MAT439: Commutative Algebra

Mahmudul Hasan Turjoy

Last updated: February 6, 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); 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 $s \in S, s^{-1} \in S$,
- $\mathrm{Im}(*|_{S \times S}) \subseteq S$.

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.

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.

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

Proposition 2.7
$\ker f \leq G$.

Proof. We verify three conditions of a subring:

1.

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

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

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

3. Let $K = \ker f$ and $s \in \mathrm{Im}(*|_{K \times K})$. 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, $\mathrm{Im}(*|_{K \times K}) \subseteq K$.

□

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

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 $\mathrm{Im} f$ 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

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

□

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

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

[2] As the name of the course suggests XD

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.

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 division algorithm, 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:

- $\langle x \rangle = \{xf(x,y) : f(x,y) \in R[x,y]\} = \{$All the polynomials with degree of x *at least* $1\}$.
- $\langle x,y \rangle = \{xf(x,y) + yg(x,y) : f,g \in R[x,y]\} = \{$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 References

References

[AM69] Michael Francis Atiyah and Ian G. MacDonald. *Introduction to commutative 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.