the argument under "Factorization by monomials" in Lecture 5.2). □

- Possible roots of polynomials with integer coefficients.

  Proposition 9.11. Let $p(X) = a_n X^n + \cdots + a_0$ be a polynomial of degree n with integer coefficients. If $r/s \in \mathbb{Q}$ is in lowest terms (i.e., $(r, s) = 1$ or r, s are relatively prime) and r/s is a root of $p(X)$, then r divides the constant term and s divides the leading coefficient of p:

  $$r \mid a_0 \qquad\qquad s \mid a_n$$

  In particular, if p is a monic polynomial with integer coefficients and $p(d) \neq 0$ for all integers d dividing the constant term of p, then p has no roots in $\mathbb{Q}$.

  Proof. Given (also related to the "Factorization by monomials" discussion from Lecture 5.2). □

- Note that Proposition 9.11 generalizes to $R[X]$ for any UFD R.
- Examples.
  1. $X^3 - 3X - 1$ is irreducible in $\mathbb{Z}[X]$.
     - Gauss' Lemma: To prove that it is irreducible in $\mathbb{Z}[X]$, it will suffice to show that it is irreducible in $\mathbb{Q}[X]$.

  - Proposition 9.10: To show that it is irreducible in $\mathbb{Q}[X]$, it will suffice to show that it has no roots in $\mathbb{Q}$.
  - Proposition 9.11: The only possible roots are the integers which divide the constant term 1, i.e., ± 1.
  - Since

$$(1)^3 - 3(1) - 1 = -3 \neq 0 \qquad (-1)^3 - 3(-1) - 1 = 1 \neq 0$$

    we have the desired result.

2. $X^2 - p$ and $X^3 - p$ are irreducible in $\mathbb{Q}[X]$ for any prime p.
   - Use the same strategy as above.
   - This is very related to my $X^2 - 1/4$ and $X^2 - 1/3$ example from Lecture 5.2, since 3 is prime and this implies irreducibility in $\mathbb{Q}[X]$.
3. $X^2 + 1$ is reducible in $\mathbb{Z}/2\mathbb{Z}[X]$.
4. $X^2 + X + 1$ is irreducible in $\mathbb{Z}/2\mathbb{Z}[X]$.
5. $X^3 + X + 1$ is irreducible in $\mathbb{Z}/2\mathbb{Z}[X]$.

- Treating higher degree polynomials.

  Proposition 9.12. Let I be a proper ideal in the integral domain R and let p be a nonconstant monic polynomial in $R[X]$. If the image of p in $(R/I)[X]$ cannot be factored in $(R/I)[X]$ into two polynomials of smaller degree, then p is irreducible in $R[X]$.

  Proof. Given. □

- This technique is not a be-all/end-all: "There are examples of polynomials even in $\mathbb{Z}[X]$ which are irreducible but whose reductions modulo every ideal are reducible (so their irreducibility is not detectable by this technique)" (Dummit & Foote, 2004, p. 309).

- Examples.

  0. $X^4 + 1$ is irreducible in $\mathbb{Z}[X]$ but reducible modulo every prime (see Chapter 14 for a proof of this). $X^4 - 72X^2 + 4$ is irreducible in $\mathbb{Z}[X]$ but is reducible modulo every integer.
  1. Using Proposition 9.12 to treat $X^2 + X + 1$ and $X^3 + X + 1$ again.
  2. The converse to Proposition 9.12 does not hold: $X^2 + 1$ is irreducible in $\mathbb{Z}[X]$ since is is irreducible in $\mathbb{Z}/2\mathbb{Z}[X]$ but it reducible mod 2.
  3. We can reduce modulo ideals in multivariable cases *to an extent*.
     - Some nonunit polynomials can reduce to units modulo certain ideals, creating challenges.

- A special case of reducing modulo an ideal to test for irreducibility.

  Proposition 9.13 (Eisenstein's Criterion)**.** Let P be a prime ideal of the integral domain R, and let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ be a polynomial in $R[X]$ (here, $n \geq 1$). Suppose $a_{n-1}, \ldots, a_0$ are all elements of P and suppose a_0 is not an element of P^2. Then f is irreducible in $R[X]$.

  Proof. Given. □

- This method is in frequent use.
  - Note that it was originally proven by Schönemann, so it is more properly known as the **Eisenstein-Schönemann Criterion**.

- Eisenstein's criterion is most frequently applied to $\mathbb{Z}[X]$, so we state that special case separately.

Corollary 9.14 (Eisenstein's Criterion for $\mathbb{Z}[X]$)**.** Let p be a prime in $\mathbb{Z}$ and let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$, $n \geq 1$. Suppose p divides a_i for all $i \in \{0, 1, \ldots, n-1\}$ but that p^2 does not divide a_0. Then f is irreducible in both $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$.

Proof. Follows from Proposition 9.13 and Corollary 9.6. □

- Example applications of Eisenstein's Criterion.
- There are now efficient algorithms for factoring polynomials over certain fields.
  - Moreover, many of these are now available as computer packages.
- **Berlekamp Algorithm**: An efficient algorithm for factoring polynomials over $\mathbb{F}_p$.
  - Described in detail in the exercises at the end of Section 14.3.

Section 9.5: Polynomial Rings Over Fields II

- Additional results for the one-variable polynomial ring $F[X]$.

Proposition 9.15. The maximal ideals in $F[X]$ are the ideals (f) generated by irreducible polynomials f. In particular, $F[X]/(f)$ is a field iff f is irreducible.

Proof. Apply Propositions 8.10 and 8.7 to the PID $F[X]$. □

Proposition 9.16. Let g be a nonconstant element of $F[X]$, and let $g(X) = f_1(X)^{n_1} \cdots f_k(X)^{n_k}$ be its factorization into irreducibles, where the f_i are distinct. Then we have the following isomorphism of rings.

$$F[X]/(g) \cong F[X]/(f_1^{n_1}) \times \cdots \times F[X]/(f_k^{n_k})$$

Proof. Follows from the Chinese Remainder Theorem. □

Proposition 9.17. If the polynomial f has roots $\alpha_1, \ldots, \alpha_k$ in F (not necessarily distinct), then f has $(x - \alpha_1) \cdots (x - \alpha_k)$ as a factor. In particular, a polynomial of degree n in one variable over a field F has at most n roots in F, even counted with multiplicity.

Proof. First statement: Induct. Second statement: $F[X]$ is a UFD (Corollary 9.4). □

Proposition 9.18. A finite subgroup of the multiplicative group of a field is cyclic. In particular, if F is a finite field, then the multiplicative group $F^\times$ of nonzero elements of F is a cyclic group.

Proof. Given; relies on more group theory than I covered in Honors Algebra I. □

Corollary 9.19. Let p be a prime. The multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ of nonzero residue classes mod p is cyclic.

