# MAT439: Commutative Algebra

Mahmudul Hasan Turjoy

Last updated: February 11, 2026

## Contents



## 1 Preface

These lecture notes were taken in the course MAT439: Commutative Algebra, taught by Nian Ibne Nazrul at BRAC University, as part of the BSc in Mathematics program in Spring 2026. Each lecture corresponds to a chapter in these notes.

Nothing in these notes is original (except my mistakes); almost everything here can be found somewhere in [AM69] or [Eis95]. In particular, we adopt the notation of [AM69] for notational consistency.

If you find any mistake, please report it at mh.turjoy@yahoo.com, even if it is something very small, even if you are not sure.

## 2 Abstract Algebra Review (2/2/26)

This lecture provides a brief review of some of the materials covered in MAT311: Abstract Algebra, with motivations and detailed explanations in definitions and proofs omitted.

### 2.1 Group Theory

**Definition 2.1** (Binary Operation)
Let $S$ be a nonempty set. A *binary operation* on $S$ is a map

$$* : S \times S \longrightarrow S.$$

We denote $*(x, y)$ by $x * y$.

**Definition 2.2**
Let $f : A \longrightarrow B$ be a map and let $C \subseteq A$. The *restriction of $f$ to $C$* is the map

$$f|_C : C \to B$$

defined by

$$f|_C(x) = f(x) \quad \text{for all } x \in C.$$

**Definition 2.3** (Group)
A *group* is an ordered pair $(G, *)$, where $G$ is a set and $*$ is a binary operation such that:

- **Associativity:** For all $g, h, k \in G$, $(g * h) * k = g * (h * k)$.
- **Identity element:** There exists an element $e \in G$ such that for all $g \in G$, $e * g = g = g * e$.
- **Inverse element:** For each $g \in G$, there exists an element $h \in G$ such that $g * h = e = h * g$.

If $(G, *)$ is a group, then we simply say $G$ is a group, when what $*$ is, is clear from the context. $G$ is called *abelian*[1] if $g * h = h * g$, for all $g, h \in G$.

**Proposition 2.4**
Let $(G, *)$ be a group. Then

- Identity element $e$ is unique.
- Inverse $h$ of an element $g \in G$ is unique. So we denote $h =: g^{-1}$.

After proving these results, we can use definite article "the" before identity element and inverse of a group element.

*Proof.*
- Suppose there are two identity elements $e_1, e_2$. Then

$$e_1 = e_1 * e_2 = e_2.$$

- Let $g \in G$ and suppose $h, k$ are two inverses of $g$. Then

$$h = h * e = h * (g * k) = (h * g) * k = e * k = k.$$

□

**Definition 2.5** (Subgroup)
Let $S$ be a subset of a group $(G, *)$, and $*|_{S \times S} : S \times S \longrightarrow G$ be the restriction of the map $*$. $S$ is called a *subgroup* of $G$ and denoted by $S \leq G$ if

- $e \in S$,
- For all $s \in S, s^{-1} \in S$,
- $\text{Im}(*|_{S \times S}) \subseteq S$.

In other words, if $(S, *|_{S \times S})$ is a group by itself.

One of the philosophies in mathematics in general is: to understand an object, you should study functions from that object. Following definition is important in that sense.

[1] Some people capitalize the letter "A" in honor of mathematician Niels Henrik Abel, who contributed enormously in the subject.

**Definition 2.6** (Group Homomorphism)
A map between groups $f : (G, *) \longrightarrow (H, \#)$ is called a *group homomorphism* if

$$f(g * h) = f(g)\#f(h) \quad \forall g, h \in G.$$

The set

$$\ker f := f^{-1}(\{e\}),$$

is called the *kernel* of $f$.

