Algebra III (Ring Theory)

Notes by Arjun Maneesh Agarwal

based on course by Clare D Cruz

Quiz 1 will be on 1st Monday of September aka 1st September

Tutorial is on every Monday.

Table of Contents

1. Dumb thing Clare says

"The most importent ring in CMI is **SUFFE-RING**. CMI kids have everything and they still complain, remember you are privlagged. I saw a kid who works in ice cream shop and then in evening goes to Loyala collage, he doesn't complain. You all shouldn't."

2. Ring Theory

Definition: Ring

A ring R is a non-empty set with operations (denoted by $+$ and $\cdot$) such that:

1. $(R, +)$ is an abelian group
2. (Associativity) $a \cdot (b \cdot c) = (a \cdot b) \cdot c \forall a, b, c \in R$
3. (Distributive) $a \cdot (b + c) = a \cdot b + a \cdot c \forall a, b, c \in R$
4. (Ring with Unity) $\exists 1_R$ s.t. $1_R \cdot a = a \cdot 1_R = a \forall a \in R$

Definition: Subring

Given a ring $S \subseteq R$ with closure property wrt $+, \cdot$ is called a subring.

Side Note

We normally assume $1_R \neq 0_R$ as otherwise, we will have a 0 ring.

Definition: Units of R

The units of R are

$$\{r \in R \mid \exists s \, s.t. \, rs = 1_R\}$$

Side Note

$\forall a \in R, n \in \mathbb{N}$, we denote by:

- $na = \underbrace{a + a + \ldots + a}_{n \text{ times}}$
- $-na = -(na)$

Lemma 2.1.

1. $0 \cdot a = a \cdot 0 = 0 \forall a \in R$

2. $(-a)b = a(-b) = -(ab) \forall a, b \in R$

3. $(-a)(-b) = ab \forall a, b \in R$

4. $(na)b = a(nb) = n(ab) \forall a, b \in R, \forall n \in \mathbb{N}$

5. $$\left(\sum_{i=1}^{n} a_i\right) \cdot \left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j$$

Proof.

1. $0 \cdot a = (0 + 0) \cdot a = (0 \cdot a) + (0 \cdot a) \Rightarrow 0 \cdot a = 0$
2. $(-a) \cdot b + a \cdot b = (-a + a) \cdot b = 0 \cdot b = 0$ by 1
3. Follows from 2
4. Follows from distibutivity and induction.
5. Follows from induction.

■

Definition: Zero Division

An element $a \in R$ is a left zero divisor if there exists a non-zero element $b \in R \, s.t. \, ab = 0$.

An element $a \in R$ is a left zero divisor if there exists a non-zero element $c \in R \, s.t. \, ca = 0$.

Definition: Multiplicative Inverse

An element $a \in R$ is left (rep. right) invertible if $\exists c \in R$ (rep. $b \in R$) $s.t.$ $ca = 1$ (rep. $ab = 1$).

a is invertible if it is both left and right invertible.

Lemma 2.2. *For an invertible $a \in R$, it's left and right inverses are equal.*

Proof. Let $ab = 1 = ca$, then:

$$\begin{aligned} b = 1b &= (ca)b \\ &= c(ab) \\ &= c1 \\ &= c \end{aligned}$$

■

Lemma 2.3. *The set of units form a group under multiplication say* $(U(R), \cdot)$

Proof. Do at home! ■

Definition: Division Ring

A ring m which every non-zero element is a unit is a division ring.

Definition: Field

A commutative division ring is a field.

Definition: Ideals

$I \subseteq R$ is an ideal if
1. $(I, +)$ is an abelian group.
2. Left Ideal (rep. right ideal) if $\forall r \in R, x \in I, rx \in I$ (rep. $xr \in I$)

Definition: Homorphims

If R, S are rings, a map $f : R \to S$ is a homorphism if

$$\forall a, b, c \in R$$

- $(a +_R b) = f(a) +_S f(b)$
- $f(a \cdot_R b) = f(a) \cdot_S f(b)$
- $f(1_R) = 1_S$

The last bullet is not part of the true definition, but it being violated leads to pathological and rather impractical stuff.

Definition: Kernal and Image

$$\ker f = \{r \in R \mid f(r) = 0\}$$

[1]We don't take $f(r) = 1$ as 1 is not always present and homorphisms should have kernals, such definition opens us ip to a lot of weirdness.

1

$$\operatorname{im} f = \{s \in S \mid \exists r \in R \, s.t. \, f(r) = s\}$$

Lemma 2.4. $\ker f$ *is an ideal in* R.

$\operatorname{im} S$ *is a subring of* S.

Definition: Ring Quoitent

$\frac{R}{I} = \{a + I \mid a \in R\}$

Definition: Addition and Multiplication in R/I

$$(a + I) + (b + I) = (a + b) + I$$
$$(a + I)(b + I) = ab + I$$

Lemma 2.5. *If* I *is a two sides ideal, then* $\frac{R}{I}$ *is a ring.*

Proof. Verify thr properties. ■

Definition: Center

The center of a ring R is:

$$C(R) = \{c \in R \mid cr = rc \forall r \in R\}$$

Theorem 2.6. *The center* $C(R)$ *is a subring of* R

Definition: Module

A left R module M ia an additive abelian group with the operation

$$R \times M \to M$$
$$r, m \mapsto rm$$

satisfying:
1. $(r + s)m = rm + sm \forall m \in M; r, s \in R$
2. $r(m + n) = rm + rn \forall m, n \in M; r \in R$
3. $(rs)m = r(sm)$
4. $1m = m$

A right R module M ia an additive abelian group with the operation

$$M \times R \to M$$
$$m, r \mapsto mr$$

satisfying:
1. $m(r+s) = mr + ms \forall m \in M; r, s \in R$
2. $(m+n)r = mr + nr \forall m, n \in M; r \in R$
3. $(mr)s = m(rs)$
4. $m1 = m$

Assuming $1 \in R$.[2]

Definition: Inregration Domain

A ring R such that $\forall r, s \in R; rs = 0 \Rightarrow r = 0$ or $s = 0$ aka if it has no non-zero zero divisors.

