MATH 25800 (Honors Basic Algebra II) Notes

Steven Labalme

February 6, 2023

Weeks

List of Figures

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.,
  $$a\times(b+c)=(a\times b)+(a\times c)\qquad\qquad (b+c)\times a=(b\times a)+(c\times a)$$
  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,
  $$l_a(b)=a\times b\qquad\qquad r_a(b)=b\times a$$
  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* $\mathbf{0}_{\boldsymbol{R}}$.
  $$0_R+a=a+0_R=a$$
  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
  $$\begin{aligned}l_a(0_R)&=0_R & l_a(-b)&=-l_a(b)\\ a\times 0_R&=0_R & a\times(-b)&=-(a\times b)\end{aligned}$$
  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 $\text{Fun}(X; \mathbb{R})$ 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 $\text{Fun}(X; R) = R^X$ 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 $\{a/p^n \mid a \in \mathbb{Z}, n = 0, 1, \dots\}$, $\{a/(p_1 p_2 \cdots p_r)^n \mid a \in \mathbb{Z}, n = 0, 1, \dots\}$, 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 $C = \{c \in R \mid cx = xc\}$, 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:
    $$\{a_R + b_R x \mid a, b \in \mathbb{Z}\} \subset M$$
  - Multiplicative closure: $x \cdot x = x^2 \in M$. Moreover, defining x^n in the usual way (i.e., inductively),
    $$x^n \in M$$
    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 $a_0, a_1, \dots, a_n \in \mathbb{Z}$ 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*

$$\mathbb{Z}[X] = \bigcup_{m=0}^{\infty} \{a_0 + a_1X + \cdots + a_mX^m \mid a_0, a_1, \dots, a_m \in \mathbb{Z}\}$$

  - 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 $f = a_0 + a_1X + \cdots + a_mX^m$, $f(x) = (a_0)_R + (a_1)_Rx + \cdots + (a_m)_Rx^m$, 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

$$ax^m = x^ma \in M$$

    for all $a \in R$, $m \in \mathbb{Z}_{\geq 0}$.
  - Thus,

$$a_0 + \cdots + a_mx^m \in M$$

    for $a_0, \dots, a_m \in R$, $m \in \mathbb{Z}_{\geq 0}$.
  - This set of polynomials is already a subring. Thus, it is not only contained in M, but must also equal M.
  - Difference between this set of polynomials and the ones from Question 1: These are the polynomials with coefficients in $R \supset \mathbb{Z}$.
    - 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*

$$R[X] = \bigcup_{m=0}^{\infty} \{a_0 + a_1X + \cdots + a_mX^m \mid a_0, a_1, \dots, a_m \in R\}$$

  - 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

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

- 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 $\beta(f) = f(x)$.
  - 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. $\square$

- **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., $F^\times = F \setminus \{0\}$.
- 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).

- **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.
- Dummit and Foote (2004) does a deep dive on quadratic integer rings.
- **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

$$a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

  with $n \geq 0$ and each $a_i \in R$.
- **Degree** $\boldsymbol{n}$ (polynomial): A polynomial for which $a_n \neq 0$.
- **Leading term**: The a_nX^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_nX^n, b_mX^m, respectively, then the leading term of $p(X)q(X)$ is $a_nb_mX^{n+m}$, provided $a_nb_m \neq 0$. But since $a_n, b_m \neq 0$ (as leading coefficients) and R has no zero divisors (as an integral domain), we have that $a_nb_m \neq 0$. 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

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

   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 $R[X]$.
- 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, $M_n(R)$ ahs 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 $i, j \in \{1, \dots, n\}$.

