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
  $$\begin{aligned} l_a(0_R) &= 0_R \\ a \times 0_R &= 0_R \end{aligned} \qquad\qquad \begin{aligned} l_a(-b) &= -l_a(b) \\ a \times (-b) &= -(a \times b) \end{aligned}$$
  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

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

  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 $a_0, a_1, \dots, a_n \in \mathbb{Z}$ 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*

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

  - 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 $f = a_0 + a_1 X + \cdots + a_m X^m$, $f(x) = (a_0)_R + (a_1)_R x + \cdots + (a_m)_R x^m$, 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 $a_0, \dots, a_m \in R$, $m \in \mathbb{Z}_{\geq 0}$.
  - 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*

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

  - 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.