**Proposition 2.7**
$\ker f \leq G$.

*Proof.* We verify three conditions of a subring:

1.

$$\begin{aligned}
& f(e_G) = f(e_G * e_G) = f(e_G)\#f(e_G) \\
\Longrightarrow\ & f(e_G)\#(f(e_G))^{-1} = (f(e_G)\#f(e_G))\#(f(e_G))^{-1} \\
\Longrightarrow\ & f(e_G)\#(f(e_G))^{-1} = f(e_G)\#(f(e_G)\#(f(e_G))^{-1}) \\
\Longrightarrow\ & e_G = f(e_G) \\
& \therefore e_G \in \ker f.
\end{aligned}$$

2. Let $s \in \ker f$, then $f(s) = e_H$. Then

$$\begin{aligned}
& f(s * s^{-1}) = f(e_G) = e_H \\
\Longrightarrow\ & f(s)\#f(s^{-1}) = e_H \\
\Longrightarrow\ & e_H\#f(s^{-1}) = e_H \\
\Longrightarrow\ & f(s^{-1}) = e_H \\
& \therefore s^{-1} \in \ker f.
\end{aligned}$$

3. Let $K = \ker f$ and $s \in \operatorname{Im}(*|_{K \times K})$. Then there exists $(r, t) \in K \times K$ such that $r * t = s$. We have to prove $s \in K$.

$$f(s) = f(r * t) = f(r)\#f(t) = e_H\#e_H = e_H.$$

Therefore, $\operatorname{Im}(*|_{K \times K}) \subseteq K$.

□

**Proposition 2.8**
For all $g \in G$, $g\ker f = \operatorname{kef} f g$.

Generalising kernel using this key property, we define the following:

**Definition 2.9** (Normal Subgroup)
A subgroup $N$ of a group $G$ is called *normal* if $gN = Ng$ for all $g \in G$. We denote it by $N \trianglelefteq G$.

**Definition 2.10** (Coset)
Let $H \leq (G, *)$. Then for an element $g \in G$, the set

$$gH := \{g * h : h \in H\},$$

is called a *left coset* of $G$. Similarly,

$$Hg := \{h * g : h \in H\},$$

is called a *right coset*.

**Definition 2.11** (Quotient Group)
Let $N \trianglelefteq G$. Then

$$G/N := \{gN : g \in G\},$$

is a group with group operation $\cdot$ given by

$$(gN) \cdot (hN) = (gh)N.$$

We call it a *quotient group*.

The map $\pi : G \longrightarrow G/N$ given via $g \mapsto gN$ is a group homomorphism. It is called *quotient map*. Kernel of this map is $N$. Hence,

**Theorem 2.12**
Any normal subgroup $N$ of a group $G$ can be written as the kernel of some group homomorphism.

**Theorem 2.13** (1st Isomorphism Theorem)
Let $f : G \longrightarrow H$ be a group homomorphism. Then $G/\ker f$ is isomorphic to $\operatorname{Im} f$ by the isomorphism given via $g\ker f \mapsto f(g)$.

## 2.2 Ring Theory

**Definition 2.14** (Ring)
A *ring* is a datum $(R, +, \cdot)$, where $R$ is a set and $+, \cdot$ are binary operations such that:

- $(R, +)$ is an abelian group (so $R$ has an identity element[a] denoted by $0$.
- $(g \cdot h) \cdot j = g \cdot (h \cdot j), \forall g, h, j \in R$.
- $g \cdot (h + j) = g \cdot h + g \cdot j$ and $(h + j) \cdot g = h \cdot g + j \cdot g, \forall g, h, j \in R$.

[a]We call it additive identity in the context of rings.

If there exists an element $1 \in R$ such that for all $x \in R, x \cdot 1 = x = 1 \cdot x$, then $1$ is called *multiplicative identity* and $R$ is called a *ring with identity*. In this course, we are primarily interested in commutative[2] rings with identity. So, from now on, every ring in these notes is a commutative ring with identity unless stated otherwise.

**Proposition 2.15**
If additive and multiplicative identities of a ring $R$ are equal, then $R$ is the trivial ring, i.e., $R = \{0\}$.