  - 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

$$a_1g_1+\cdots+a_ng_n$$

  under componentwise addition

$$(a_1g_1+\cdots+a_ng_n)+(b_1g_1+\cdots+b_ng_n)=(a_1+b_1)g_1+\cdots+(a_n+b_n)g_n$$

  and multiplication defined by the distributive law as well as $(ag_i)(bg_j)=(ab)g_k$ (where $g_k=g_ig_j$) such that the coefficient of g_k in the product $(a_1g_1+\cdots+a_ng_n)\times(b_1g_1+\cdots+b_ng_n)$ is

$$\sum_{g_ig_j=g_k}a_ib_j$$

  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_1g_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 $p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ 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 $g(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0$ be a nonzero polynomial of minimal degree such that $g(x)p(x) = 0$. Show that $b_ma_n = 0$ and so $a_ng(x)$ is a polynomial of degree less than m that also gives 0 when multiplied by $p(x)$. Conclude that $a_ng(x) = 0$. 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 $b_mp(x) = 0$.

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 $\text{ev}_x : \mathbb{Z}[X] \to R$ 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 ($H_1, H_2 \lhd G$ implies $H_1 \cap H_2$ and $H_1 H_2$ 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 $I_1 I_2$ are also two-sided ideals.
- Constructing ideals.
- **Kernel** (of a ring homomorphism): The set defined as follows, where $f : A \to B$ is a ring homomorphism. *Denoted by* $\textbf{ker}(\boldsymbol{f})$. *Given by*

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

- Immediate consequences.

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

  Proof. We will not check associativity, identity, and inverses (but these can all be checked). Do remember that we are working with *addition* as our group operation here, though, so the identity of interest is 0, not 1. We will check closure.

  Let $h \in \ker(f)$ and let $a \in A$. We WTS 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*
$$R/I = \{a + I \mid a \in R\}$$
  - 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 subgroup 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.
$$\pi^{-1}(y_1) \cdot \pi^{-1}(y_2) = \{x_1 \cdot x_2 \mid x_1 \in \pi^{-1}(y_1), x_2 \in \pi^{-1}(y_2)\}$$
  - 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 exists $a_1, a_2 \in R$ 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,

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

  Since c_2, c_1 are part of an ideal, a_1c_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.

$$\subset a_1a_2 + I$$

- Therefore,

$$\pi(\pi^{-1}(\alpha_1)\cdot\pi^{-1}(\alpha_2)) = \{a_1a_2+I\}$$

  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 $a_1a_2 - a_1'a_2' \in I$.
  - 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 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, $n_Rx = xn_R$ 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 $a_pX^pb_qX^q = a_pb_qX^pX^q$ 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 $a_pX^pb_qX^q = a_pb_qX^pX^q$ 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 $\text{ev}_i : \mathbb{R}^{\mathbb{R}} \to \mathbb{R}$ 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, $\text{ev}_i : \mathbb{R}[X] \to \mathbb{R}$ *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,

$$\begin{aligned}(a_1 + I) \cdot (a_2 + I) &= (a_1' + I) \cdot (a_2' + I) \\ a_1a_2 + I &= a_1'a_2' + I\end{aligned}$$

so

$$a_1a_2 - a_1'a_2' \in I$$

    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

$$a_1a_2 - a_1'a_2' = (a_1 - a_1')a_2 + a_1'(a_2 - a_2')$$

       - 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

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi"'] & B \\ A/I \arrow[r, "\bar{f}"'] & f(A) \arrow[u, "i"'] \end{tikzcd}$$

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.
- **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??
- 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*

$$Rb = \{ab \mid a \in R\}$$

  - $(Rb, +)$ 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*

$$I + J = \{a + b \mid a \in I, b \in J\}$$

  - 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

$$\sum_{\lambda \in \Lambda} I_\lambda = \{a_1 + a_2 + \cdots + a_n \mid n \in \mathbb{N}, a_i \in I_{\lambda_i} \text{ for some } \lambda_i \in \Lambda\}$$

  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,

$$AX + AY = \{f(X, Y)X + g(X, Y)Y \mid f, g \in A\}$$

  - 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 (see below).
  - Note that similarly, AX is the set of all functions vanishing on the y-axis.
- Exercise: Prove that $AX + AY$ is not a prime ideal.
- **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 left (resp. right, two-sided) ideal.
- **Product** (of ideals): The ideal defined as follows, where I, J are ideals. *Denoted by* $\boldsymbol{IJ}$. *Given by*

$$IJ = \{a_1 b_1 + a_2 b_2 + a_n b_n \mid n \in \mathbb{N},\ a_1, \dots, a_n \in I,\ b_1, \dots, b_n \in J\}$$

