Math 210B Notes

Spring, 2026

Contents

Chapter 1

Introduction to Rings

1.1 Ring and Field Definitions

We move on from studying groups to studying rings and fields. First, lets compare some analogues between groups and rings.

Groups:

(i) 1 operation
(ii) Subgroups
(iii) Normal groups N
(iv) Quotient groups G/N
(v) Morphisms of groups

Rings:

(i) 2 operations
(ii) Subrings
(iii) Ideals I
(iv) Quotient rings R/I
(v) Morphisms of rings

We build the theory of rings and fields in a similar way to the theory of groups. An important type of ring we wish to study is the ring of polynomials with coefficients in a field. Our goal is to be able to study Galois Theory and make a connection between automorphisms of fields and their subfields.

Before we get started, consider the following example.

Example 1.1.1. Let R be a set with operations $+$ and $\times$ such that distribution holds for all elements in the set:

$$\begin{aligned}\forall a,b,c \in R \quad a \times (b+c) &= (a \times b) + (a \times c)\\ (a+b) \times c &= (a \times c) + (b \times c)\end{aligned}$$

Further assume $+$ and $\times$ are associative and that there exists $1 \in R$ such that $1 \times a = a \times 1 = a$ for all $a \in R$. Let $-a$ and $-b$ be the additive inverses of $a, b \in R$. Show that

$$a + b = b + a$$

Proof.

$$\begin{aligned}(a+b)\times(1+1) &= (a+b)\times 1 + (a+b)\times 1\\ &= a\times 1 + b\times 1 + a\times 1 + b\times 1\\ &= a+b+a+b \qquad \text{(I)}\end{aligned}$$

$$\begin{aligned}(a+b)\times(1+1) &= a\times(1+1) + b\times(1+1)\\ &= a\times 1 + a\times 1 + b\times 1 + b\times 1\\ &= a+a+b+b \qquad \text{(II)}\end{aligned}$$

From (I) and (II), we have

$$\begin{aligned}
a+b+a+b &= a+a+b+b \\
\implies a+b+a+b-b &= a+a+b+b-b \\
\implies -a+a+b+a+0 &= -a+a+a+b+0 \\
\implies 0+b+a &= 0+a+b \\
\implies b+a &= a+b
\end{aligned}$$

□

This example motivates the following definition.

Definition 1.1.1. (Ring)
A ring is a set R together with two binary operations $+$ (called addition) and $\times$ (called multiplication) satisfying the following:

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

(ii) Multiplication is associative $\forall a,b,c \in R$

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

(iii) Distributive laws hold $\forall a,b,c \in R$

$$\begin{aligned}
\text{Left distribution: } a \times (b \times c) &= (a \times b) + (a \times c) \\
\text{Right distribution: } (a+b) \times c &= (a \times c) + (b \times c)
\end{aligned}$$

If multiplication is commutative, we call R a commutative ring. The ring R is said to have an identity denoted 1 (or contains a unity element) if

$$1 \times a = a \times 1 = a \quad \forall a \in R$$

In this case, R is called a ring with unity.

Notation . $a \times b$ will be written as ab. The additive identity of $(R,+)$ will be denoted 0. The additive inverse of an element $a \in R$ will be denoted $-a$.

Notice that our definition for a ring does not require the existence of a multiplicative inverse for each element in the ring. The addition of multiplicative inverses leads to more specific types of rings, and with the addition of multiplicative commutativity, we get fields.

Definition 1.1.2. (Division Ring, Field)
A ring R with unity 1 (where $1 \neq 0$) is called a division ring if every $a \in R$ where $a \neq 0$ has an element $b \in R$ such that $ab = ba = 1$. That is, if all nonzero elements have a multiplicative inverse. If R is also commutative, then R is called a field.

Example 1.1.2.

1. Trivial rings: Given any group $(G,*)$ if we take $*$ as addition and define multiplication as $ab = 0 \quad \forall a,b \in G$, then this forms a ring.
2. If $R = \{0\}$, this is called the zero ring with multiplication and addition defined as $0 \cdot 0 = 0$ and $0+0=0$. Note that this is the only ring where $1=0$. Show that if $1=0$, then $R=\{0\}$.