Definition: Division Ring

A ring R whoch evert non-zero element is invertible is a division ring.

Definition: Field

A commutative division ring is a field.

Side Note

In an integral domain.

$$S \subseteq R \text{ is a subring}$$
$$1_S \in S, 1_R \in R \text{ are the identities}$$
$$1_S \cdot 1_S = 1_S \in S, R$$
$$1_S \cdot 1_R = 1_R \in R$$
$$1_S 1_S - 1_S 1_R = 0$$
$$1_{S(1_S - 1_R)} = 0$$
$$1_S = 1_R$$

This implies that we havea natuataal homomorphism $\varphi : S \to R$, $s \mapsto r$.

$\varphi(1_S) = 1_R = 1_S \Rightarrow 1_S \mapsto 1_R, 1_S = 1_R$

[2]Is sometimes not considered in rings, atleast in old books for more genrality. We shall take this as true to avoid ideals becomming rings.

2.1. Some Special Rings

Example : On $\mathbb{Z}$

What are the ideas in $\mathbb{Z}$?

Wrt $+, n\mathbb{Z}$ is a subgroup $(n \in \mathbb{Z})$.

<u>Need to see</u> $\forall r \in \mathbb{Z}$ and $\alpha \in \mathbb{Z}, \alpha \in n\mathbb{Z}$.

$$r(n\alpha) \in n\mathbb{Z}$$
$$\|$$
$$n(r\alpha)$$
$$\Rightarrow nZ \text{ is an ideal!}$$

Proper ideas in $\mathbb{Z}$ are of the form $n\mathbb{Z}$ where $n \neq \pm 1$. $\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$.

$(\frac{\mathbb{Z}}{n\mathbb{Z}}, +$ is a group.

$(i + n\mathbb{Z})(j + n\mathbb{Z}) = ij + n\mathbb{Z}$

$\frac{\mathbb{Z}}{n\mathbb{Z}}$ is an integral domain and a field $\Leftrightarrow n$ is prime.

Example : $\mathbb{Z}$ and $\frac{\mathbb{Z}}{p\mathbb{Z}}$

In $\mathbb{Z}$, if we take any $r \neq 0$, $\underbrace{r + r + ... + r}_{nr \neq 0 \forall n > 0}$.

In $\frac{\mathbb{Z}}{p\mathbb{Z}}$, adding $\overline{r}, p$ times will give zero.

Definition: Characteristic of a Ring

The characteristic of a ring is the smallest integer $n > 0$ s.t. $nr = 0 \forall r \in R$. If $nr \neq 0 \forall n > 0$, we say $\text{char}(R) = 0$. For example, $\text{char}(\mathbb{Z}) = 0$

$\text{char}\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right) = p$ $\text{char}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right) = n$

Definition: Polynomial Rings

Let R be a ring and $x_1, x_2, ..., x_n$ be variables.

We define

$$S = R[X_1, ..., X_n] = \sum \alpha_{(i_1, i_2 ..., i_n)} x_1^{i_1} x_2^{i_2} ... x_n^{i_n}$$

Theorem 2.7. *If R is a field, $R[X_1, ..., X_n]$ is an integral domain.*

Theorem 2.8. $1_R = 1_S$

Side Note

R is a subring of S aka constent polynomials.

Example

$$S = R[X]$$
$$\Rightarrow f \in S \Rightarrow f(x) = a_0 + a_1 x + \ldots + a_n x^n$$

Constent polynomials are of the form $f(x) = a_0$.

Example : Ideals in $Z[X]$

TODO. *by prof!!!*

Remark

If R is a ring then, for $x \in R$, (x^i) is an ideal where i ranges over $\mathbb{N}$.

Question

If R is a ring and I is a two sided ideal, what are the ideals in $\frac{R}{I}$.

Remark

We have a natuataal homomorphism

$$\Pi : R \to \frac{R}{I}$$
$$r \mapsto r + I$$

If J is an ideal in R, then $\Pi(J) \in \frac{R}{I}$ is an idea in $\frac{R}{I}$ and is the ideal $\frac{J+I}{I} \rightsquigarrow$ an ideal in $\frac{R}{I}$.

We shall now ***verify*** that $\frac{J+I}{I}$ is an ideal.

1. $(a+b)+I = (a+I)+(b+I) = (b+I)+(a+I) = (b+a)+I$
$$\forall a, b \in J$$
2. Let $r + I \in \frac{R}{I}, a + I \in \frac{J+I}{I}$, then

$(r+I)(a+I) = \underbrace{ra}_{\in J} + I \in \frac{J+I}{I}$.

Definition

Let $\varphi : R \to S$ be a ring homomorphism.

Let I be an idea in R.

Consierr $(\varphi(I)) \cdot S$, the idea generated by $\varphi(I)$. This is called extension of the ideal I in S.

Let J be an idea in S.

Definition

$$K = \{r \in R \mid \varphi(r) \in J\}$$

Exercise

K is an ideal in R. C is called contraction o J.