  - Note that $IJ \neq \{ab \mid a \in I, b \in I\}$. 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:

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

    - 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 $f = \text{lcm}(d, e)$.
- 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., $I = F$. $\square$

- 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

$$S = \{n \in \mathbb{Z}_{\geq 0} \mid a_n \neq 0\}$$

  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. □

- Corollary: $R[X][Y] = R[X, Y]$ is an integral domain.
- Corollary: $R[X_1, \dots, X_n]$ 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.

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

- 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* $\textbf{char}(\boldsymbol{R})$.
- 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) $\Rightarrow$ (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) $\Rightarrow$ (2): Not covered in class. □

- R is a field if it satisfies $1 \sim 2$.
- Question: I is an ideal of R. How is $\{$ideals in $R\}$ related to $\{$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.

- 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

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

  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. ☐

- **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 $A+B = \{a+b \mid a \in A, b \in B\}$ 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 $\boldsymbol{A}$**: The smallest (two-sided) ideal of R containing $A \subset R$. *Denoted by* $(\boldsymbol{A})$.
  - 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 $\boldsymbol{A}$**: 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

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

- 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,
     $$(2, X) = \{2p(X) + Xq(X) \mid p(X), q(X) \in \mathbb{Z}[X]\}$$
     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. $M = \{f \mid f(1/2) = 0\} = \ker(\text{ev}_{1/2}) \subset \mathbb{R}^{[0,1]}$ 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 $\{g - 1 \mid g \in G\}$.
     - 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. □

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. $\square$

- 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. $\square$

- 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. $\square$

- 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.
    - "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.

[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 $\mathbb{Z}$.

   - Counterexample: $(X) \subsetneq (2, X) \subsetneq \mathbb{Z}[X]$.
   - Alternate proof: Since $(x) = \ker(\text{ev}_0 : \mathbb{Z}[X] \to \mathbb{Z})$, we know that $\mathbb{Z}[X]/(x) \cong \mathbb{Z}$, which is not a field.
4. $M_a = \ker(\text{ev}_a : \mathbb{R}^{[0,1]} \to \mathbb{R}) \subset \mathbb{R}^{[0,1]}$ is a maximal ideal.
   - Since ev_a is surjective, $\mathbb{R}^{[0,1]}/M_a \cong \mathbb{R}$ a field.
   - Similarly, $\ker(\text{ev}_a : C([0,1], R) \to \mathbb{R}) \subset C([0,1], R)$ 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. $\square$

- 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. $\square$

- 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. $\square$

- 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,
    $$\begin{aligned} h(a) &= q(a)(a - a) + r \\ r &= h(a) \end{aligned}$$
    implying that
    $$h(X) - h(a) = q(X)(X - a)$$
    for arbitrary polynomials h.
- Corollary: Let $a \in R$. $\{h \in R[X] \mid h(a) = 0\}$ is the **principal ideal generated by $\boldsymbol{X - a}$**.
- **Ideal generated by $\boldsymbol{b \in B}$**. *Denoted by* $\boldsymbol{Bb}$, $\boldsymbol{(b)}$.
- Corollary: Let $f \in R[X]$ be monic of degree d. Then
  $$\{g \in R[X] \mid \deg(g) < d\} \hookrightarrow R[X] \twoheadrightarrow R[X]/(f)$$
  and, in particular,
  $$\{g \in R[X] \mid \deg(g) < d\} \cong R[X]/(f)$$
  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 $\varphi(h) = 0 = 0 + (f) = (f)$. 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. $\square$