Proof. This is the multiplicative group of the finite field $\mathbb{Z}/p\mathbb{Z}$, so apply Proposition 9.18. □

Corollary 9.20. Let $n \geq 2$ be an integer with factorization $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ in $\mathbb{Z}$, where $p_1, \ldots, p_r$ are distinct primes. We have the following isomorphisms of multiplicative groups.

1. $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^\times$.
2. $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ is the direct product of a cyclic group of order 2 and a cyclic group of order $2^{\alpha-2}$ for all $\alpha \geq 2$.
3. $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ is a cyclic group of order $p^{\alpha-1}(p-1)$ for all odd primes p.

Proof. Given. □

- Note that Corollary 9.20 gives the group-theoretic structure of the automorphism group of the cyclic group of order n since $\mathrm{Aut}(Z_n) = \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Section 9.6: Polynomials in Several Variables Over a Field and Gröbner Bases

- A potentially useful result.

  Corollary 9.22. Every ideal in the polynomial ring $F[X_1, \ldots, X_n]$ with coefficients from a field F is finitely generated.

- Everything else is unquestionably beyond the scope of this class.

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.
  - We should read Sections 10.1-10.3 of Dummit and Foote (2004) in their entirety, even though Nori may run out of time.
- 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 $v, v_1, v_2 \in M \ldots$

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

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

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

  (4) $1_A v = v$.

- Notes on the definition.
  - We need the last constraint so that multiplication is nontrivial.
  - A **right A-module** puts the scalar on the right. Will we ever consider these??
- Equivalent definition of A-modules: A pair (M, ρ) where $(M, +)$ is an abelian group and $\rho : A \to \text{End}(M)$ the ring homomorphism defined as follows: For all $a \in A$, $\rho(a) : M \to M$ is given by $\rho(a)v = av$ for all $v \in M$ and satisfies the following constraints. *Constraints*
  (1) $\rho(a)$ is a group homomorphism from $M \to M$.
  (2) $\rho(a + b) = \rho(a) + \rho(b)$.
  (3) $\rho(a)\rho(b) = \rho(ab)$.
  (4) $\rho(1_A) = 1_{\text{End}(M)}$
- More on the ring-homomorphism nature of ρ.
  - 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 $a(b_1, \ldots, b_n) = (ab_1, \ldots, ab_n)$.
     - 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

$$T(a_1v_1 + a_2v_2) = a_1T(v_1) + a_2T(v_2)$$

  for all $a_1, a_2 \in A$ and $v_1, v_2 \in M$.

- Question: What are all of the module homomorphisms $T : A \to M$?
  - If $T(1) = v$, then $T(a \cdot 1) = aT(1) = av$ for all $a \in A$. 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 $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, 0, \ldots, 0)$, etc. Then

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

  - Therefore,

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

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

- **Isomorphism** (of A-modules): A bijective module homomorphism $T : M \to N$, where M, N are A-modules.
  - It follows that $T^{-1} : N \to M$ is also a homomorphism.
  - 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 $\mathrm{im}(\phi)$ is a submodule of N.

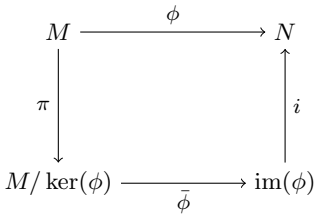

Figure 6.1: First isomorphism theorem of modules.

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

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

  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 $\pi(a_1, \ldots, a_n) = a_n$, 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, $m_i + n_i = 0$ $(i = 1, \ldots, h)$, so $m_i, n_i = 0$ for these i. Additionally, $m_0 + n_0 = 1$, so WLOG let $m_0 = 1$. Then $n_0 = 0$ and b is a unit. Therefore, π is irreducible.
- Lecture 5.2: Why do we assume that $a_n \neq 0$?
- Lecture 5.2: Clarification on the end of Method 1.
  - See Week 5 notes.
  - Key takeaway: You want to get a bound; it doesn't matter if it's the best possible bound, but a bound on the coefficients of a monic polynomial implies a bound on the roots.
- Lecture 5.2: What is going on at the end of Method 2?
- Lecture 5.2: What was the thing about reducing polynomials modulo primes?
- Lecture 6.1: Will we ever consider right A-modules?
  - No — and going forward, ***A*-module** means "left A-module."
- Lecture 6.1: How long have in-class definitions matched those in the book?

  - Practically any book has a different definition of EDs. The book has the weakest definition (i.e., that with the Dedekind-Hasse norm). This definition is basically used nowhere, though.
  - The **class group** is a measure of the failure of unique factorizations. This is an example of something that's actually useful.
  - Rings, ring homomorphisms, etc. But basically stopped in second week.
  - We need the $\phi(1) = 1$ property for instance because otherwise the image of 1 might not act like 1 in the product.
- Lecture 6.1: Axiom of Choice needed to pick an element out of each set?
- Lecture 6.1: What is the direct product a submodule of?
- Lecture 6.1: Is the submodule under the same binary operation as Example?
  - The direct sum is a submodule of the product.

6.3 Office Hours (Ray)

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

6.4 Midterm Review Sheet

2/8:
- Definitions and alternate definitions.
- **Ring**: Abelian group, associative multiplication, distributive laws.
- **Subring**: Closed under addition, multiplication, inverses; contains 1_R.
- **Ring homomorphism**: Respects addition, multiplication, identites.
- **Field**: Commutative, multiplicative inverses for every element save 0_R.
  - A commutative division ring.
  - Commutative, $0_F \neq 1_R$, multiplicative inverses.
- **Polynomial ring**: Union of all formal sums of finite length.

- **Power series ring**: $R^{\mathbb{Z}_{\geq 0}}$ under

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

- **Division ring**: Multiplicative inverses only.
- **Trivial ring**: Multiplication is the zero function.
- **Zero ring**: The ring $R = \{0\}$.
- **Zero divisor**: A nonzero element $a \in R$ to which there corresponds a nonzero element $b \in R$ such that either $ab = 0$ or $ba = 0$.
- **Unit**: An element $u \in R$ to which there corresponds some $v \in R$ such that $uv = 1$.
- **Integral domain**: Commutative, no zero divisors.
  - Commutative, $0_R \neq 1_R$, $a \neq 0$ and $ab = 0$ implies $b = 0$.
  - Commutative, $0_R \neq 1_R$, $a, b \neq 0$ implies $ab \neq 0$.
- **Gaussian integers**: $\mathbb{Z}[i]$.
- **Ideal**: A subset I of a ring R for which $(I, +) \leq (R, +)$ and aI, Ia, or both are subsets of I.
  - Left, right, and two-sided variations.
- **Quotient ring**: The set of all additive cosets.
- **Canonical injection**: ι.
- **Canonical surjection**: i.
- **Isomorphism** (of rings): $f \circ g$ and $g \circ f$ definition formally.
  - Bijectivity isn't always enough.
- **Principal ideal**: An ideal with a single generator.
- **Sum** (of ideals): $\{a + b : a \in I,\ b \in J\}$.
- **Product** (of ideals): $\{a_1 b_1 + \cdots + a_n b_n : n \in \mathbb{N},\ a_1, \ldots, a_n \in I,\ b_1, \ldots, b_n \in J\}$.
- **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).
     - $a = q_0 b + r_0$, $b = q_1 r_0 + r_1$, $r_0 = q_2 r_1 + r_2$, ..., $r_{n-1} = q_{n+1} r_n$.

