# Math 110BH Notes

Nathan Solomon

January 14, 2024

## Contents



# 1 Rings

## 1.1 1/8/2024 lecture

### 1.1.1 Definition of a ring

A *ring* is a set $R$ with two operations, *addition* and *multiplication*, such that

- $(R, +)$ is an abelian group
- *Left & right distibutivity* – For any $a, b, c \in R$, $(a+b)c = ac+bc$ and $c(a+b) = ca+cb$
- *Associativity* – $(ab)c = a(bc)$
- *Unitarity* – There exists an element called 1 such that $1a = a = a1$ for any $a \in R$

Sometimes people leave of those last two criteria, but in this class, we will only talk about associative, unital ring.

A ring $R$ is called *commutative* iff $ab = ba$ for any $a, b \in R$.

### 1.1.2 Examples of rings

The simplest ring is the zero ring, which is the zero group with $1 = 0$.

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, and $\mathbb{Z}/n\mathbb{Z}$ are all commutative rings.

If $R$ is a ring, then $M_n(R)$, the set of $n \times n$ rings over $R$ where $n \in \mathbb{N}$, is a ring. If $R$ is not the zero ring and $n > 1$, then $M_n(R)$ is noncommutative.

If $(A, +)$ is an abelian group and $R = \mathrm{End}(A) = \{f : A \to A \text{ is a homomorphism}\}$ is the set of endomorphisms of $A$, then $R$ becomes a ring when you define addition by $(f + g)(a) = f(a) + g(a)$ and define multiplication to be composition of endomorphisms.

For any ring $R = (R, +, \cdot)$, there exists another ring, $R^{op} = (R, +, *)$, defined by $a * b := b \cdot a$.

If $R$ is a ring, then $R[x]$ (the set of polynomials in the variable $x$ over $R$) is also a ring. If $R$ is commutative, then so is $R[x]$. In this case, "polynomials" are essentially lists of coefficients, with addition and multiplication defined the way you would expect for polynomials. This can be generalized to a finite set $X$ of variables – in that case, $R[X]$ is the set of polynomials over the variables in $X$, which are assumed to commute with each other.

If $R$ is a ring and $X$ is a set, then $S := \{f : X \to R\}$ with the operations defined by $(f + g)(x) = f(x) + g(x)$ and $(f \cdot g)(x) = f(x) \cdot g(x)$ forms a ring. If $|X| = 1$, then $R = S$.

### 1.1.3 Properties of rings

- $0a = 0 = a0$
- $(-a)(b) = -(ab) = (a)(-b)$
- A nonzero element $a$ of a commutative ring is called *invertible* iff there exists a nonzero element $b \in R$ such that $ab = 1 = ba$. If $b$ exists, it is unique, and it is called the *inverse* of $a$.
- If $a$ and $b$ are both invertible, then $(ab)^{-1} = b^{-1}a^{-1}$.

### 1.1.4 The multiplicative group

If $R$ is a commutative ring, let $R^\times$ be the set of invertible elements in $R$. Then $R^\times$ is a multiplicative group. $R$ is called a *field* iff it is commutative, $R$ is not the zero ring, and $R^\times = R \backslash \{0\}$. $\mathbb{Q}$ and $\mathbb{R}$ are examples of fields.

- $\mathbb{Z}^\times = \{-1, 1\}$
- $M_n(R)^\times = GL_n(R)$ is called the general linear group (of $n \times n$ matrices over $R$.
- $(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] : \gcd(a, n) = 1\}$ has $\varphi(n)$ elements
- If $(A, +)$ is an abelian group, then $\mathrm{End}(A)^\times = \mathrm{Aut}(A)$
- A nonzero element $a$ of a commutative ring $R$ is called a *zero divisor* iff there exists a nonzero element $b$ in $R$ such that $ab = 0$

## 1.2 1/10/2024 lecture

### 1.2.1 Integral domains & subrings

If $R$ is a nonzero commutative ring with no (nonzero) zero divisors, we call it an *integral domain* (or sometimes just *domain* for short). In an integral domain, mulltiplication by any nonzero element is an injection. If $R$ is finite, an injection from $R$ to itself is invertible, so $R$ is a field. However, not every integral domain is a field – for example, $\mathbb{Z}$ is a domain but not a field.