- $R[X]$ is also a vector space with $1, X, X^2, \dots$ as the basis.
- We have that
$$\{g \in R[X] \mid \deg(g) < d\} = \{a_0 + \cdots + a_{d-1}X^{d-1} \mid a_0, \dots, a_{d-1} \in R\}$$
  - As an abelian group (ignoring multiplication), this set is group isomorphic to $(R^d, +)$.
- 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 $f(\bar{X}) = 0$.
- 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, $\mathbb{Z}[X]/(2) \cong \mathbb{Z}/2\mathbb{Z}[X]$.
     - What is $\bar{X}$ in this set?? It must be some integer??
  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
$$\{a/2^n \mid a \in 3\mathbb{Z}\}$$
which is the diadic rationals with numerator equal to a multiple of 3.
     - This construction will be integral to Spring Quarter.
- Question/exercise: Let $\alpha \in R$. Then $R[X]/R[X]\alpha \cong (R/R\alpha)[X]$.
- 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
$$d = \min\{\deg(g) \mid g \in I,\ g \neq 0\}$$
  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, $h \in (f)$. $\square$

- 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 $(\mathbb{Z} \times \mathbb{Z}) \setminus \{(a, 0) \mid a \in \mathbb{Z}\}$. In particular, we let $\mathbb{Q}$ be the set of equivalence classes in $\mathbb{Z} \times \mathbb{Z}$ under the equivalence relation
$$\frac{a}{b} = \frac{c}{d} \quad \Longleftrightarrow \quad ad - bc = 0$$
    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 closed under multiplication (that is, $b, d \in D$ implies $bd \in D$).
    - 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**.
- $\sim$: The equivalence relation on a product ring $(A \times B, +, \cdot)$ defined as follows. *Given by*
$$(a_1, b_1) \sim (a_2, b_2) \quad \Longleftrightarrow \quad a_1 \cdot b_2 - a_2 \cdot b_1 = 0$$
- 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. *Denoted by* $\boldsymbol{D^{-1}R}$. *Given by*

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

  1. Addition:
$$\frac{x_1}{t_1} + \frac{x_2}{t_2} = \frac{x_1t_2 + x_2t_1}{t_1t_2}$$
     - 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:
$$\frac{x_1}{t_1} \cdot \frac{x_2}{t_2} = \frac{x_1x_2}{t_1t_2}$$
     - 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 $D = R \setminus \{0\}$. *Also known as* **quotient field**. *Denoted by* $\textbf{Frac}\,\boldsymbol{R}$.
  - 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 $R_2 = \{a/b \in \mathbb{Q} \mid b = 2^n\}$. Recall that these are the diadic 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.

- We have a canonical injection $\iota : R \to D^{-1}R$ defined by $x \mapsto x/1$.
- Theorem (universal property of the ring of fractions):

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, hook, "\iota"'] & S \\ D^{-1}R \arrow[ur, "\tilde{\varphi}"'] & \end{tikzcd}$$

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 $D = R \setminus \{0\}$, 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! $\square$

- Theorem 36 in Section 15.4 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. $\square$

- 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. $\text{Frac}(2\mathbb{Z}) = \mathbb{Q}$.
   - Notice how an identity "appears" in the field of fractions.
4. The **rational functions**.
   - $\text{Frac}(R[X])$ contains $\text{Frac}(R)$.
   - $\text{Frac}(R[X]) = \text{Frac}(R)(X)$.
     - Example: We have that

$$\text{Frac}(\mathbb{Z}[X]) = \text{Frac}(\mathbb{Q}[X]) = \mathbb{Q}(X) = \text{Frac}(\mathbb{Z})(X)$$

     - We can easily see this since if $p(X)/q(X) \in \text{Frac}(\mathbb{Q}[X])$, 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 $p(X)/q(X) = Np(X)/Nq(X) \in \text{Frac}(\mathbb{Z}[X])$, 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* $\mathbf{Frac(}\boldsymbol{R[X]}\mathbf{)}$.
- **Field of rational functions**: The rational functions in X over a field F. *Denoted by* $\boldsymbol{F(x)}$.