   Proof. Let $a \in R$.

   $$\begin{aligned}
   a \cdot 0 = a(0+0) &= a \cdot 0 + a \cdot 0 \\
   \implies a \cdot 0 &= a \cdot 0 + a \cdot 0 \\
   \implies 0 &= a \cdot 0 = a \cdot 1 = a
   \end{aligned}$$

   □

   Many theorems will state $1 \neq 0$ instead of $R \neq 0$.
3. $\mathbb{Z}$ with the usual multiplication and addition. Note that in $\mathbb{Z}/\{0\}$ we do not have a group with

respect to multiplication.

4. $\mathbb{Q}$ is a ring with the usual operations and $\mathbb{Q}/\{0\}$ is a group with respect to multiplication, that is $\mathbb{Q}$ is a field (multiplication in $\mathbb{Q}$ is commutative). $\mathbb{C}$ and $\mathbb{R}$ are fields as well.

5. $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with unity $\bar{1}$ ($\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, ..., n \bar{-} 1\}$) where the multiplication is defined $\bar{a} \cdot \bar{b} = \bar{ab}$.

6. The quaternians: recall the imaginary units $i^2 = j^2 = k^2 = ijk = -1$. Looking at the set $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ where addition is defined by

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k$$

and multiplication is defined by distribution

$$\begin{aligned}&(a + bi + cj + dk)(a' + b'i + c'j + d'k)\\ =&aa' - bb' - cc' - dd' + (ab' + ba' + cd' - dc')i + (a'c - bd' + ca' + db')j + (ad' + bc' - cb' + da')k\end{aligned}$$

Then $\mathbb{H}$ forms a ring. We see that, for $x \in \mathbb{H}$,

$$\begin{aligned}x\bar{x} &= (a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2\\ x^{-1} &= \frac{\bar{x}}{x\bar{x}} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}\end{aligned}$$

each analogous to the complex numbers. Every $x \neq 0$ in $\mathbb{H}$ has a multiplicative inverse. However, multiplication does not commute in all of $\mathbb{H}$ ($ik = -j \neq j = ki$), so $\mathbb{H}$ is a division ring but not a field.

7. Let X be a nonempty set and A be any ring. The set of all mappings $f : X \to A$ where $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$ forms a ring.

Since rings add an additional operation to a group structure, we have new properties that arise from the interaction of the two operations.

Proposition 1.1.1. Let R be a ring.

(i) $0 \cdot a = a \cdot 0 = 0 \quad \forall a, b \in R$

(ii) $(-a)b = a(-b) = -(ab) \quad \forall a, b \in R$

(iii) $(-a)(-b) = ab \quad \forall a, b \in R$

(iv) If R has identity 1, then that identity is unique and

$$-a = (-1)a \quad \forall a \in R$$

Proof. (i) Given $a \in R$, we have

$$\begin{aligned}a \cdot 0 &= a(0 + 0) = a \cdot 0 + a \cdot 0\\ &\implies 0 = a \cdot 0\end{aligned}$$

Similarly,

$$\begin{aligned}0 \cdot a &= (0 + 0)a = 0 \cdot a + 0 \cdot a\\ &\implies 0 = 0 \cdot a\end{aligned}$$

(ii) Given $a, b \in R$, we have

$$\begin{aligned}ab + (-a)b &= (a + -a)b\\ &= 0 \cdot b\\ &= 0 \implies -(ab) \qquad\qquad = (-a)b\end{aligned}$$

$-(ab) = a(-b)$ is analogous.

(iii) Given $a, b \in R$, we have

$$\begin{aligned} -(ab) + (-a)(-b) &= (-a)b + (-a)(-b) \\ &= (-a)(b + -b) \\ &= (-a) \cdot 0 \\ &= 0 \\ \implies -(-(ab)) &= (-a)(-b) \\ \implies ab &= (-a)(-b) \end{aligned}$$

(iv) Let 1 and e both be identity elements in R. Then

$$\left.\begin{aligned} 1 \cdot e = e \\ 1 \cdot e = 1 \end{aligned}\right\} \implies 1 = e$$

Thus the identity element of R is unique. Let $a \in R$ be given. We have

$$\begin{aligned} 0 &= (1 + (-1))a \\ &= 1 \cdot a + (-1) \cdot a \\ &= a + (-1)a \\ \implies -a &= (-1)a \end{aligned}$$

□