

MATH 25800 (Honors Basic Algebra II) Notes

Steven Labalme

January 4, 2023

Weeks

1	???	1
1.1	Rings, Subrings, and Ring Homomorphisms	1
References		5

Week 1

???

1.1 Rings, Subrings, and Ring Homomorphisms

1/4:

- Intro to the course.
- What will be covered: Most of Chapters 7-12 in Dummit and Foote (2004).
 - Mostly rings, a bit of modules.
 - Modules tend to get more complicated.
 - The topics covered in class will all be in the book, but not necessarily in the same order.
 - Some of Nori's definitions will be different from those used in the book.
 - Different enough, in fact, to get us the wrong answers in PSet and Exam questions.
 - We should use his, though.
 - He diverges from the book because his is the mathematical literature standard.
 - Three main differences: Definition of a ring, subring, and ring homomorphism.
- Homework will be due every Wednesday.
 - The first will be due next week (on Wednesday, 1/11).
 - Rings, subrings, and ring homomorphisms, only, are needed for the first HW.
- Grading breakdown.
 - HW (30%).
 - Midterm (30%) — third or fourth week.
 - Final (40%).
- Office hours for Nori in Eckhart 310.
 - M (3:00-4:30).
 - Tu (3:30-5:00).
 - Th (3:00-4:30).
- Callum is our TA; Ray is for the other section. Their OH are TBA.
- All important course info will be in Files on Canvas.
- There will be course notes provided for the course.
- If we think something Nori writes down looks suspicious, feel free to ask!

- We now start the course content.
- **Ring**^[1]: A triple $(R, +, \times)$ comprising a set R equipped with binary operations $+$ and \times that satisfies the following three properties.

(i) $(R, +)$ is an abelian group.

(ii) (R, \times) is associative, i.e.,

$$a \times (b \times c) = (a \times b) \times c$$

for all $a, b, c \in R$.

(iii) The left and right distributive laws hold, i.e.,

$$a \times (b + c) = (a \times b) + (a \times c) \qquad (b + c) \times a = (b \times a) + (c \times a)$$

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 $l_a : R \rightarrow R$ and $r_a : R \rightarrow R$. In particular,

$$l_a(b) = a \times b \qquad r_a(b) = b \times a$$

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 0_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 $-a$.
- Since l_a is a group homomorphism, this must mean that

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

for all $a, b \in R$.

- The same holds for r_a /positions interchanged.
- These are consequences of the distributive law.

¹Definition from Dummit and Foote (2004).

²Since 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 $f, g : X \rightarrow \mathbb{R}$. We can define $f + g : X \rightarrow \mathbb{R}$ by $(f + g)(x) = f(x) + g(x)$ and $f \times g : X \rightarrow \mathbb{R}$ by $(f \times g)(x) = f(x)g(x)$.
 - Thus, the set of all functions from $X \rightarrow \mathbb{R}$ — 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:

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \quad (a_1, a_2) \times (b_1, b_2) = (a_1 \times b_1, a_2 \times b_2)$$

- 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 $f : A \rightarrow B$, where A, B are rings, such that

$$f(a_1 + a_2) = f(a_1) + f(a_2)$$

$$f(a_1 \times a_2) = f(a_1) \times f(a_2)$$

$$f(1_A) = f(1_B)$$

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 $i : S \rightarrow R$ is the inclusion map, then it is a ring homomorphism.
 2. R_1, R_2 are rings. Then $\pi : R_1 \times R_2 \rightarrow R_1$ 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. $i : R_1 \rightarrow R_1 \times R_2$ 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. $f : M_2(\mathbb{R}) \rightarrow M_3(\mathbb{R})$ 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

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \left(\begin{array}{cc|c} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{array} \right)$$

- The integers have no subrings except for itself.
 - Consider $\mathbb{Z}/10\mathbb{Z}$, for instance. Doesn't work because we postulate the existence of an identity, but $1 \notin \mathbb{Z}/10\mathbb{Z}$.
- Subrings of \mathbb{Q} :
 - \mathbb{Z}, \mathbb{Q} , the p -adic rationals $\{a/p^n \mid a \in \mathbb{Z}, n = 0, 1, \dots\}$, $\{a/(p_1 p_2 \cdots p_r)^n \mid a \in \mathbb{Z}, n = 0, 1, \dots\}$, arbitrary subsets of primes in the denominator.
 - Exercise: There's a bijective correspondence between the subrings of \mathbb{Q} and the power set of the prime numbers.

References

Dummit, D. S., & Foote, R. M. (2004). *Abstract algebra* (third). John Wiley and Sons.