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: Diadic 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 $\boldsymbol{F}$ generated by $\boldsymbol{R}$**: 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 $D = R \setminus \{0\}$ 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. $\square$

- 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**.
- 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
  $$d = \min\{N(a) \mid a \in I \setminus \{0\}\}$$
  Pick $f \in I \setminus \{0\}$ 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. $\square$

- 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. $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ (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 $a, b \in \mathbb{Q}$.
     - 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 $\cos(120) + i\sin(120)$.
     - 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
       $$\left\{\alpha + \beta\frac{-1+\sqrt{-3}}{2} \mid \alpha, \beta \in \mathbb{Z}\right\} \cong \left\{a + b\sqrt{-3} \mid a, b \in \mathbb{Q},\ a = \alpha - \frac{1}{2}\beta,\ b = \frac{1}{2}\beta,\ \alpha, \beta \in \mathbb{Z}\right\}$$

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

- **Square-free integer**: An integer that is not divisible by the square of any integer.
- **Gaussian integers**: The Euclidean domain $\mathbb{Z}[\sqrt{-1}]$.
- **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. $F^\times = F \setminus \{0\}$.
  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. $\mathbb{Z}^\times = \{\pm 1\}$.
  4. $\mathbb{Z}[\sqrt{-1}]^\times = \{\pm 1, \pm i\}$.
  5. $R[X]^\times = R^\times$ (R an integral domain).
  6. Suppose R is not an integral domain. Then we get things like $a \neq 0 \in R$ 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.
- $R \setminus \{0\}$ is a disjoint union of...
  (i) Units;
  (ii) Reducible elements;
  (iii) And irreducible elements.

  Proof. Suppose for the sake of contradiction that $a \in R \setminus \{0\}$ 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. □

- 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 $\pi_1, \dots, \pi_r \in R$. *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., $R \setminus P$ is a multiplicative set.
- 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): An element...
  - Think of them a bit like primes, though this is very dangerous.
- **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 $u_1, \dots, u_r \in R^\times$ such that $\pi_i' = u_i\pi_{\sigma(i)}$ $(i = 1, \dots, r)$ 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 $u_2, \dots, u_r \in R^\times$ such that $\pi_i' = u_i\pi_{\sigma(i)}$ $(i = 2, \dots, r)$. Extend σ to S_r by defining $\sigma(1) = 1$. Thus, taking $\sigma \in S_r$ and $u_1, \dots, u_r \in R^\times$, we know that $\pi_i' = u_i\pi_i$ $(i = 1, \dots, r)$. 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 $d' \mid d$.

- 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 on Dummit and Foote (2004, pp. 287–89).
- 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 $a_n = b_na_{n+1}$. Then $(a_n) \subset (a_{n+1})$. and $b_n \notin R^\times$.
- If $(a_n) = (a_{n+1})$, then $a_{n+1} = ca_n$, $a_n = b_n \subset a_n$, $1 = b_nc$.

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 $I_1I_2 \subset I_1 \cap I_2$ 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 $\phi \circ \psi = \psi \circ \phi = \text{id}$, 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 $a^2 = 1^2a^2$ 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. $\underline{(2) \implies (3)}$: Since (π) is a maximal ideal, $R/(\pi)$ is a field. Thus, it's an integral domain. Therefore, (π) is a prime ideal.

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

  $\underline{(1) \implies (2)}$: 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 $R \setminus \{0\}$ (or R??) is an integral domain.
  - Thus, if $a, b \in R \setminus \{0\}$, 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 $R \setminus \{0\}$.
  - $\gcd(a,b) \in \sim \backslash R - \{0\}$.
    - This allows us to define a unique gcd; recall that gcd's are only unique up to multiplication by units, so by making all elements multiplied by units part of 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. $\square$

- 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

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

  - 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 explain 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 $R_2 a + R_2 b = R_2 d$. $\square$

- Explanation of what's in quotes: We're taking gcd's in different rings. See the commutative diagram below.

$$\begin{tikzcd}
R_1 - \{0\} \arrow[r, hook] \arrow[d] & R_2 - \{0\} \\
\sim \backslash R_1 - \{0\} \arrow[r] & \sim \backslash R_2 - \{0\} \arrow[u]
\end{tikzcd}$$

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.