- 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 $\mathrm{ev}_a : \mathbb{Z}[X] \to \mathbb{R}$ be the ring homomorphism such that $\mathrm{ev}_a = \phi \circ \pi$. (That there is a *unique* ev_a corresponding to ϕ follows directly from the universal property of a quotient, since we have define $\mathrm{ev}_a(f) = 0$.) We know that $\phi(\bar{f}) = 0$ and $\pi(f) = \bar{f}$; thus, $0 = \mathrm{ev}_a(f) = f(a)$. 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: $(f) \neq \ker(\mathrm{ev}_a)$ in general: If $f = 10(X-75)$, for instance, $(10(X-75)) = (f) \neq \ker(\mathrm{ev}_a) = (X - 10)$. 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

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

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 $\psi = \mathrm{ev}_r$. 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 $0 = \mathrm{ev}_r(f) = f(r)$. Thus,

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

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,

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

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 $1 = \mathrm{ev}_0(f) = \tilde{f}(0)$ or $1 = \mathrm{ev}_1(f) = \tilde{f}(1)$ 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 $\mathrm{ev}_i(f) = 1$ $(i = 0, 1)$, then $\phi(X) = \mathrm{ev}_i(X) = i$.

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

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

□

(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, $\phi_0(X) = \mathrm{ev}_0(X) = 0$ and $\phi_1(X) = \mathrm{ev}_1(X) = 1$, 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 $a_1, \ldots, a_d$ 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 $F[X]_f = \text{im}(\phi)$.

Proof.

My write-up: We are given that $\phi(X) = X$; figuring out what $\phi(Y)$ is will fully characterize ϕ (and $\text{im}(\phi)$ 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

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

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 $1/f \in \text{im}(\phi)$. □

[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
  $$\varphi(a_1, \ldots, a_h) = a_h$$
  for all $m = (a_1, \ldots, a_h) \in M$. 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
  $$\{(a_1, \ldots, a_{h-1}, 0) : a_i \in R\} \cong R^{h-1}$$
  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 $A = \mathrm{End}_F(V)$. 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 $\mathrm{End}_A(A^2)$. For a field, it's 2×2 matrices. Here,

      $$\mathrm{End}_A(A^2) \cong M_2(A^{\mathrm{opp}})$$

      where the opp notation denotes that multiplication has been reversed and addition is still the same, i.e.,

      $$a \cdot_{\mathrm{new}} b = b \cdot_{\mathrm{old}} a$$

    - 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 n-space** and notes that it's a vector space of dimension n over F the same way that **Euclidean n-space** is.
3. The **free module of rank 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 n-space** (over F): The vector space defined as follows. *Denoted by* $\boldsymbol{F^n}$. *Given by*
$$F^n = \{(a_1, \ldots, a_n) : a_i \in F \ \forall \ i\}$$
with
$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$
$$\alpha(a_1, \ldots, a_n) = (\alpha a_1, \ldots, \alpha a_n)$$
- **Euclidean n-space**: The vector space defined as follows. *Denoted by* $\boldsymbol{\mathbb{R}^n}$. *Given by*
$$\mathbb{R}^n = \{(a_1, \ldots, a_n) : a_i \in \mathbb{R} \ \forall \ i\}$$
with analogous addition and scalar multiplication to the above.
- **Free module of rank n** (over R): The module defined as follows. *Denoted by* $\boldsymbol{R^n}$. *Given by*
$$R^n = \{(a_1, \ldots, a_n) : a_i \in R \ \forall \ i\}$$
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 $p(X) = a_n X^n + \cdots + a_0 \in F[X]$ on $v \in V$. In particular, we let

$$p(X)v = (a_n T^n + \cdots + a_0)(v) = a_n T^n(v) + \cdots + a_0 v$$

- 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.
- **$\mathbf{Hom}_R(M, N)$**: 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 $\varphi, \psi \in \mathrm{Hom}_R(M, N)$. Define $\varphi + \psi$ by
  $$(\varphi + \psi)(m) = \varphi(m) + \psi(m)$$
  for all $m \in M$. Then $\varphi + \psi \in \mathrm{Hom}_R(M, N)$ and with this operation, $\mathrm{Hom}_R(M, N)$ 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 $r\varphi \in \mathrm{Hom}_R(M, N)$ and with this action of the commutative ring R, the abelian group $\mathrm{Hom}_R(M, N)$ is an R-module.
  3. If $\varphi \in \mathrm{Hom}_R(L, M)$ and $\psi \in \mathrm{Hom}_R(M, N)$, then $\psi \circ \varphi \in \mathrm{Hom}_R(L, N)$.
  4. With addition as above and multiplication defined as function composition, $\mathrm{Hom}_R(M, M)$ is a ring. When R is commutative, $\mathrm{Hom}_R(M, M)$ is an R-algebra.

  Proof. Given. □

- **Endomorphism ring** (of M): The ring defined as follows. *Denoted by* $\mathbf{End_R(M)}$, $\mathbf{End(M)}$. *Given by*
$$\mathrm{End}(M) = (\mathrm{Hom}_R(M, M), +, \circ)$$
- **Endomorphism**: An element of $\mathrm{End}(M)$.
  - When R is commutative, there is a natural map $R \to \mathrm{End}_R(M)$ which sends every $r \in R$ to the endomorphism defined by left multiplication by r.
  - More on $\mathrm{End}(M)$ 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 M generated by 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*

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

  - 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 $\{T^n v : n \geq 0\}$.

- 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.

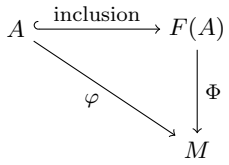

Figure 6.2: Decomposition of a map through a free module.

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

  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* $\boldsymbol{\bigoplus_{i \in I} M_i}$.

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 $v_1, \ldots, v_r \in M$ 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 $v_i \in \mathcal{N}_C$ $(i = 1, \ldots, r)$. Thus, as before, there must exist $N_1, \ldots, N_r \in C$, not necessarily distinct, such that $v_i \in N_i$ $(i = 1, \ldots, r)$. 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, $v_j \in N_j \subset N_i$ $(j = 1, \ldots, r)$. 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. □

- 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. □

- 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 $d_0, d_1, \ldots, d_k$ to denote the dimensions of the vector spaces.
  - $d_0, \ldots, d_k$ 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) $\mathrm{Tor}(M)$ is an R-submodule of M.

