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 $a \in R$.
  - 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: $a_1-a_2'\in I$ 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

$$\begin{aligned}\alpha_1\cdot\pi(a_2+a_3) &= (\alpha_1\cdot\alpha_2)+(\alpha_1\cdot\alpha_3)\\ \alpha_1\cdot(\alpha_2+\alpha_3) &= (\alpha_1\cdot\alpha_2)+(\alpha_1\cdot\alpha_3)\end{aligned}$$