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

1/11:

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

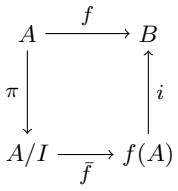

Figure 2.1: Noether isomorphism theorem.

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

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

We now just need to prove that $\bar{f}$ respects multiplication and sends 1 to 1 to complete our verification that it is a ring homomorphism. We will do this indirectly. First, observe that f is a ring homomorphism and i is a one-to-one ring homomorphism (really; do you mean that i is one-to-one with the subset $f(A) \subset B$ so that defining $i^{-1} \circ f$ makes sense??). Thus, $\bar{f} \circ \pi = i^{-1} \circ f$ is a ring homomorphism (as we can confirm). This combined with the fact that π is onto implies that $\bar{f}$ is a ring homomorphism (as we can confirm).

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

- Notes on the Noether Isomorphism Theorem.
  - Nori leaves out some of the grueling detail in this proof in favor of a simple statement of the idea (the "as we can confirm" statements) because we can work out that detail for ourselves.
    - Nori accidentally presented all of the detail last class, and people got very confused.
    - The language used in the proof we have now is not intended to confuse but to provide intuition; we can investigate rigor to whatever depth we choose.
  - More on the structure of the decomposition: π is the canonical surjection and i is the canonical injection; $\bar{f}$ is in the middle.
- **Isomorphism** (of rings): A ring homomorphism $f : A \to B$ for which...
  (i) There exists a corresponding ring homomorphism $g : B \to A$ such that...
  (ii) $f \circ g = \mathrm{id}_A$ and $g \circ f = \mathrm{id}_B$.
- Notes on the definition of an isomorphism of rings.
  - If f is a ring homomorphism, then (ii) implies that f is a bijection of sets.
    - Implication: If f is a ring homomorphism and if f is a bijection, then there exists a function $g : B \to A$ such that (ii) holds.
    - It is fairly clear that this g is also a ring homomorphism.
  - "Iso" means bijective homomorphism.
  - We need bijective because continuous functions don't have continuous inverses??
- Let's go back to talking about ideals.
- **Principle left ideal**: An ideal of the following form, where R is a ring and $b \in R$. *Denoted by* $\boldsymbol{Rb}$. *Given by*
$$Rb = \{ab \mid a \in R\}$$
  - $(Rb, +)$ is an additive subgroup of R.
    - This follows from the fact that $r_b : (R, +) \to (R, +)$ is a group homomorphism and Rb is equal to the image $r_b(R)$ of R under this group homomorphism.
  - This motivates the linear algebra exercises in HW2??
  - There also exist principal right ideals and principle two-sided ideals.
  - It is correct that Rb is a principal "left" ideal (closed under *left* multiplication), even though Hg is a "right" coset (multiplying the coset by an element of G on the right).
- Let $c \in R$, let $h \in Rb$. Is $ch \in Rb$?
  - Yes, because $h = ab$ implies that there exists $a \in R$ such that $ch = (ca)b \in Rb$. Check??

- We now look at three constructions originating from ideals: Sums, intersections, and products.
- **Sum** (of ideals): The ideal defined as follows, where $I, J \subset R$ are ideals. *Denoted by* $\boldsymbol{I+J}$. *Given by*

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

  - Definitions for left, right, and two-sided ideals.
  - We can check all of the properties to confirm that this is an ideal.
  - Let $\alpha \in R$, $\alpha I \subset I$. Well $\alpha I \subset J$ implies $\alpha(I + J) \subset I + J$.
- Let $\{I_\lambda\}_{\lambda\in\Lambda}$ be a (finite??) family of ideals (left, right, or two-sided). Then

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

  is a (left, right, or two-sided) ideal.
- Example: Given $a_1, a_2 \in R$, $Ra_1 + Ra_2$ is a left ideal.
  - Note that it is not a principal ideal, however.
- R a ring implies that $R[X]$ is a ring, which in turn implies that $R[X][Y] = R[X, Y]$ is also a ring.
  - Let $R[X, Y] = A$ and $R = \mathbb{R}$. Then, for instance,