*Proof.* Let $x \in R$, then

$$x = x \cdot 1 = x \cdot 0 = 0 \implies R = \{0\}.$$

□

[2]As the name of the course suggests XD

**Definition 2.16** (Ring Homomorphism)
Suppose $(R_1, +_1, *_1)$ and $(R_2, +_2, *_2)$ are two rings. Then a map $f : (R_1, +_1, *_1) \longrightarrow (R_2, +_2, *_2)$ is called a *ring homomorphism* if

- $f(a +_1 b) = f(a) +_2 f(b)$,
- $f(a *_1 b) = f(a) *_2 f(b)$,
- $f(1_{R_1}) = 1_{R_2}$.

**Exercise 2.17**
To show that the third condition of the ring homomorphism is independent of the other twos, find an example of a map between two rings that satisfies first two conditions, but not the third one.

**Answer** (Instructor). *An example that satisfies the conditions $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ but not $f(1) = 1$ is the map $f : (\mathbb{Z}, +, *) \to (\mathbb{Z}, +, *)$, $f(n) = 0$ for all $n$, i.e. the zero map. $f(a+b) = 0 = 0 + 0 = f(a) + f(b)$, $f(ab) = 0 = 0 \times 0 = f(a)f(b)$, but $f(1) = 0 \neq 1$.*

**Definition 2.18** (Subring)
Suppose $S \subseteq R$ where $(R, +, \cdot)$ is a ring. If $(S, +|_{S\times S}, *|_{S\times S})$ is a ring by itself, then $S$ is called a subring of $R$.

**Definition 2.19** (Ideal)
An *ideal* $I$ of a ring $R$ is a subset of $R$ and satisfies:

- $I$ is a subgroup of $(R, +)$,
- Let $IR := \{i \cdot r : i \in I \text{ and } r \in R\}$. Then $IR \subset I$.

**Example 2.20** (Principle Ideal)
Suppose $a \in R$. Then $(a) := \{a \cdot r : r \in R\}$ is an ideal, also called as *principle ideal* or ideal generated by $a$.[a]

[a] It seemed like every non-trivial ideal should be of this form. But Ernest Kummer first discovered ideals that were not generated by a single element, which exploded the subject.

**Example 2.21**
$R = \mathbb{Z}$ has an infinite number of ideals, explicitly

$$I = (n) = n\mathbb{Z}, \quad \forall\, n \geq 0.$$

In fact, every ideal of $\mathbb{Z}$ is of this form[a]. For all $n \in \mathbb{Z}$, $(n)$ is an ideal of $\mathbb{Z}$. We now prove the converse.

Let $P$ be an ideal of $\mathbb{Z}$. If $P = \{0\}$, then $P = (0)$.

Assume $P \neq \{0\}$. Since $P \leq \mathbb{Z}$, there exists a positive integer in $P$. Let

$$n = \min\{\, k \in P \mid k > 0 \,\}.$$

We claim that $P = (n)$. Since $n \in P$ and $P$ is an ideal, for any $z \in \mathbb{Z}$,

$$zn \in P,$$

hence $(n) \subseteq P$.

Conversely, let $p \in P$. By the Euclid's Division lemma, there exist $q, r \in \mathbb{Z}$ such that

$$p = qn + r, \quad 0 \leq r < n.$$

Since $p \in P$ and $qn \in P$, and $P$ is an ideal, we have

$$r = p - qn \in P.$$

By the minimality of $n$, it follows that $r = 0$. Hence

$$p = qn \in (n),$$

and therefore $P \subseteq (n)$.

Thus,

$$P = (n).$$

[a] It is very rare that when you have a ring, you can list all of its ideals.

