MA 450: Honors Abstract Algebra Notes

Lecturer: Linquan Ma
Transcribed by Josh Park

Fall 2024

Contents

Lecture 32 (11/12)

12 Introduction to Rings

12.1 Motivation & Definition

Definition 1 (Ring)
A ring R is a set with two binary operations: $a + b$ and $a \cdot b = ab$ such that for all $a, b, c \in R$,

1. $a + b = b + a$
2. $(a + b) + c = a + (b + c)$
3. $\exists$ an additive identity 0, $a + 0 = a$
4. $\exists$ an element $-a \in R$ such that $a + (-a) = 0$
5. $(ab)c = a(bc)$
6. $a(b + c) = ab + ac$
   $(b + c)a = ba + ca$

So a ring is an abelian group under addition, and also has an associative multiplication that is left and right distributive over addition.

- The multiplication need not be commutative. When it is, we say the ring is commutative.
- A unity (or identity): a nonzero element that is an identity under multiplication.
- unit: a nonzero element of a commutative ring with identity that has a multiplicative inverse.
- In R, $a \mid b$ if $\exists c \in R$ such that $b = ac$.
- $n \in \mathbb{Z}_{>0}$, $na = \underbrace{a + a + \cdots + a}_{\text{n times}}$

12.2 Examples of Rings

Example 1
$(\mathbb{Z}, +\times)$ is a commutative ring with identity and units $= \pm 1$

Example 2
$(\mathbb{Z}_n, +\times)$ is a commutative ring with identity and units $= U(n)$

Example 3
$(\mathbb{Z}[x], +\times)$ is a commutative ring with identity

Example 4
$(\mathbb{M}_2[\mathbb{Z}], +\times)$ is a non-commutative ring with identity

Example 5
$(2\mathbb{Z} = \{\text{even integers}\}, +\times)$ is a comm ring without identity

Example 6
({continuous functions on $\mathbb{R}, +\times$}) is a comm ring with identity $f(x) = 1$

Example 7
({continuous functions on $\mathbb{R}$ whose graphs pass through $(1, 0), +\times$}) is a comm ring without identity

Note $f(1) = 0,\ g(1) = 0,\ f + g, fg$

Definition 2 (Direct sum of rings)
Let $R_1, R_2, \ldots, R_n$ be rings. Construct

$$R_1 \oplus R_2 \oplus \cdots \oplus R_n = \{(r_1, r_2, \ldots, r_n) \mid r_i \in R_i\}$$

endowed with component-wise addition and multiplication. This is called the direct sum of $R_1, R_2, \ldots, R_n$.

12.3 Properties of Rings

Theorem 12.1 (Rules of Multiplication)
For all $a, b, c \in R$,

1. $a \cdot 0 = 0 \cdot a = 0$
2. $a(-b) = (-a)b = -(ab)$
3. $(-a)(-b) = ab$
4. $a(b - c) = ab - ac$

   $(b - c)a = ba - ca$
5. $(-1)a = -a$
6. $(-1)(-1) = 1$

Note 1
Properties 5 and 6 only hold if R has an identity 1

Proof of property 1. Clearly $0+a0 = a0 = a(0+0) = a0+a0$, so by cancellation $0 = a0$ and similarly $0a = 0$ □

Theorem 12.2 (Uniqueness of the Unity and Inverses)
If a ring R has a unity, it is unique. If a ring element has a multiplicative inverse, it is unique.

Proof. 1, 1' $\implies$ 1=1·1' = 1'

$a \qquad ab = ba = 1$

$\qquad ac = ca = 1$

$c = c \cdot 1 = c(ab) = (ca)b = 1 \cdot b = b$ □

Warning
In general, $ab = ac \not\Longrightarrow b = c$ (cancellation rule does not hold in general for multiplication).

Example 8
In $\mathbb{Z}_6$, notice $2 \cdot 3 = 0 = 3 \cdot 0$ but $2 \neq 0$

12.4 Subrings

Definition 3 (Subring)
A subset $S \subseteq R$ is a subring of R if S is itself a ring with the operations of R

Theorem 12.3 (Subring Test)
A nonempty subset S of a ring R is a subring if S is closed under sutraction and multiplication.

i.e. if $a, b \in S$ then $a - b \in S$ and $ab \in S$

Example 9
$\{0\}$ and R will always be subrings of any ring R.

Example 10
$\{0, 2, 4\} \subseteq \mathbb{Z}_6$ is a subring

1 is the identity in $\mathbb{Z}_6$

4 is the identity in $\{0, 2, 4\}$ $(0 \cdot 4 = 0,\ 2 \cdot 4 = 2,\ 4 \cdot 4 = 4)$

Example 11
$n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$ is a subring of $\mathbb{Z}$ that does not have any identity (if $n \neq 1$).