  Proof. To prove that $\mathrm{Tor}(M)$ is an R-submodule of M, Proposition 10.1 tells us that it will suffice to show that $\mathrm{Tor}(M) \neq \emptyset$ and that $x + ry \in \mathrm{Tor}(M)$ for all $r \in R$, $x, y \in \mathrm{Tor}(M)$. Consider $0 \in M$. By definition, $r \cdot 0 = 0$. Thus, $0 \in \mathrm{Tor}(M)$ as desired. Additionally, let $r \in R$ and $x, y \in \mathrm{Tor}(M)$ be arbitrary. Since $x, y \in \mathrm{Tor}(M)$, 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 $x + ry \in \mathrm{Tor}(M)$, as desired. □

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

  Proof. To prove that $M/\mathrm{Tor}(M)$ is torsion-free, it will suffice to show that every torsion element of $M/\mathrm{Tor}(M)$ is 0. Let's begin. Let $v \in M/\mathrm{Tor}(M)$ be an arbitrary torsion element. Then there exists $a \in R$ nonzero such that $av = 0$. Now lift $v \in M/\mathrm{Tor}(M)$ to $w \in M$. The constraint $av = 0 = 0 + \mathrm{Tor}(M)$ from the quotient module implies that $0 = a\pi(w) = \pi(aw)$, hence $aw \in \mathrm{Tor}(M)$. 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, $w \in \mathrm{Tor}(M)$, 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) $\mathrm{Tor}(M) \oplus R^h \cong M$ for some $h \geq 0$;
  (ii) $\mathrm{Tor}(M)$ is finitely generated.
- **Rank** (of a module): The number h pertaining to an R-module M, where $M/\mathrm{Tor}(M) \cong R^h$. *Denoted by* $\mathbf{rank}(\boldsymbol{M})$.
  – 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) $\mathrm{Tor}(M_1)$ is isomorphic to $\mathrm{Tor}(M_2)$.

  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 $\mathrm{rank}(M_1) = \mathrm{rank}(M_2)$, then $M_1/\mathrm{Tor}(M_1) \cong M_2/\mathrm{Tor}(M_2)$. This combined with the hypothesis that $\mathrm{Tor}(M_1) \cong \mathrm{Tor}(M_2)$ implies that

$$\begin{aligned} \mathrm{Tor}(M_1) \oplus M_1/\mathrm{Tor}(M_1) &\cong \mathrm{Tor}(M_2) \oplus M_2/\mathrm{Tor}(M_2) \\ M_1 &\cong M_2 \end{aligned}$$

  where the second line follows from the preceding theorem. □
- 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 $M_1, \ldots, M_k$ be submodules of M. Then $T : \prod_{i=1}^k M_i \to M$ defined by

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

     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 $T : \oplus_{(p)} M_{(p)} \to \mathrm{Tor}(M)$ 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 $p_1, \ldots, p_r$ (i.e., the prime ideals $(p_1), \ldots, (p_r)$ are pairwise distinct sets). Let $(m_1, \ldots, m_r) \in \prod_{(p)\in F} M_{(p)}$. Then as per the notation and observations section above, T is defined such that
  $$T(m_1, \ldots, m_r) = m_1 + \cdots + m_r$$
  We first prove that T is injective. Let $(m_1, \ldots, m_r) \in \ker(T)$ be arbitrary. Then $T(m_1, \ldots, m_r) = m_1 + \cdots + m_r = 0$. By hypothesis, there exist $k_1, \ldots, k_r$ such that $p_i^{k_i} m_i = 0$ $(i = 1, \ldots, r)$. 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., $(m_1, \ldots, m_r) = (0, \ldots, 0)$. Therefore, $\ker(T) = 0$, as desired.

  We now prove that T is surjective. Let $m \in \mathrm{Tor}(M)$ 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* **Ann(M)**. *Given by*
  $$\mathrm{Ann}(M) = \{a \in R : am = 0 \ \forall\ m \in M\}$$
- **Annihilator** (of an element): The set of all $a \in R$ such that $am = 0$ pertaining to a specific $m \in M$. *Denoted by* **Ann(m)**. *Given by*
  $$\mathrm{Ann}(m) = \{a \in R : am = 0\}$$
- Consider $l_m : R \to M$ defined by $l_m(a) = am$.
  - By the FIT, there exists a module isomorphism $\overline{l_m} : R/\mathrm{Ann}(m) \to Rm$.

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

- **Cyclic** (module): An R-module M for which there exists $m \in M$ such that $M = Rm$.
  - Cyclic modules are isomorphic to $R/\text{Ann}(m)$ 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) $\text{Ann}(e) = (p^n)$;

  (ii) $p^n M = 0$.

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

  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 $p^k \in \text{Ann}(v)$. 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 $\text{Ann}(v)$ 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 $p^k \in \text{Ann}(v)$, we have that $\text{Ann}(v) = (p^k)$.

  We now begin the bidirectional inclusion argument in earnest. Our strategy is thus: We will construct a lift w' of v, prove that $\text{Ann}(v) \subset \text{Ann}(w')$, and then prove that $\text{Ann}(w') \subset \text{Ann}(v)$. 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, $p^{n-k}\alpha \in \text{Ann}(e)$. It follows since $\text{Ann}(e) = (p^n)$ 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 $p^k \in \text{Ann}(w')$. Since annihilators are ideals, as discussed above, it follows that $\text{Ann}(v) = (p^k) \subset \text{Ann}(w')$.

  To finish the proof, it will just suffice to show that $\text{Ann}(w') \subset \text{Ann}(v)$. Let $a \in \text{Ann}(w')$ 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 $e_1, \ldots, e_s$ 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 $i = 1, \ldots, r$. 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 $\bar{v}_1, \ldots, \bar{v}_r$. But since $\bar{v}_1 = 0$ by the definition of M', we have that M/M' is generated by $\bar{v}_2, \ldots, \bar{v}_r$.

Therefore, by the induction hypothesis, there exist $e_1, \ldots, e_s$ 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 $w_1, \ldots, w_s \in M$ of $e_1, \ldots, e_s$, respectively, such that $\text{Ann}(w_i) = \text{Ann}(e_i)$ for all $i = 1, \ldots, s$.