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 $A_1, \dots, A_k$ be ideals in R. The map from $R \to R/A_1 \times \cdots \times R/A_k$ defined by

$$r \mapsto (r + A_1, \dots, r + A_k)$$

is a ring homomorphism with kernel $A_1 \cap \cdots \cap A_k$. If for each $i, j \in \{1, \dots, k\}$ 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**.
- **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 $\text{Frac}\, R$, 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 to be 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.
     - Gaussian integers are a subset.
  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*

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

- **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. Quadratic integer rings; specifically, $\mathbb{Z}[\sqrt{-5}]$.
- 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* ***b* divides *a***.
- Definition of the **greatest common divisor** of a, b.
- Note:

$$b \mid a \quad \Longleftrightarrow \quad a \in (b) \quad \Longleftrightarrow \quad (a) \subset (b)$$

  - 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. Given. Very slick. ☐

- 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 $0 < N(sa - tb) < N(b)$.

- 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 reducible.

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

  Proof. Given (see Lecture 4.2). ☐
- Irreducible $\not\Rightarrow$ prime in general.
  - Example using quadratic integer rings given.
- Prime $\Longleftrightarrow$ 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. $\square$

- 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 $p_1, \dots, p_n$ are *distinct*, and the exponents $e_i, f_i \geq 0$ $(i = 1, \dots, n)$. 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). $\square$

- 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 $r_{1\cdots 1}$ 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*.

<u>Uniqueness</u>: 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*.
- 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.

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

- 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 $R[X_1,\dots,X_n]$ is a UFD.

  Proof. Use induction. □
- Corollary: $R[X]$ is a field implies R is a PID implies $R[X_1,\dots,X_n]$ 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 $g(X) = X^d + a_1 X^{d-1} + \cdots + a_d$ 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 $\mathcal{P}(R) \subset R \setminus \{0\}$ be such that...
  (i) Every $\pi \in \mathcal{P}(R)$ is irreducible.
  (ii) For all $\alpha \in \mathbb{R} \setminus \{0\}$, 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 $|\{\pi \in \mathcal{P}(R) \mid k(\pi) > 0\}|$ 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 $f = a_0 + a_1 X + a_2 X^2 + \cdots$ 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

$$\varphi(a_0 + a_1 X + \cdots + a_d X^d) = \bar{a}_0 + \bar{a}_1 X + \cdots + \bar{a}_d X^d$$

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.
- $\mathcal{P}(R[X]) = \mathcal{P}(R) \sqcup \{\tilde{g} \mid g \in K[X] \text{ is monic and irreducible}\}$.
- 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 diadic 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: $R \setminus \{0\}$ 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

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

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

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

    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

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

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

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

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

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

  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

$$\begin{aligned} T(g) &= 0 \\ (g(c_0), \dots, g(c_d)) &= (0, \dots, 0) \end{aligned}$$

Thus, g has $d+1$ distinct roots $c_0, \dots, c_d$. It follows that $g \in ((X - c_0) \dots (X - c_d))$, 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. $\square$

- 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 $e_0, \dots, e_d \in F$ arbitrary, there exists a unique $g \in P_d$ such that $g(c_i) = e_i$ ($i = 0, \dots, d$).
  - 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 $g(c_0), \dots, g(c_d)$. But $g(c_i) \mid f(c_i)$ for all $i = 0, \dots, d$. 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

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

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 $g = b_0 X^d + b_1 X^{d-1} + \cdots + b_d$ ($b_i \in \mathbb{Z}$). 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. $a_0 b_r/b_0 \in \mathbb{Z}$ 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.

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

$\square$

- 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. $\square$

- Hilbert null statement The only maximum ideals of $\mathbb{C}[X_1, \dots, X_n]$ are $(X_1 - a_1, \dots, X_n - a_n)$ where $(a_1, \dots, a_n) \in \mathbb{C}^n$.
  - 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!