**Example 2.22** (Polynomial Ring)
Let $R$ be a ring, $x$ be an indeterminate and define $R[x]$ be the set of all formal sums of the form

$$\sum a_i x^i = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad \text{where } \{i : a_i \neq 0\} \text{ is finite.}$$

Given two polynomials $f = \sum a_i x^i$ and $g = \sum b_i x^i$ in $R[x]$, the sum of $f$ and $g$ is defined as

$$f + g = \sum (a_i + b_i) x^i,$$

and the product of $f$ and $g$ as

$$f \cdot g = \sum c_i x^i, \quad \text{where } c_i = \sum_{j,k : j+k=i} a_j b_k.$$

With this rule of addition and multiplication, $(R[x], +, \cdot)$ becomes a ring, called *polynomial ring*.[a] We can further define polynomial ring $R[x][y]$ over $R[x]$ and it turns out that $R[x][y] \cong R[x,y]$[b]. Some of the ideals of the ring $R[x,y]$ are:

- $\langle x \rangle = \{xf(x,y) : f(x,y) \in R[x,y]\} = \{\text{All the polynomials with degree of } x \textit{ at least } 1\}$.
- $\langle x, y \rangle = \{xf(x,y) + yg(x,y) : f, g \in R[x,y]\} = \{\text{All the polynomials with degree of no constant term}\}$.

[a] In the definition above, each $a_i \in R$ is called the coefficients of the polynomial; $a_i$ is the coefficient of $x^i$ and the zero element given as the polynomial with zero coefficients.
[b] Polynomial ring of several indeterminates is not defined here though.

## 3 Ideals (09/02/26)

**Proposition 3.1**
Let $\mathbb{K}$ be a field. Then every ideal of $\mathbb{K}[x]$ is principle, but it is not true in general in $\mathbb{K}[x_1, \cdots, x_n]$ for $n > 1$.

*Proof.* We proceed similarly as in we did in the case of $\mathbb{Z}$. But before that, we have to prove analogous Euclid's Division lemma for $\mathbb{K}[x]$.

**Claim 3.2.** *Let $f, g \in \mathbb{K}[x]$. If $g \neq 0$, then there exists polynomials $q, r \in \mathbb{K}[x]$ such $f = gq + r$, where $\deg r < \deg g$.*

*Proof of claim.* If $g$ divides $f$, then $r = 0$ and we are done. If not, let $r = f - gq$ be the polynomial of least degree among all polynomials of the form $f - lg$ with $l \in \mathbb{K}[x]$. Then we must have $\deg g > \deg r$. Otherwise, let the leading term of $r$ and $g$ be $ax^m$ and $bx^n$ respectively. Then

$$r - g \cdot ab^{-1}x^{m-n} = f - gq - g \cdot ab^{-1}x^{m-n} = f - g(q + ab^{-1}x^{m-n}),$$

has smaller degree than $r$ and is of the given form, which contradicts minimality of the degree of $r$. □

If $f \in \mathbb{K}[x]$, then $(f)$ is an ideal. Conversely, if $I$ is an ideal of $\mathbb{K}[x]$, we claim that $(g) = I$, where $g$ is a polynomial of least positive degree in $I$. Clearly, $(g) \subseteq I$. Let $f \in I$, then by the Claim 3.2, there exists $q, r \in \mathbb{K}[x]$ such that

$$f = gq + r, \quad \text{where } \deg r < \deg g.$$

Here $r = 0$, otherwise, $r = f - gq \in I$, which contradicts the minimality of the degree of $g$. Hence, $f = gq \in (g)$, which implies $I \subseteq (g)$. Therefore, $I = (g)$.

However, in general, in $\mathbb{K}[x_1, \cdots, x_n]$ for $n > 1$, every ideal is not principle. As counter-example, we can consider the finitely generated ideal $(x_1, x_2)$. □

## 3.1 Quotient Ring

**Definition 3.3** (Quotient Ring)
Suppose $R$ is a (commutative) ring (with identity), and suppose $I$ is an ideal of $R$. So, $I$ is an additive subgroup of the abelian group $(R,+)$[a]. $R/I$ is a quotient group where elements look like $r+I$. Define multiplication on $R/I$:

$$(r+I)\cdot(r'+I) = rr'+I.$$

Then $(R/I,+,\cdot)$ becomes a ring called *quotient ring* of R modulo $I$.