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 $a, a_1, \ldots, a_s$ be such that $ae + a_1w_1 + \cdots + a_sw_s = 0$. Then we have the equation $a_1e_1 + \cdots + a_se_s = 0$ in M/M'. It follows by the injectivity of T'' that $a_i \in \text{Ann}(e_i)$ for all $i = 1, \ldots, r$. Since $\text{Ann}(e_i) = \text{Ann}(w_i)$ by the above, it follows that $a_iw_i = 0$ $(i = 1, \ldots, s)$. Thus,

$$0 = ae + a_1w_1 + \cdots + a_sw_s = ae + 0 + \cdots + 0 = ae$$

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

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^hR 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 $a_2 \mid a_1$, $a_3 \mid a_2$, …, $a_\ell \mid a_{\ell-1}$.
- 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 $p_1, \ldots, p_\ell$ 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 $r = 1, \ldots, s_i$. It follows by the construction that $a_{r+1} \mid a_r$ $(r = 1, \ldots, s_i - 1)$. Additionally, we have by the Chinese Remainder Theorem that for each $r = 1, \ldots, s_i$,

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

WLOG, let $s_\ell \geq s_i$ $(i = 1, \ldots, \ell)$. 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: $\mathrm{Tor}(M) \cong R/(a_1) \oplus \cdots \oplus R/(a_\ell)$ 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 $j = 1, \ldots, h$.
- 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 $I_{\ell+h+1}, I_{\ell+h+2}, \ldots$ to be equal to R.

□

- 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 $u_1, \ldots, u_\ell \in M$ such that the constraints

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

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

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

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 $T = \{u_1, \ldots, u_h\}$. Then by definition,

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

where the latter isomorphism follows from Proposition 10.5. □

(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 $(a_1, \ldots, a_{h+1}) \in R^{h+1}$ such that

$$a_1 u_1 + \cdots + a_h u_h + a_{h+1} w = 0$$

If $a_{h+1} = 0$, then $(a_1, \ldots, a_h) \neq 0$ makes $a_1 u_1 + \cdots + a_h u_h = 0$, 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. □

- 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. □

- 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) $\mathrm{Tor}(M) \oplus R^h \cong M$ for some $h \geq 0$;

  Proof. To prove that $\mathrm{Tor}(M) \oplus R^h \cong M$, the second theorem from Lecture 6.3 tells us that it will suffice to show that $M/\mathrm{Tor}(M) \cong R^h$ for some $h \geq 0$. By part (ii) of the lemma from last time (Lecture 7.2), we have that $M/\mathrm{Tor}(M)$ is torsion-free. This combined with the fact that $M/\mathrm{Tor}(M)$ 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 $T : \mathrm{Tor}(M) \oplus R^h \to M$ is given by

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

  where $e_1, \ldots, e_h$ generate R^h. □

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

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

- Nori reproves the claim that $M/\mathrm{Tor}(M)$ 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 $\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$ with $\alpha_1, \ldots, \alpha_n \in F$ and $v_1, \ldots, v_n \in S$ 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., $M = \mathrm{Span}(A)$

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* $\mathbf{dim_F} \boldsymbol{V}$, $\mathbf{dim}\, \boldsymbol{V}$.
- **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. □

- 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. □

- 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. □

- 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. □

- **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.
  - $\mathcal{B} = \{v_1, \ldots, v_n\}$ is an (ordered) basis of V, and $\mathcal{E} = \{w_1, \ldots, w_m\}$ is an (ordered) basis of W.
  - $\varphi \in \mathrm{Hom}(V, W)$.
- **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

$$\varphi(v_1) = \frac{\mathrm{d}}{\mathrm{d}t}\left(\mathrm{e}^t\right) = \mathrm{e}^t = v_1 \qquad \varphi(v_2) = \frac{\mathrm{d}}{\mathrm{d}t}\left(\mathrm{e}^{2t}\right) = 2\mathrm{e}^{2t} = 2v_2$$

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. □

- **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* $\mathbf{Tor(R)}$. *Given by*

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

- **A torsion submodule** (of M): Any submodule of $\mathrm{Tor}(M)$.
- **Torsion module**: A module M for which $\mathrm{Tor}(M) = M$.
- **Torsion-free** (module): A module M for which $\mathrm{Tor}(M) = 0$.
- **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* $\mathbf{Ann(N)}$. *Given by*

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

  - If N is not a torsion submodule of M, then $\mathrm{Ann}(N) = 0$.
  - $N \subset L$ submodules of M implies $\mathrm{Ann}(L) \subset \mathrm{Ann}(N)$.
  - R a PID, $N \subset L \subset M$, $\mathrm{Ann}(N) = (a)$, and $\mathrm{Ann}(L) = (b)$ 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 $y_1, \ldots, y_n$ of M such that $a_1 y_1, \ldots, a_m y_m$ is a basis of N where $a_1, \ldots, a_m$ 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 $(a) = \mathrm{Ann}(C)$ 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 $a_1, \ldots, a_m \in R$ 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 $a_1, \ldots, a_m \in R$ 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 $p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$ 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

  $$a = u p_1^{\alpha_1} \cdots p_n^{\alpha_n}$$

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 $r, n_1, n_2, \ldots, n_s$ 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 $m_1, \ldots, m_u$ 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.

Week 8

???

8.1 Linear Algebra Review and Rational Canonical Form

2/20:

- Nori's change of heart.
  - We've all seen linear algebra; thus, we'll speedrun it and then do exterior algebra and determinants. That's where we'll finish.
- The following is part 1 of a linear algebra course.
- Let F be a field.
- **Vector space**: An F-module.
- **Linearly independent** (subset $S \subset V$): Same definition we're familiar with.
- **Spanning** (subset $S \subset V$): A subset S of V that is a set of generators of V.
- S is a **basis** implies that S generates V and is linearly independent.
- Every linearly independent subset of V can be extended to a basis.
- Every spanning set S contains a basis.
  - Any maximal linearly independent subset of S is a basis.
- S_1, S_2 are bases for V implies that $|S_1| = |S_2|$.
  - The replacement theorem in Dummit and Foote (2004) is a good way to prove this.
- We are now done with part 1; this is part 2 of a linear algebra course.
- Let $T : V \to V$ be a linear transformation.
- Let A be a ring. What is an $A[X]$-module M?
  - It is an abelian group $(M, +)$ and a ring homomorphism $\rho : A[X] \to \mathrm{End}(M, +)$.
  - Since $A \hookrightarrow A[X]$, $\rho|_A$ turns M into an A-module.
  - Since $aX = Xa$, $\rho(a)\rho(X) = \rho(X)\rho(a)$.
  - But since we consider M to be a module, we write $a := \rho(a)$: Thus, $a\rho(X)m = \rho(X)am$ for all $m \in M$.
  - Note that $\rho(X) \in \mathrm{End}_A(M)$ (which is the set of all A-module endomorphisms).
  - Additionally, $\rho(X) : M \to M$ is an A-module homomorphism.

- Put $\rho(X) = T$. Thus, an $A[X]$-module is a pair (M, T), where M is an A-module and $T \in \mathrm{End}_A(M)$.
- Conversely, such (M, T) gives rise to an $A[X]$-module with action

$$\left(\sum_{n=0}^{\ell} a_n X^n\right) m = \sum_{n=0}^{\ell} a_n T^n m$$

- Let F be a field, and consider (V, T) where V is any F-vector space and $T : V \to V$ is a linear transformation.
  - This induces a module over $F[X]$.
- V finite dimensional induces $\rho : F[X] \to \mathrm{End}_F(V) \cong M_n(F)$ defined by $X \mapsto T$.