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 $X_1, \dots, X_n$ with coefficients in R): The ring defined inductively as follows. *Denoted by* $\boldsymbol{R[X_1, \dots, X_n]}$. *Given by*

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

  - 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*

$$(d_1, \dots, d_n)$$

- **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, $p_1 R[X]$ 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. $\square$

- 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

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

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 $a_{n-1}, \dots, a_0$ 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

???

6.1 Module Tools

2/6:
- A fifth week summary has been posted.
  - Week 5 content is not in the midterm syllabus.
    - In particular, Gauss's Lemma is not on the midterm.
  - Lecture 5.3 won't even be on the final syllabus.
  - The techniques are applicable to a variety of problems, though, so it is good to know them.
- Today: Modules.
  - We depart from commutative rings and return to simple rings with identity to start.
- Notation: What kinds of sets different letters denote.
  - A, B: Rings.
  - R: Commutative ring.
  - F, K: Fields.
  - D: Division ring.
- Linear algebra is the study of division rings but only over fields.
- Definition of a **division ring**.
  - The only ideals of a division ring are $0, D$, just like with fields.
  - Linear independence, spanning, basis, etc. all hold in a general division ring; you only need fields for things like JCF.
- **Left $\boldsymbol{A}$-module**: An abelian group $(M, +)$ equipped with a binary operation $\cdot : A \times M \to M$ defined by $(a, m) \mapsto am$ (or $a \cdot m$ in the case of potential ambiguity) satisfying the following. *Constraints*

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

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

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

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

  (4) $1_A v = v$.
- We need the last one so that multiplication is nontrivial.
- A **right $\boldsymbol{A}$-module** puts the scalar on the right. Will we ever consider these??

- Notation: For all $a \in A$, define the function $\rho(a) : M \to M$ by $\rho(a)v = av$ for all $v \in M$. *Constraints*
  (1) $\rho(a)$ is a group homomorphism from $M \to M$.
  (2) $\rho(a+b) = \rho(a) + \rho(b)$.
  (3) $\rho(a)\rho(b) = \rho(ab)$.
  (4) $\rho(1_A) = 1_{\mathrm{End}(M)}$
- Conditions 2-4 imply that $\rho : A \to \mathrm{End}(M)$ is a ring homomorphism.
  - Recall HW1 Q1.14, which led up to the result that
  $$\mathrm{End}(M) = \{f : M \to M \mid f \text{ is a group homomorphism}\}$$
  is a ring with identity under componentwise addition and composition (i.e., $g \cdot f = g \circ f$).
- Going forward, in-class definitions will always match those in the book.
  - It's been this way for a while??
- Examples.
  1. Let $M = A$. Then $\rho(a)b = ab$ for all $a \in A$, $b \in M = A$.
  2. If M_i ($i \in I$ an indexing set) is a (left) A-module, then the product $\prod_{i\in I} M_i$ is also an A-module.
  3. Denote an element of $\prod_{i\in I} M_i$ by $\prod_{i\in I} m_i$. An arbitrary choice of $m_i \in M_i$ for all $i \in I$ is allowed (do we need the Axiom of Choice??). We define $\cdot$ by
  $$a\left(\prod_{i\in I} m_i\right) = \prod_{i\in I}(am_i)$$
  4. The collection
  $$\oplus_{i\in I} M_i = \left\{\prod_{i\in I} m_i \mid \{i \in I : m_i \neq 0\} \text{ is a finite set}\right\}$$
  is an A-module.
     - This is a submodule of something??
     - Under the same binary operation as Example 3??
  5. In particular, A^m is an A-module with $a(b_1, \dots, b_n) = (ab_1, \dots, ab_n)$.
- **Submodule**: A subgroup $(N, +)$ of $(M, +)$ such that for all $a \in A$ and $\omega \in N$, $a\omega \in N$.
- Observation: If N_1, N_2 are submodules of M, then $N_1 + N_2$ and $N_1 \cap N_2$ are submodules.
- Question (base case): What are the submodules of A, itself?
  - Left ideals.
- **Module homomorphism**: A function $T : M \to N$ such that T is a homomorphism of abelian groups and commutes with scalar multiplication (i.e., $T(av) = aT(v)$ for all $a \in A$, $v \in M$). In full, we have
  $$T(a_1v_1 + a_2v_2) = a_1T(v_1) + a_2T(v_2)$$
  for all $a_1, a_2 \in A$ and $v_1, v_2 \in M$.
- Question: What are all of the module homomorphisms $T : A \to M$?
  - If $T(1) = v$, then $T(a \cdot 1) = aT(1) = av$ for all $a \in A$.
  - For all $v \in M$, there exists a unique $T : A \to M$ such that $T(1) = v$. This is more linear algebra.