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

  - All of these functions vanish at $(0, 0)$. Thus, this ideal is not principal??
    - It'll be a while before we treat such rings formally.
    - We can take this claim as an exercise for now, though (see below).
  - Note that similarly, AX is the set of all functions vanishing on the y-axis.
- Exercise: Prove that $AX + AY$ is not a principal ideal.
- **Intersection** (of ideals): The ideal defined as follows, where $\{I_\lambda\}_{\lambda\in\Lambda}$ is a family of ideals. *Given by*

$$\bigcap_{\lambda\in\Lambda} I_\lambda$$

  - Definitions for left, right, and two-sided ideals.
  - Easy said aloud, not written down??
- **Product** (of ideals): The ideal defined as follows, where I, J are ideals. *Denoted by* $\boldsymbol{IJ}$. *Given by*

$$IJ = \{a_1b_1 + a_2b_2 + a_nb_n \mid n \in \mathbb{N},\ a_1, \ldots, a_n \in I,\ b_1, \ldots, b_n \in J\}$$

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

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

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

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

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

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

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

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

2.4 Office Hours (Callum)

- HW1 Q11.
  - I need to factor in some -1's to account for all integers $\mathbb{Z}$.
- Do we have to justify $0 \cdot x = 0$ in our proof of HW1 Q1?
  - It's ok to assume things like this that were either covered in class or in the relevant sections of Dummit and Foote (2004).

- Do we need to go more formal for HW1 Q2, explaining different forms of addition, functional equality, etc.?
- Additional sophistication in HW1 Q10?
- Using HW1 Q7 to solve HW1 Q9?
  - Use the diagonal $\Delta : R \to R \times R$[1] defined by $r \mapsto (r, r)$.
  - We know that Δ is a ring homomorphism (see HW1 Q4) and that $A \times B \subset R \times R$ is a subring.
  - It follows from the set theoretic definition that $A \cap B = \Delta^{-1}(A \times B)$; apply HW 1 Q7.

2.5 Chapter 7: Introduction to Rings

From Dummit and Foote (2004).

Section 7.3: Ring Homomorphisms and Quotient Rings

1/9:

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

  Proposition 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.

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

  - 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

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

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

- **Trivial ideal**: The ideal $\{0\}$. *Denoted by* $\mathbf{0}$.
- **Proper** (ideal): An ideal I such that $I \neq R$.
- **Reduction mod n**: The natural projection $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.
- **Evaluation** (at c): The map from $A^X \to A$, where A is a ring and X is a nonempty set, defined as follows, where $c \in X$. *Denoted by* $\boldsymbol{E_c}$. *Given by*

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

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

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

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

1/11:

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

Theorem 8.

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

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

- Definition of **sum**, **product** of ideals.
  - Note that n is not fixed in the product definition, so that all *finite* sums (not just all sums of length n for n fixed) are included in the set.
- $\boldsymbol{n^{\text{th}}}$ **power** (of I): The set consisting of all finite sums of elements of the form $a_1 a_2 \cdots a_n$ with $a_i \in I$ for all i. *Denoted by* $\boldsymbol{I^n}$.
  - Alternate definition: Define $I^1 = I$ and $I^n = II^{n-1}$.
- $I + J$ is the smallest ideal of R containing both I and J.
- IJ is an ideal contained in $I \cap J$ (but may be strictly smaller).
- Examples.
  1. Let $I = 6\mathbb{Z}$ and $J = 10\mathbb{Z}$.
     - $I + J$ consists of all integers of the form $6x + 10y$.
       - In particular, all of these integers are divisible by 2, so $I + J \subset 2\mathbb{Z}$. On the other hand, $2 = 6(2) + 10(-1) \in I + J$ implies that $2\mathbb{Z} \subset I + J$. Therefore, $I + J = 2\mathbb{Z}$.
       - In general, $m\mathbb{Z} + n\mathbb{Z} = \gcd(m, n)\mathbb{Z}$
     - IJ consists of all integers of the form $(6x)(10y)$ (note that this does account for all finite sums due to the distributive law), i.e., in $60\mathbb{Z}$.
  2. Let I be the ideal in $\mathbb{Z}[X]$ consisting of the polynomials with integer coefficients whose constant term is even.
     - We know, for example, that $2, x \in I$. Thus, $4 = 2 \cdot 2$ and $x^2 = x \cdot x$ are elements of $I^2 = II$, as is their sum $x^2 + 4$; however, $x^2 + 4$ cannot be written as a single product $p(x)q(x)$ of two elements of I.