[a] For an abelian group, every subgroup is normal, $r+H = H+r$.

Since cosets of an additive group $(R,+)$ can have multiple representatives, we have to check well-definedness of the multiplication defined above, i.e., if $r+I = h+I$ and $r'+I = h'+I$, then $(r+I)\cdot(r'+I) = (h+I)\cdot(h'+I)$. Notice, $r+I = h+I$ and $r'+I = h'+I \Leftrightarrow r-h \in I$ and $r'-h' \in I$. Since $I$ is an ideal,

$$(r-h)r' \in I \implies rr' - hr' \in I \text{ and}$$

$$h(r'-h') \in I \implies hr' - hh' \in I.$$

Since $I$ is an additive subgroup,

$$\begin{aligned}
&(rr'-hr') + (hr'-hh') \in I \\
\implies &rr' + (-hr' + hr') - hh' \in I \\
\implies &rr' - hh' \in I \\
\implies &rr' + I = hh' + I \\
&\therefore (r+I)\cdot(r'+I) = (h+I)\cdot(h'+I).
\end{aligned}$$

Associativity, distributive property, existence of identity (which is $0+I = I$) and commutativity of $(R/I,+,\cdot)$ are routine checks.

**Student Question**
Can we take quotient modulo an ideal of a non-commutative ring?

**Answer** (Instructor). *Yes, we can! In that case, the ideal should be two-sided ideal. Recall, in a non-commutative ring $R$, an additive subgroup $I$ of $R$ is called a* left ideal *if $RI \subseteq I$ and* right ideal *if $IR \subseteq I$. If $I$ is both left and right ideal, then we call it a* two-sided ideal. *For example,* ***to be written....***

**Proposition 3.4**
Suppose $R$ is a ring and $I$ is is an ideal. Then there is an $1-1$ order-preserving correspondence between the ideals of $R$ containing $I$ and the ideals of the quotient ring $R/I$. The order-preserving $1-1$ correspondence is given by: if $J'$ is an ideal of $R/I$, then the corresponding ideal in $R$ is given by $\pi^{-1}(J')$.[a]

[a] $\pi$ is the canonical projection map that maps each element $r$ of $R$ to $r+I$ in $R/I$.

*Proof.* Step (1). First we show that if $J'$ is an ideal of the quotient $R/I$, then $\pi^{-1}(J')$ is an ideal in $R$.

Firstly, $0 \in \pi^{-1}(J')$, because $\pi(0) = I \in J'$ as $J'$ is an ideal of $R/I$, so it must contain the additive identity $I$ of $R/I$.

Suppose $x, y \in \pi^{-1}(J')$. So $\pi(x) = x+I, \pi(y) = y+I \in J'$. Since $J'$ is an ideal, we have

$$\begin{aligned}
&(x+I) - (y+I) \in J' \\
\implies &(x-y) + I \in J' \\
\implies &\pi(x-y) \in J' \\
\implies &(x-y) \in \pi^{-1}(J').
\end{aligned}$$

Hence, using subgroup criterion, $pi^{-1}(J')$ is an additive subgroup of $R$.

Also, if $r \in R$, then $r \cdot \pi^{-1}(J') \subseteq \pi^{-1}(J')$. To see that, suppose $x \in \pi^{-1}(J')$, which implies $x + I \in J'$, which implies $(r+I)(x_I) \in J'$ as $(r+I) \in R/I$, and that implies

$$rx + I \in J' \implies \pi(rx) \in J' \implies rx \in \pi^{-1}(J').$$

$\therefore \pi^{-1}(J')$ is indeed an ideal of $R$.

Step (2). We want to show that if $J'$ is an ideal of $R/I$, then the ideal $J = \pi^{-1}(J')$ of $R$ contains $I$.

Let $x \in I$, then $\pi(x) = I \in J'$, which implies $x \in \pi^{-1}(J')$. Therefore, $\ker \pi = I \subseteq \pi^{-1}(J')$.