A subset $S$ of a ring $R$ is called a *subring* iff

- For any $a, b \in S$, $a + b, ab$, and $-a$ are also in $S$
- $S$ contains 1, and $1_S = 1_R$.

If $S$ is a subring of $R$, then $(S, +)$ is a subgroup of $(R, +)$.

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ is a sequence of subrings.

The set of $n \times n$ matrices of the form

$$\begin{bmatrix} * & 0 \\ 0 & 0 \end{bmatrix}$$

is a ring and is also a subset of $M_2(\mathbb{R})$, but is not a subring of $M_2(\mathbb{R})$, because they do not have the same multiplicative identity element.

### 1.2.2 Ring homomorphisms

If $R$ and $S$ are rings, a map $f : R \to S$ is called a *ring homomorphism* iff

- $f(a + b) = f(a) + f(b)$ (that is, $f$ is a group homomorphism)
- $f(ab) = f(a)f(b)$
- $f(1_R) = 1_S$

If $S$ is a subring of $R$, then the inclusion map from $S$ to $R$ is a ring homomorphism.

A ring homomorphism is called a *ring isomorphism* iff it is bijective.

In **Ring**, $\mathbb{Z}$ is the initial object and 0 is the terminal object.

The map from $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ (for $n \in \mathbb{N}, n > 1$) which takes $a$ to $[a]_n$ is a ring homomorphism.

One can show that there is no ring homomorphism from $\mathbb{Q}$ to $\mathbb{Z}$.

### 1.2.3 Ideals

If $I$ is a subset of a ring $R$, we call $I$ a *left ideal* iff

- $I$ is closed under addition ($I + I \subset I$)
- For any $a \in I, x \in R$, $xa$ is also in $I$ ($I$ is closed under left multiplication by any element of $R$, so $R \cdot I \subset I$)

- $I \neq \emptyset$ (we can use this to show that $0 \in I$)

The definition for a *right ideal* is the same, but with left multiplication replaced by right multiplication. A two-sided ideal is simply called an *ideal*.

Every ring has at least two ideals (itself, which is called the "unit ideal", and the zero ring), except for the zero ring (in which case those are the same). If $R$ is a field, those are the only ideals. Conversely, if $R$ is a commutative ring whose only ideals are 0 and $R$, then $R$ is a field.

For any $a \in R$, $Ra$ is a left ideal and $aR$ is a ring ideal. These are called the *principal left and right (respectively) ideals generated by $a$*. Every ideal of $\mathbb{Z}$ is principal, so we say that $\mathbb{Z}$ is a *principal ideal domain (PID)*.

In $M_n(\mathbb{R})$, the set of $n \times n$ real matrices with zeros everywhere except the first column is a left ideal.

If a left or right ideal $I$ of $R$ contains 1, then $I = R$. This is why we call $I$ the "unit ideal". More generally, if $I$ contains any invertible element (that is, $\exists u \in I \cap R^\times$), then $I = R$.

If $I_\alpha$ is a (possibly infinite) set of left (right) ideals, then $\cap_\alpha I_\alpha$ is a left (right) ideal. Also,

$$\sum_\alpha I_\alpha = \left\{ \sum_\alpha x_\alpha : x_\alpha \in I_\alpha, \text{ all except finitely many } x_\alpha \text{ are zero} \right\}$$

(the subgroup generated by $I_\alpha$) is the smallest ideal containing all $I_\alpha$.

For any elements $a_1, a_2, \ldots, a_n \in R$, we call $Ra_1 + Ra_2 + \cdots + Ra_n$ the *left ideal generated by $a_1, \ldots, a_n$*. Replacing $Ra_i$ by $a_iR$, we get the *right ideal generated by the $a_i$s.*

For any ring homomorphism $f : R \to S$, the kernel of $f$ is an ideal of $R$, and the image of $f$ is a subring of $S$.

## 1.3 1/12/2024 lecture

### 1.3.1 Quotient rings

If $I \subset R$ is an ideal and $a, b \in R$, then we say that $a$ and $b$ are *congruent* ($a \cong b \pmod I$) iff $b - a \in I$. If $a_1 \cong b_1 \pmod I$ and $a_2 \cong b_2 \pmod I$, then $a_1 + a_2 \cong b_1 + b_2 \pmod I$ and $a_1 a_2 \cong b_1 b_2 \pmod I$.

