MATH 25800 (Honors Basic Algebra II) Notes

Steven Labalme

January 9, 2023

Weeks

Week 1

Rings Intro

1.1 Rings, Subrings, and Ring Homomorphisms

1/4:

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

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

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

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

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

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

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

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

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

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

for all $a, b \in R$.

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

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

for all $a \in R$.

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

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

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

□

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

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

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

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

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

  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).
    - 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 $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ and $n \in \mathbb{Z}_{\geq 0}$.
    - Naturally, terms of this form are called **polynomials**.
    - As the set of polynomials is at last closed under $+, \times$, M must be a **polynomial ring**.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

  - This is the **power series ring**.

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

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

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

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

- 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 1. Let R be a ring. Then

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

  Proof. Given. □

- **Zero divisor**: A nonzero element $a \in R$ to which there corresponds a nonzero element $b \in R$ such that either $ab = 0$ or $ba = 0$.
- **Unit** (in R a nonzero ring with identity): An element $u \in R$ to which there corresponds some $v \in R$ such that $uv = vu = 1$.
  - As the phrasing of the term implies, the property of being a unit depends on the ring in which an element is viewed. For example, 2 is not a unit in $\mathbb{Z}$, but 2 is a unit in $\mathbb{Q}$.
- **Group of units** (of R): The set of all units in R. *Denoted by* $\boldsymbol{R^\times}$.
  - 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 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 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.

Exercises

9. For a fixed element $a \in R$, define $C(a) = \{r \in R \mid ra = ar\}$. Prove that $C(a)$ is a subring of R containing a. Prove that the center of R is the intersection of the subrings $C(a)$ over all $a \in R$.

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

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

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

  with $n \geq 0$ and each $a_i \in R$.
- **Degree n** (polynomial): A polynomial for which $a_n \neq 0$.
- **Leading term**: The $a_n x^n$ term.
- **Leading coefficient**: The a_n coefficient.
- **Monic** (polynomial): A polynomial for which $a_n = 1$.
- Definition of $R[X]$ (Dummit & Foote, 2004, p. 234).
- **Constant polynomials**: The set of polynomials $R \subset R[X]$.
- It follows from its construction that $R[X]$ is a commutative ring with identity (specifically 1_R).
- Definition of $\mathbb{Z}[X], \mathbb{Q}[X]$.
- We can also define polynomial rings like $\mathbb{Z}/3\mathbb{Z}[X]$.
  - This ring consists of the set of polynomials with coefficients $0, 1, 2$ and calculations on the coefficients performed modulo 3.
  - Example: If $p(x) = x^2 + 2x + 1$ and $q(x) = x^3 + x + 2$, then $p(x) + q(x) = x^3 + x^2$.

- The ring in which the coefficients are taken makes a substantial difference in the polynomials' behavior.
  - Example: x^2+1 is not a perfect square in $\mathbb{Z}[X]$, but is in $\mathbb{Z}/2\mathbb{Z}[X]$ since here,

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

- Properties of polynomials over integral domains.

  Proposition 4. Let R be an integral domain and let $p(x), q(x)$ be nonzero elements of $R[X]$. Then

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

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

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

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

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

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

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

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

- If R has zero divisors, then so does $R[X]$.
  - If $f \in R[X]$ is a zero divisor, then $cf = 0$ for some nonzero $c \in R$ (see Exercise 7.2.2).
- If S is a subring of R, then $S[X]$ is a subring of $R[X]$.
- 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 $i, j \in \{1, \ldots, n\}$.
  - The scalar matrices form a subring of $M_n(R)$, specifically one that is isomorphic to R.

  - We have that

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

  - If R is commutative, the scalar matrices commute with all elements of $M_n(R)$.

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

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

  under componentwise addition

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

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

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

  where $a_i \in R$, a commutative ring with identity $1 \neq 0$, and $g_i \in G$, a finite group with group operation written multiplicatively, for all $1 \leq i \leq n$. *Denoted by* $\boldsymbol{RG}$.
  - Note that the commutativity of R is not technically needed.
  - The associativity of multiplication follows from the associativity of the group operation in G.
  - RG is commutative iff G is abelian.
  - If $g_1 \in G$ is the identity of G, then we denote $a_1 g_1$ by a_1.
  - Similarly, if $1 \in R$ is the multiplicative identity of R, then we denote $1 g_i$ 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 $1 g_i$.
  - 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

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

Week 2

???