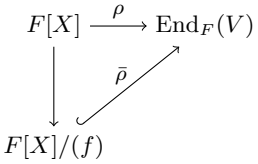

Figure 8.1: $F[X]$-module actions.

  - $\rho(X) = T$ and $\rho(c) = c$ for all $c \in F$.
  - $\ker(\rho) = (f)$ for some monic polynomial f of degree $d \leq n^2$.
  - We have the constraint on the degree of f by the isomorphism from Lecture 3.1.
- **Minimal polynomial** (of T): The polynomial f that generates $\ker(\rho)$.
  - In particular, V is a finitely generated torsion $F[X]$-module.
- **Cyclic vector**: A vector $v \in V$ belonging to (V, T) such that $v, Tv, T^2v, \ldots$ spans V.
- Using cyclic vectors to compute the minimal polynomial.
  - Assume $v, Tv, T^2v, \ldots, T^{k-1}v$ are linearly independent, but $v, Tv, \ldots, T^k v$ are not.
  - Then
$$T^k v = a_0 v + a_1 Tv + \cdots + a_{k-1} T^{k-1} v$$
where all $a_i \in F$ and not all $a_i = 0$.
  - Let $W = \langle v, Tv, \ldots, T^{k-1}v \rangle$. It follows that $T^m k \in W$.
  - Let
$$g(X) = X^k - (a_{k-1}X^{k-1} + \cdots + a_1 X + a_0)$$
Then $g(T)v = 0$. This implies that g is the minimal polynomial of T.
  - It follows that $T^h g(T)v = 0$. Thus, $g(T)T^h v = 0$ for all h.
  - Lastly, it follows that $g(T)w = 0$ for all $w \in W$.
  - Assume v is a cyclic vector. Then $W = V$. It follows that $g(T)v = 0$ for all $v \in V$.
  - The original assumption posits that no polynomial of degree less than or equal to $k - 1$ can annihilate v.
- Consider $V = F[X]/(f)$. Let $\deg(f) = d$, let $T : V \to V$, and let T be the "multiply by X" linear transformation. It follows that if $v_i = \overline{X^{i-1}}$ $(i = 1, \ldots, d)$, then

$$Tv_i = v_{i+1}$$

for $i = 1, \ldots, d-1$ and

$$Tv_d = -(a_0 v_1 + a_1 v_2 + \cdots + a_{d-1} v_d)$$

  - If $d = 3$, then we have
$$M(T) = \begin{pmatrix} 0 & 0 & -a_0 \\ 1 & 0 & -a_1 \\ 0 & 1 & -a_2 \end{pmatrix}$$
  - The above matrix is called the **companion matrix** of f, for f monic of degree 3.

- **Rational canonical form**: The form (V, T) given by
$$F[X]/(f_1) \oplus \cdots \oplus F[X]/(f_s)$$
where $f_2 \mid f_1, \ldots, f_s \mid f_{s-1}$ and $\deg(f_s) > 0$.
  - When $V = 0$, then $s = 0$. In this case, f_1 is the minimal polynomial of T.
  - The form consisting of a block diagonal matrix of companion matrices.

- **Jordan canonical form**:
  - Has to do with p-primary components!

- There's one more canonical form, too.

- Since no one knows what canonical forms are and we very much need them for what Nori was planning to do, Nori will change his plans. No tensors in the last week, either.

- p-primary components: When $p = X - a$, $a \in F$.

- (V, T) is ***p*-primary** if there exists an n such that $(T - a)^n v = 0$ for all $v \in V$.

- $1_V : V \to V$ is the identity.

- $a \cdot 1_V = a_V : V \to V$.

- $(T - a_v)^n = 0 \in \mathrm{End}_F(V)$.

- We're now doing generalized eigenspaces ?? lol.

- The p-primary component is as the generalized a-eigenspace.
  - $(T - a)v = 0$, i.e., $Tv = av$ is the a-eigenspace; the eigenspaces are components of the generalized eigenspaces.

- Let $V = F[X]/(X - a)^n$. Let $v_1 = 1$, $v_2 = \overline{X - a}$, $\ldots$, $v_n = \overline{(X - a)^{n-1}}$.
  - We know that $X(X - a)^r = (X - a + a)(X - a)^r = (X - a)^{r+1} + a(X - a)^r$.
  - Nori writes Jordan blocks as
$$\begin{pmatrix} a & 0 & 0 & 0 \\ 1 & a & 0 & 0 \\ 0 & 1 & a & 0 \\ 0 & 0 & 1 & a \end{pmatrix}$$
not with 1's in the superdiagonal.
    - Thus, the *last* generalized eigenvector is an eigenvector here, instead of the *first*.

8.2 Office Hours (Nori)

- Midterm: We never covered the universal property of a quotient in class, did we?
  - That's the special lemma from last office hours.
- PSet 7: 7.3 and 7.4 typos.
- Wednesday lecture?
  - Seventh week summary will suffice.
- What do you need us to know about the rational canonical form? Should I still read Dummit and Foote (2004), Section 12.2 or is that no longer necessary?
  - Nori will probably push ahead with 12.2. Thus I should read it. He's not sure what he'll do beyond that, though, since he doesn't want to jam tensors into the last week.
  - I will need tensor products for representation theory, regardless, so if I want to take it, I should self-study it.
  - No chance tensor products will be covered next quarter.
  - Serre is a terrific mathematician whose wife is a super chemist, and that's why he wrote his book on representation theory (and wrote it in a less terse manner than usual).
  - No tensors means no exterior algebra, too.
  - Nori hasn't read any of Dummit and Foote (2004).
  - The transfer theory of groups arises in a later chapter, and that's important for representation theory, though.
- Nori doesn't think any teacher pays attention to what courses are supposed to cover as stated in the course catalog.
  - We will never do modules, multilinear and quadratic forms.
  - p-adic field and Galois theory.
  - Nori thinks the proof of Theorem 12.4 is very difficult to follow for a first-timer.
  - Solvable groups were supposed to be a MATH 25700 topic, but got cut because of 9-week quarters.
  - Syclotomic fields have applications to the representation theory of finite groups; there are theorems of representation theory that you need syclotomic fields to prove.
  - Emil Artin: Galois Theory is worth looking up.
  - Gauss and constructions of 17-gons also needs syclotomic fields.

8.3 Office Hours (Nori)

2/21:

- 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.