The set of cosets of $I$, $\{a + I \in R/I : a \in R\}$, is also a ring, called the *quotient ring* or the *factor ring*. $\mathbb{Z}/n\mathbb{Z}$ (for some natural number $n > 1$) is a classic example of a quotient ring.

For any ideal $I \subset R$, we can show that the canonical map $\pi : R \to R/I$ given by $\pi(a) = a + I$ is a surjective ring homomorphism, with $\operatorname{Ker}(\pi) = I$.

If $f : R \to S$ is a ring homomorphism, then we know that $\operatorname{Im}(f)$ is a subring of $S$ and $\operatorname{Ker}(f)$ is an ideal of $R$. The *first isomorphism theorem for rings* says that the map $\overline{f} : R/\operatorname{Ker}(f) \to \operatorname{Im}(f)$ defined by $\overline{f}(a + \operatorname{Ker}(f)) = f(a)$ is not only a group homomorphism, but also a ring homomorphism.

Consider the function $f : \mathbb{R}[x] \to \mathbb{C}$ defined by $f(h) = h(i)$. This is a surjective ring homomorphism, and the kernel of $f$ is the set of polynomials for which $i$ is a root. Since $f$ is real, it is invariant under complex conjugation, so a real polynomial $h$ is in $\operatorname{Ker}(f)$ iff it is divisible by both $x - i$ and $x + i$. Therefore $\operatorname{Ker}(f) = (x^2+1)\mathbb{R}[x]$, so $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x] \cong \mathbb{C}$.

### 1.3.2 Product of rings

An element $e$ in any ring $S$ is called *idempotent* iff $e^2 = e$. For example, 0 and 1 are idempotent in any ring.

For a ring $R$ that is defined as the product of rings, $R := R_1 \times R_2 \times \cdots \times R_n$, the 0 element in $R$ is $(0_{R_1}, \ldots, 0_{R_n})$, and similarly, $1_R = (1_{R_1}, \ldots, 1_{R_n})$. If $e_1 \in R_1, e_2 \in R_2, \ldots, e_n \in R_n$ are idempotents, the $e_i$s are orthogonal (meaning $e_i e_j = 0$ when $i \neq j$), the $e_i$s are all central ($e_i x = x e_i$ for any $x \in R$), and their sum is $1_R$, then let the function $f : R \to Re_1 \times Re_2 \times \cdots \times Re_n$ be defined by $f(a) = (ae_1, \ldots, ae_n)$. We can prove that $f$ is an isomorphism.

Fun example: the quotient ring $\mathbb{Z}/10^n\mathbb{Z}$ is isomorphic to $\mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/5^n\mathbb{Z}$. By Bézout's identity, $\mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/5^n\mathbb{Z}$ contains the elements $(0, 0$, $(1, 0)$, $(0, 1)$, and $(1, 1)$, which are all idempotent – in fact, these are the only idempotent elements. Since that group is isomorphic to $\mathbb{Z}/10^n\mathbb{Z}$, we know that for any $n$, there are exactly 4 integers between 1 and $10^n$ whose square has the last same $n$ digits as the original number. Those are precisely the 4 numbers which are conguent to either 0 or 1 in both $\mathbb{Z}/2^n\mathbb{Z}$ and $\mathbb{Z}/5^n\mathbb{Z}$. Two of those numbers are boring (zero and one), but the other cases are interesting.

### 1.3.3 Chinese remainder theorem

Let $I$ and $Y$ be ideals of $R$. We say that they are *coprime* iff $I + Y = R$. For example, if $n$ and $m$ are relatively prime, then $n\mathbb{Z}$ and $m\mathbb{Z}$ are coprime.

If $I_1, I_2, \ldots, I_n$ are pairwise coprime ideals of a ring $R$, then for every tuple $(a_1, \ldots, a_n) \in R^n$, there exists $a \in R$ such that $a \cdot a_i = e_i$ (for each $i$), where $e_i$ is an idempotent element of $I_i$ (NOT SURE THIS IS CORRECT).