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.
  1. (i) $(R, +)$ is an abelian group.
  2. (ii) $(R, \times)$ is associative, i.e.,
  $$a \times (b \times c) = (a \times b) \times c$$
  for all $a, b, c \in R$.
  3. (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
$$\begin{aligned} l_a(0_R) &= 0_R & \qquad l_a(-b) &= -l_a(b) \\ a \times 0_R &= 0_R & a \times (-b) &= -(a \times b) \end{aligned}$$
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 $\{a/p^n : a \in \mathbb{Z}, n = 0, 1, \dots\}$, $\{a/(p_1 p_2 \cdots p_r)^n : a \in \mathbb{Z}, n = 0, 1, \dots\}$, arbitrary subsets of primes in the denominator.
  - Exercise: There's a bijective correspondence between the subrings of $\mathbb{Q}$ and the power set of the prime numbers.

1.2 Office Hours (Nori)

1/5:

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

1.3 Polynomial Rings and Power Series Rings

1/6:

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

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

  - 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 $f = a_0 + a_1X + \cdots + a_mX^m$, $f(x) = (a_0)_R + (a_1)_R x + \cdots + (a_m)_R x^m$, 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 these polynomials and the ones from Question 1: These are the polynomials with coefficients in $R \supset \mathbb{Z}$, where this containment is homomorphic (not necessarily injective).
    - ■ Therefore, we need to define a broader type of polynomial ring.

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

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

  - 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

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

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

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

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

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

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

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

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

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

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

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

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

  as desired. □

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

1.4 Chapter 7: Introduction to Rings

From Dummit and Foote (2004).

A Word on Ring Theory

1/7:

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

Section 7.1: Basic Definitions and Examples

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

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

  - Thus, by transitivity and the cancellation law,

    $$b + a = a + b$$

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

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

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

  $$a + bi + cj + dk$$

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

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

  and distributive noncommutative multiplication subject to the relations

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

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

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

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

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

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

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

  Proposition 7.1. Let R be a ring. Then

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

  Proof. Given. □

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

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

    a contradiction. The argument is symmetric if we assume $ba = 0$.
  - It follows that fields contain no zero divisors.
- Examples of zero divisors and units.

  1. $\mathbb{Z}$.
     - No zero divisors and $\mathbb{Z}^\times = \{\pm 1\}$.

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

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

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

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

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

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

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

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

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

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

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

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

- Properties of integral domains.

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

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

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

  Corollary 7.3. Any finite integral domain is a field.

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

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

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

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

  where

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

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

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

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

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

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

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

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

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

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

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

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

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

- **Degree n** (polynomial): A polynomial for which $a_n \neq 0$.
- **Leading term**: The a_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 $R[X]$.
  - Think back to the definition.
- More on polynomial rings in Chapter 9.

1/9:

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

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

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

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

  for some $a \in R$ and all $i, j \in \{1, \dots, n\}$.
  - 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 $(a g_i)(b g_j) = (ab) g_k$ (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_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* $\boldsymbol{\mathbb{Z}G}$.
- **Rational group ring** (of G): The group ring of G with coefficients in $\mathbb{Q}$. *Denoted by* $\boldsymbol{\mathbb{Q}G}$.
- 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 $i = 0, 1, \dots, n$ and show that this implies $b_mp(x) = 0$.