- Lecture 7.2: Why does $\text{Ann}(v) = (p^k)$, why not just $(p^k) \subset \text{Ann}(v)$? Additionally, how does $p^k w' = 0$ imply that $p^k \in \text{Ann}(w)$?
  - R is a PID!
  - $\text{Ann}(w)$ should be $\text{Ann}(w')$ in the centered line.
  - We don't need to know the theorem from the book for a while (second year of graduate school at least).
  - It's good to know the proofs from class just for going forward in math, but we probably will not be asked to reproduce them on an exam.
- Lecture 7.3: RCF proof?
  - It's not $m_i, 1$, it's $m_{i,1}$!
  - Rewrite the proof when I'm awake enough to understand it.

8.4 Chapter 12: Modules over Principal Ideal Domains

From Dummit and Foote (2004).

Section 12.2: The Rational Canonical Form

2/21:

- As stated previously, we apply the results of Section 12.1 to $F[X]$-modules herein.
- Let V be a finite dimensional vector space over F of dimension N. Let (V, T) be an $F[X]$-module.
- Since V is finite dimensional, it is finitely generated as an F-module and hence also as an $F[X]$-module.
- If V were free, it would be isomorphic to a direct sum of copies of $F[X]$ (by Theorem 12.5(1)) and hence be infinite dimensional.
  - Thus, V is a torsion $F[X]$-module.
  - Theorem 12.5(3): V is isomorphic to the direct sum of cyclic, torsion $F[X]$-modules.
  - This decomposition will allow us to choose a basis for V with respect to which the matrix representation for the linear transformation T is in a specific simple form.
- **Rational canonical form** (of a matrix): The form obtained when we use the invariant factor decomposition of the relevant vector space.
- **Jordan canonical form** (of a matrix): The form obtained when we use the elementary divisor decomposition (and when F contains all the eigenvalues of T).
- Theorem 12.9 ensures that the RCF and JCF are unique, justifying the labeling of them as *canonical*.
- An application of canonical forms: Classifying distinct linear transformations.
  - Two matrices that represent the same linear transformation (hence are similar) have the same RCF and JCF.
  - This is another instance of the structure of the space being acted upon (e.g., the invariant factor decomposition of V) providing information on the algebraic objects (e.g., linear transformations) which are acting.
- **Representation Theory of Groups**: The special case of algebraic objects acting on spaces concerning groups acting on vector spaces.
- **Eigenvalues**, **eigenvectors**, **eigenspaces**, and the **determinant** are defined for linear transformations and analogously for matrices.

- Properties of eigenvalues.

  Proposition 12.12. TFAE.

  1. λ is an eigenvalue of T.
  2. $\lambda I - T$ is a singular linear transformation of V.
  3. $\det(\lambda I - T) = 0$.

  Proof. Given. □

- **Characteristic polynomial** (of a linear transformation): The polynomial defined as follows, where T is the linear transformation in question. *Denoted by* $\boldsymbol{c_T(X)}$. *Given by*

$$c_T(X) = \det(XI - T)$$

  - Defined similarly for matrices A.
  - A monic polynomial of degree $\dim V$.
  - The eigenvalues are the roots.

- **Minimal polynomial** (of of a linear transformation): The unique monic polynomial which generates the ideal $\mathrm{Ann}(V)$ in $F[X]$. *Denoted by* $\boldsymbol{m_T(X)}$.

  - Defined similarly for matrices A.
  - We know that such a polynomial exists by Theorem 12.5(3).
  - Exercise 12.2.5: The degree of the minimal polynomial is at most n^2.

- **Cayley-Hamilton Theorem**: The minimal polynomial for T is a divisor of the characteristic polynomial for T.

  - Thus, the degree of the minimal polynomial is at most n.

- We now build up to the **rational canonical form**.

- Introduction.

  - Theorem 12.5: There exists an isomorphism

$$V \cong F[X]/(a_1(X)) \oplus \cdots \oplus F[X]/(a_m(X)) \tag{12.1}$$

  - The invariant factors a_i are only determined up to units, but since $F[X]^\times = F - \{0\}$, we can make the a_i unique by requiring them to be monic.
  - Theorem 12.5(3) asserts that $(a_m(X)) = \mathrm{Ann}(V)$.

- The minimal polynomial and the invariant factors.

  Proposition 12.13. The minimal polynomial $m_T(X)$ is the largest invariant factor of V. All of the invariant factors of V divide $m_T(X)$.

- We now build up to calculating the minimal polynomial of T and the other invariant factors.

- Choosing a basis for each of the summands in Equation 12.1.

  - Recall that the action of T on V is equivalent to the action of X on each summand.
  - Recall also (from the Example following Proposition 11.1) that $1, \bar{X}, \bar{X}^2, \ldots, \bar{X}^{k-1}$ gives a basis of $F[X]/(a(X))$, where $a(X) = X^k + b_{k-1}X^{k-1} + \cdots + b_0$.

- With respect to this basis, the linear transformation $T = l_X$ acts via

$$\begin{aligned} 1 &\mapsto \bar{X} \\ \bar{X} &\mapsto \bar{X}^2 \\ \bar{X}^2 &\mapsto \bar{X}^3 \\ &\vdots \\ \bar{X}^{k-2} &\mapsto \bar{X}^{k-1} \\ \bar{X}^{k-1} &\mapsto \bar{X}^k = -b_0 - b_1\bar{X} - \cdots - b_{k-1}\bar{X}^{k-1} \end{aligned}$$

  - The last equality holds since $a(\bar{X}) = 0$ in $F[X]/(a(X))$.
- With respect to this basis, the matrix for multiplication by X is called the **companion matrix** of $a(X)$.
- Applying this procedure to each of the cyclic modules on the right side of Equation 12.1 under an appropriate basis yields the **direct sum** of the companion matrices for the invariant factors as the matrix of T.
- Note that this matrix is uniquely determined by the invariant factors of the $F[X]$-module V. These invariant factors, in turn, uniquely determine V up to isomorphism by Theorem 12.9.

- **First subdiagonal**: The set of entries in a matrix which lie directly below a diagonal entry. *Also known as* **subdiagonal**.
- **Companion matrix** (of a polynomial): The $k \times k$ matrix, pertaining to the polynomial $a(X) = X^k + b_{k-1}X^{k-1} + \cdots + b_0$, which consists of 1's down the first subdiagonal, $-b_0, \ldots, -b_{k-1}$ down the last column, and zeros elsewhere. *Denoted by* $\boldsymbol{\mathcal{C}_{a(X)}}$. *Given by*

$$\mathcal{C}_{a(X)} = \begin{pmatrix} 0 & 0 & \cdots & \cdots & \cdots & -b_0 \\ 1 & 0 & \cdots & \cdots & \cdots & -b_1 \\ 0 & 1 & \cdots & \cdots & \cdots & -b_2 \\ 0 & 0 & \ddots & & & \vdots \\ \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & \cdots & 1 & -b_{k-1} \end{pmatrix}$$

- **Direct sum** (of matrices): The block diagonal matrix consisting of the component matrices.
  - See the RCF example below.
- **Rational canonical form** (of a matrix): A matrix that is the direct sum of companion matrices for monic polynomials $a_1(X), \ldots, a_M(X)$ of degree at least one with $a_1(X) \mid a_2(X) \mid \cdots \mid a_m(X)$. *Also known as* **RCF**. *Given by*

$$\begin{pmatrix} \mathcal{C}_{a_1(X)} & & & \\ & \mathcal{C}_{a_2(X)} & & \\ & & \ddots & \\ & & & \mathcal{C}_{a_m(X)} \end{pmatrix}$$

- **Invariant factors** (of the RCF): The polynomials a_i in the above definition.
- Definition of a **block diagonal** matrix.
- **Rational canonical form** (of a linear transformation): The matrix representing T which is in rational canonical form.
- Dummit and Foote (2004) proves that the rational canonical form is unique by means of running the generation process in reverse.