Step (3). Lastly, we have to prove **to be written...**

□

**Definition 3.5**
Let $R$ be a ring.

An element $r \in R$ is called a *zero-divisor* if there is a non-zero $y \in R$ such that $r \cdot y = 0$.

$R$ is called an *integral domain* if it does not have any non-zero zero-divisors.

An element $r \in R$ is called *nilpotent* if $r^n = 0$ for some $n > 0$.

A *unit* $r \in R$ is an element that "divides 1" – i.e., for which there exists $y \in R, y \neq 0$ such that $xy = 1$.

$R$ is a *field* if $1 \neq 0$ and every non-zero element is a unit.

**Note 3.6**
- 0 is also a zero-divisor.
- Nilpotent elements are all zero-divisors. To see that, suppose $r$ is a nilpotent element and $r^n = 0$. If $n = 1$, then $r$ is trivially zero-divisor. Otherwise, we have $r^{n-1} \in R$ such that $r \cdot r^{n-1} = 0$.
- The set of all units of a ring $R$ forms an abelian group under multiplication and it is denoted by $R^\times$.
- A unit cannot be a zero-divisor in $R \neq (0)$. Suppose $x$ is a unit with $xy = 1$. If $x$ is also a zero-divisor, $sx = 0$ for some $s \neq 0$.

$$sx = 0 \implies (sx)y = 0y \implies s(xy) = 0 \implies s \cdot 1 = 0 \implies s = 0 \text{ (contradiction!)}.$$

So,
- A field is an integral domain.

**Proposition 3.7**
Suppose $R$ is a ring and $R \neq (0)$. Then the following are equivalent:

1. $R$ is a field.
2. $R$ only has two ideals: (0) and $(1)$.
3. Every homomorphism[a] of $R$ to a non-zero ring is injective.

[a]Remember we require $f(1) = 1$ for a ring homomorphism $f$.

*Proof.*
- (1) $\implies$ (2). Suppose $R$ is a field. That means, every non-zero element is a unit. Let $I$ be an ideal of $R$. If $I = (0)$, we are done. Otherwise, there exists non-zero $x \in I \subseteq R$. Hence, $x$ is a unit, i.e., there exits $y \in R$ such that $xy = yx = 1$. Since $I$ is an ideal, $y \cdot x \in I \implies 1 \in I \implies I = (1) = R$.
- (2) $\implies$ (3). Suppose $R$ has only two ideals: $(0)$ and $(1)$. And let $f : R \longrightarrow S \neq (0)$ be a ring homomorphism. $\ker f$ is an ideal of $R$, and it can be either $(0)$ or $(1)$ as per hypothesis. But $\ker f \neq R$ since we at least have $1_R \neq \ker f$ by definition. Hence, $\ker f = (0)$, which implies $f$ is injective[3].

[3]Recall from the first course in algebra: A ring homomorphism is injective iff its kernel is $(0)$.

- (3) $\implies$ (1). Suppose every homomorphism of $R$ to a non-zero ring is injective. We want to show that $R$ is a field, i.e., every non-zero element is a unit. Suppose there is an element $x \in R$ which is not a unit. Then $(x) \neq (1)$ (because if it was $(1)$, then that would mean $y \cdot x = 1 \implies x$ is a unit).

  Consider the canonical projection map $\pi : R \to R/(x)$ for which $\ker \pi = (x)$. Since $(x) \neq (1)$, i.e., since $(x) \neq R, R/(x) \neq (0)$. So, $\ker \pi = (0)$ by hypothesis, which implies $(x) = (0) \implies x = 0$. Hence, the only non-unit in $R$ is 0, and so every non-zero element should be a unit.

$\square$

# 4 References

# References

[AM69] Michael Francis Atiyah and Ian G. MacDonald. *Introduction to Aommutative Algebra*. Addison-Wesley Publishing Company, 1969.

[Eis95] David Eisenbud. *Commutative Algebra: with a View Toward Algebraic Geometry*. New York: Springer-Verlag, 1995. ISBN: 978-0387942681.