

# 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  $a : \mathbb{Z}_{\geq 0} \rightarrow R$ ).
    - 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  $\text{ev}_x : \mathbb{Z}[X] \rightarrow R$  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  $R[X] \rightarrow B$  is a ring homomorphism. Additional implication in this case??
  - There is a problem if  $R$  is not commutative, though??
  - Also, does the fact that  $\text{ev}$  is a ring homomorphism follow from the universal property of a polynomial ring??
- “Evaluation at a point is always a ring homomorphism.”
  - Why does  $\text{ev}_x : \mathbb{Z}[X] \rightarrow R$  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  $H_1H_2$  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  $I_1I_2$  are also two-sided ideals.
- Constructing ideals.
- **Kernel** (of a ring homomorphism): The set defined as follows, where  $f : A \rightarrow B$  is a ring homomorphism. Denoted by  $\ker(f)$ . 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.  $\square$

- 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 subgroup 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  $\mathcal{P}(A)$ .
- **Quotient ring:** The following set, where  $I \subset R$  is a two-sided ideal of a ring  $R$ . Denoted by  $R/I$ . Given by

$$R/I = \{a + I \mid a \in R\}$$

- A subset of  $\mathcal{P}(R)$ .
- We define an associated projection function  $\pi : R \rightarrow R/I$  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  $\pi$ , 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  $\pi : X \rightarrow Y$  is onto.
  - Question: Does there exist a binary operation  $\cdot$  on  $Y$  such that  $\pi$  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  $\pi$  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  $\cdot : Y \times Y \rightarrow Y$  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,  $a_1 c_2$  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  $I$ .

$$\subset a_1 a_2 + I$$

– Therefore,

$$\pi(\pi^{-1}(\alpha_1) \cdot \pi^{-1}(\alpha_2)) = \{a_1 a_2 + I\}$$

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  $a_1 a_2 - a'_1 a'_2 \in I$ .

– 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)  $\pi$  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  $\pi$ . 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  $R$ ,  $n_R x = x n_R$  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  $a_p X^p b_q X^q = a_p b_q X^p X^q$  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  $j : \mathbb{R} \rightarrow \mathbb{C}$  by  $a \mapsto (a, 0)$  and check that it is a ring homomorphism.
    - Define  $i = (0, 1) \in \mathbb{C}$ .
    - Define a map from  $\mathbb{R} \times \mathbb{R} \rightarrow \mathbb{C}$  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  $f : \mathbb{R} \rightarrow \mathbb{R}$ , on which the evaluation function is a ring homomorphism.
    - Letting  $i \in \mathbb{C}$  be the unit imaginary number, it is not true that  $\text{ev}_i : \mathbb{R}^{\mathbb{R}} \rightarrow \mathbb{R}$  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  $i$ ,  $\text{ev}_i : \mathbb{R}[X] \rightarrow \mathbb{R}$  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  $\text{ev}$  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,

$$\begin{aligned}(a_1 + I) \cdot (a_2 + I) &= (a'_1 + I) \cdot (a'_2 + I) \\ a_1 a_2 + I &= a'_1 a'_2 + I\end{aligned}$$

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.