- Question: What are all linear transformations $T : A^n \to M$?
  - Suppose $e_1 = (1, 0, \dots, 0)$, $e_2 = (0, 1, 0, \dots, 0)$, etc. Then
  $$(a_1, \dots, a_n) = \sum_{i=1}^{n} a_i e_i$$
  - Therefore,
  $$T(a_1, \dots, a_n) = \sum_{i=1}^{n} a_i T e_i$$
  - Take any ordered n-tuple of elements in M; then given $v_1, \dots, v_n \in M$, there is a unique A-module homomorphism $T : A^n \to M$ such that $T(e_i) = v_i$ $(i = 1, \dots, n)$.
- **Isomorphism** (of A-modules): A bijective module homomorphism $T : M \to N$, where M, N are A-modules.
- It follows that $T^{-1} : N \to M$ is also a homomorphism.
- 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.

  <u>Existence</u>: For all $a \in A$, we have that $\rho(a) : M \to M$ take $\rho(a)N \subset N$. It induces $\overline{\rho(a)} : M/N \to M/N$. Take $\overline{\rho(a)}$, which is scalar multiplication by a on M/N. ☐

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

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

Figure 6.1: First isomorphism theorem of modules.

- Example: $A = \mathbb{Z}$ and $M = \mathbb{Z}/(27)$.
- Theorem: Let R be a PID. Then every R-submodule of R^n is isomorphic to R^m for some $0 \leq m \leq n$.
- Think in terms of fields! If Nori had been couching all of this in terms of vector spaces, we would all get all of this immediately.
- Let $n = 1$, $(2) \subsetneq \mathbb{Z}$. Then $m = n$ does not imply $M = R^n$.
- Submodules of R are ideals. Thus, in a PID, they're principal ideals.

  Proof. Case 1 (base case): Let $n = 1$. We know that $M = (b)$ for some $b \in R$. If $b = 0$, then we're done. Thus, assume $b \neq 0$. Then $T : R \to (b)$ given by $T(a) = ab$ for all $a \in A$. It follows that T is onto. From the fact that R is an integral domain, we have that T is 1-1.

  Case 2 (general case): We induct on n. Suppose that $i : R^{n-1} \hookrightarrow R^n$ is given by
  $$i(a_1, \dots, a_{n-1}) = (a_1, \dots, a_{n-1}, 0)$$

Let M be a submodule of R^n. Then $R^{n-1} \times \{0\} \hookrightarrow R^n$ and $M \cap (R^{n-1} \times \{0\}) \cong R^\ell$ for $0 \leq \ell \leq n-1$. Suppose that you define the ideal $\pi(a_1, \ldots, a_n) = a_n$. Let $\pi(M) = I$. Then you have some ideal I. It follows that $\pi : M \to I \subset R$. Let $M' = \ker \phi$. $M/M' \cong I$. At this point, there are only two cases ($a = 0$ and $a = M$). $\square$

- Next time: We will wrap up this proof with the following proposition.
- Proposition: If M' is a submodule of M and $M/M' \cong R$ as an R-module, then $M \cong M' \oplus R$.

References

Dummit, D. S., & Foote, R. M. (2004). *Abstract algebra* (third). John Wiley and Sons.