Theorem 12.14 (Rational Canonical Form for Linear Transformations)**.** Let V be a finite dimensional vector space over the field F, and let T be a linear transformation of V.

1. There is a basis for V with respect to which the matrix for T is in rational canonical form, i.e., is a block diagonal matrix whose diagonal blocks are the companion matrices for monic polynomials $a_1(X), \ldots, a_m(X)$ of degree at least one with $a_1(X) \mid a_2(X) \mid \cdots \mid a_m(X)$.
2. The rational canonical from for T is unique.

- Why the *rational* canonical form?
  - "Rational" refers to the fact that this canonical form is calculated entirely within the field F and exists for any linear transformation T.
  - This is not the case for the JCF, which only exists if the field F contains the eigenvalues for T.
- Similar matrices, modules, and the RCF.

Theorem 12.15. Let S and T be linear transformations of V. Then TFAE.

1. S and T are similar linear transformations.
2. The $F[X]$-modules obtained from V via S and via T are isomorphic $F[X]$-modules.
3. S and T have the same rational canonical form.

Proof. Given. □

- Observation: Any $n \times n$ matrix A with entries in F arises as the matrix for some linear transformation T of an n-dimensional vector space.
- This observation allows us to restate Theorems 12.14-12.15 in the language of matrices.

Theorem 12.16 (Rational Canonical Form for Matrices)**.** Let A be an $n \times n$ matrix over the field F.

1. The matrix A is similar to a matrix in rational canonical form, i.e., there is an invertible $n \times n$ matrix P over F such that $P^{-1}AP$ is a block diagonal matrix whose diagonal blocks are the companion matrices for monic polynomials $a_1(X), \ldots, a_m(X)$ of degree at least one with $a_1(X) \mid a_2(X) \mid \cdots \mid a_m(X)$.
2. The rational canonical from for A is unique.

Theorem 12.17. Let A, B be $n \times n$ matrices over the field F. Then A, B are similar iff A, B have the same RCF.

- **Invariant factors** (of a matrix): The invariant factors of the matrix's RCF.
- RCF and similarity questions for A do not depend on which field contains the entries of A.

Corollary 12.18. Let A, B be two $n \times n$ matrices over a field F, and suppose F is a subfield of the field K.

1. The rational canonical form of A is the same whether it is computed over K or over F. The minimal and characteristic polynomials and the invariant factors of A are the same whether A is considered as a matrix over F or as a matrix over K.
2. The matrices A, B are similar over K iff they are similar over F, i.e., there exists an invertible $n \times n$ matrix P with entries from K such that $B = P^{-1}AP$ iff there exists an (in general different) invertible $n \times n$ matrix Q with entries from F such that $B = Q^{-1}AQ$.

Proof. Given. □

- Takeaways from Corollary 12.18.
  - The RCF for A is an $n \times n$ matrix with entries in the smallest field containing the entries of A.
  - Further explanation of the word *rational*: The RCF is the same matrix even if we allow conjugation of A by nonsingular matrices whose entries come from larger fields.
- Characteristic polynomials and invariant factors.

Lemma 12.19. Let $a(X) \in F[X]$ be any monic polynomial.

1. The characteristic polynomial of the companion matrix of $a(X)$ is $a(X)$.
2. If M is the block diagonal matrix

$$M = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_k \end{pmatrix}$$

given by the direct sum of matrices $A_1, \ldots, A_k$, then the characteristic polynomial of M is the product of the characteristic polynomials of $A_1, \ldots, A_k$.

Proof. See the exercises. □

Proposition 12.20. Let A be an $n \times n$ matrix over the field F.

1. The characteristic polynomial of A is the product of all the invariant factors of A.
2. (The Cayley-Hamilton Theorem) The minimal polynomial of A divides the characteristic polynomial of A.
3. The characteristic polynomial of A divides some power of the minimal polynomial of A. In particular, these polynomials have the same roots, not counting multiplicities.

Proof. Given. □

- The relations in Proposition 12.20 are frequently useful in determining the invariant factors of A, particularly for $\deg(A)$ small.
- **Elementary row and column operations**: The following three operations, where A is an $n \times n$ matrix over the field F and $XI - A$ is an $n \times n$ matrix with entries in $F[X]$. *Given by*
  - (i) Interchanging two rows or columns.
  - (ii) Adding a multiple (in $F[X]$) of one row or column to another.
  - (iii) Multiplying any row or column by a unit in $F[X]$, i.e., by a nonzero element in F.
- **Smith Normal Form** (of a matrix): The following form of the $n \times n$ matrix $XI - A$ with entries from $F[X]$, where $a_1, \ldots, a_m$ are the invariant factors of A. *Given by*

$$\begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & a_1(X) & & & & \\ & & & & a_2(X) & & & \\ & & & & & \ddots & & \\ & & & & & & a_m(X) & \end{pmatrix}$$

- Computing the invariant factors in general.

  Theorem 12.21. Let A be an $n \times n$ matrix over the field F. Using the three elementary row and column operations above, the $n \times n$ matrix $XI - A$ is with entries in $F[X]$ can be put into Smith Normal Form.

- Dummit and Foote (2004) provides algorithms for computing the invariant factor decomposition and the RCF. Return to later.

Exercises

5. Prove directly from the fact that the collection of all linear transformations of an n-dimensional vector space V over F to itself form a vector space over F of dimension n^2 that the minimal polynomial of a linear transformation T has degree at most n^2.

References

Dummit, D. S., & Foote, R. M. (2004). *Abstract algebra* (third). John Wiley and Sons.

Ikenaga, B. (2018). *The universal property of the quotient*. https://sites.millersville.edu/bikenaga/abstract-algebra-1/universal-property-of-the-quotient/universal-property-of-the-quotient.pdf

Labalme, S. (2021). *Linear Algebra Done Right notes*. Retrieved February 20, 2023, from https://github.com/shadypuck/LADRNotes/blob/master/main.pdf