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 $a : \mathbb{Z}_{\geq 0} \to R$).
  - According to Nori, Dummit and Foote (2004) explains this pretty well.
- A question from both classes: What is X in the polynomial ring?
  - First ask: What does $a^7 + 6a^5 - 8 = 0$ mean?
    - It is a constraint that a must satisfy, given that a lies in some world (be it $\mathbb{R}$, $\mathbb{C}$, or elsewhere).
  - Then ask: What does $a^7 + 6a^5 - 8$ mean?
    - It is like a function $f(a)$.
    - It means that if $a \in R$, then $f(a)$ is defined in R, where R is a ring.
  - At this point, switch the arbitrary notation to $f(X) = X^7 + 6X^5 - 8$.
    - Then f is a function in $\mathbb{Z}[X]$.
    - But it is more than that, too: We know that if $x \in R$, R a ring, then $f(x) \in R$. Thus, the evaluation function $\mathrm{ev}_x : \mathbb{Z}[X] \to R$ is a ring homomorphism sending $f \mapsto f(x)$.

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

- We now start the lecture officially.
- Today: Continuing doing what we did with groups but with rings.
- Last time: Extended the notions of subgroups and homomorphisms.
- Other concepts up for grabs:
  - Normal subgroups (recall that these arose as the kernels of group homomorphisms).
  - Quotient groups.
  - The FIT (aka the Noether isomorphism theorem),.
  - The second isomorphism theorem ($H_1, H_2 \triangleleft G$ implies $H_1 \cap H_2$ and $H_1 H_2$ 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 SIT does 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* $\mathbf{ker(}f\mathbf{)}$. *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 $a_p X^p b_q X^q = a_p b_q X^p X^q$ example.
  - Example of where this matters.
    - Consider the ring of functions $f : \mathbb{R} \to \mathbb{R}$, on which the evaluation function is a ring homomorphism.
    - Letting $i \in \mathbb{C}$ be the unit imaginary number, it is not true that $\mathrm{ev}_i : \mathbb{R}^{\mathbb{R}} \to \mathbb{R}$ is a ring homomorphism since only certain functions on the reals can naturally be extended to the complex numbers.
    - However, consider the subring $\mathbb{R}[X]$ of $\mathbb{R}^{\mathbb{R}}$. Since i does commute with every real number and polynomials are made of products of real numbers and i, $\mathrm{ev}_i : \mathbb{R}[X] \to \mathbb{R}$ *is* a ring homomorphism.
  - All of this should be kept in mind, but it's not too important at this point.
  - Misc. note: Think more about why it's so "obvious" that evaluating at a point defines a ring homomorphism.
    - Perhaps it's not so much that it's "obvious" as that it follows directly from the axioms and not much creativity is needed in the proof.

- Was there a problem if R is not commutative with the evaluation function?
  - See above.

- Does the fact that ev is a ring homomorphism follow from the universal property of a polynomial ring?
  - Maybe? Didn't want to belabor the point.

- Is the in-class statement of the SIT correct?
  - That the product of two normal subgroups is normal is true, but it is not part of the SIT. In fact, it is part of one of the other isomorphism theorems. Nori just included these SIT and other statements to show what can be transferred. We will not talk about these results further, though, because they can all be deduced from the FIT.

- How do we know the subtraction/multiplication statement?
  - Two ways of looking at this.
    1. Proof in terms of coset properties.
       - $a_i' \in a_i + I$ iff $a_i' + I = a_i + I$.
       - Thus,
$$(a_1 + I) \cdot (a_2 + I) = (a_1' + I) \cdot (a_2' + I)$$
$$a_1 a_2 + I = a_1' a_2' + I$$
       so
$$a_1 a_2 - a_1' a_2' \in I$$
    2. Proof in terms of a clever trick and properties of ideals.
       - We are given $a_1 - a_1' \in I$ and $a_2 - a_2' \in I$.
       - We can write that
$$a_1 a_2 - a_1' a_2' = (a_1 - a_1')a_2 + a_1'(a_2 - a_2')$$
       - The two terms in parentheses on the RHS above are in I by hypothesis.
       - Since I is a two-sided ideal, $(a_1 - a_1'), (a_2 - a_2') \in I$, and $a_2, a_1' \in R$, we have that $(a_1 - a_1')a_2, a_1'(a_2 - a_2') \in I$.
       - Since I is a subgroup (and hence closed), $(a_1 - a_1')a_2 + a_1'(a_2 - a_2') \in I$, as desired.

2.3 Chapter 7: Introduction to Rings

From Dummit and Foote (2004).

Section 7.3: Ring Homomorphisms and Quotient Rings

- 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
$$\phi_n(xy) = nxy = n^2 xy = nxny = \phi_n(x)\phi_n(y)$$
       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 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 6. Let R be a ring and let I be an ideal of R. Then the (additive) quotient group R/I is a ring under the binary operations

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

  for all $r, s \in R$. Conversely, if I is any subgroup such that the above operations are well-defined, then I is an ideal of R.

- Definition of a **quotient ring**.
- Isomorphism theorem analogies.

  Theorem 7.

  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 $\boldsymbol{n}$**.
  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.

References

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