MA-5101

ALGEBRA-II

10.08.2020

§1. Introduction

- Writing assignments
- Presentations → definitely will happen
- Might do quizzes via (Zoom) polls

- Best $n/n+2$ or something.
  (or $n/n+1$)

- What to recall from 419? → Rings, we'll start with def^n
  Should still be familiar

  Familiarity with Alg I also nice. Problem sets still should be sufficient

Won't define Integral Domains & Fields but will still use.
(Should be comfortable with 2^{nd} half of Basic Alg.)

maybe not UFDs but PIDs

(same link should go on.)

13.08.2020

$$\{\text{Subgroups of } \mathbb{Z}\} = \{n\mathbb{Z} : n \in \mathbb{Z}\}.$$

(precisely)

17 · 08 · 2020

LECTURE - 1

Def^n. (Ring) $(R, +, *)$ — a set R with binary operations $+$ and $*$ satisfying:

(i) $+$ is commutative. $\forall a, b \in R$: $a+b = b+a$

lets you add finitely many elements unambiguously

(ii) $+$ is associative. $\forall a, b, c \in R$: $a+(b+c) = (a+b)+c$

$$\begin{tikzcd} \underset{(a,b,c)}{R \times R \times R} \arrow[r, "id_R \times +"] \arrow[d, "+ \times id_R"'] \arrow[dr, phantom, "\circlearrowright"] & \underset{(a,\, b+c)}{R \times R} \arrow[d, "+"] \\ \underset{(a+b,\, c)}{R \times R} \arrow[r, "+"'] & R \end{tikzcd}$$

The diagram commutes

Existence of add. identity (iii) $\exists 0 \in R$: $\forall a \in R$: $a + 0 = a = 0 + a$ (No need to write this, though.)

Existence of add. inv. (iv) $\forall a \in R$: $\exists b \in R$: $a + b = 0$

(v) $*$ is associative. $\forall a, b, c \in R$: $a*(b*c) = (a*b)*c$

(vi) $*$ distributes over $+$.

$\forall a,b,c \in R$: $a*(b+c) = a*b + a*c$

$(b+c)*a = b*a + c*a$

Existence of $*$ id. (vii) $\exists 1 \in R$: $\forall a \in R$: $1*a = a = a*1$.

Shall always assume this in course!

Def^n. A ring $(R, +, *)$ is commutative if $*$ is commutative.

A ring in which every non-zero element has a multiplicative inverse is called a division ring.

Furthermore, a non-zero commutative ring is called a field if every non-zero element has a mult. inverse.

Examples / non-examples

1. $\{0\}$ is a ring. (The operations are forced.)

   (any singleton, in fact.)

   We call this the zero ring and simply denoted as 0.

2. $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ $\rightarrow$ standard operations

   $\mathbb{N}$: no, no 0
   ↳ $\mathbb{N} \cup \{0\}$ → no inverses

   $\mathbb{Z}$: ring, not field

   $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$: → a ring, in fact a field
   ↳ in fact, commutative

3. Let R be a ring. Then, $M_n(R)$ is a ring under the usual matrix operations.

   ↳ $\begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$ is the mult. identity.

4. $R[x]$ → set of polynomials with co-efficients in R

   $R[[x]]$ → set of formal power series in R

N. Jacobson "Algebra" → Section called "Rngs".

18·08·2020

LECTURE - 2

Let R be a ring.

Rings that can be constructed:

$R[x] \to$ polynomials

$R[[x]] \to$ power series

$A \neq \phi$, $\mathcal{F}(A,R) \to$ set of functions from A to R

$M_n(R) \to n\times n$ matrices with entries in R.

$R[x] = \{ f \mid \exists n \in \mathbb{N}\cup\{0\}, a_0, \dots, a_n \in R \ (f = a_0 + \dots + a_n x^n) \}$

where $a_0 + \dots + a_n x^n = a_0 + \dots + a_n x^n + 0 \cdot x^{n+1}$.

Moreover, two polynomials are equal if their like terms are equal.

Addition is term-wise.

Multiplication is the usual one: We define it this way to have $x^n \cdot x^m = x^{n+m}$ and distributivity.

Every element of R can be thought of as a polynomial.

$R[[x]] = \{ f \mid \exists a_0, a_1, \dots \in R \ (f = a_0 + a_1 x + \dots) \}$.

Equality is again term-wise.

Note that $f = 1 + x + x^2 + \cdots$ is a pow. series.

Also, $1, x, x^2, \dots$ are pow series

However, f cannot be written as a sum of infinitely many pow series!

(Only finite sums are defined in rings!)

$$(a_0 + a_1 x + \cdots)(b_0 + b_1 x + \cdots) = c_0 + c_1 x + \cdots$$

where $c_n = \sum_{i=0}^{n} a_i b_{n-i}$

$= a_0 b_n + a_1 b_{n-1} + \cdots + a_{n-1} b_1 + a_n b_0.$

$\mathcal{F}(A, R) = \{f : A \to R\}$ $\quad (A \neq \phi)$

For $f, g \in \mathcal{F}(A, R)$, we define $f+g \in \mathcal{F}(A,R)$ and $f*g \in \mathcal{F}(A,R)$ as

$$(f+g)(a) = f(a) + g(a), \qquad \forall a \in A$$

$$(f*g)(a) = f(a) * g(a).$$

$+$ and $*$ are from R.

20·08·2020

LECTURE - 3

Let R and S be rings. Then, $R \times S$ is a ring under Component-wise operations.

$$(r, s) + (r', s') := (r+r', s+s'),$$

$$(r,s) \cdot (r', s') := (r \cdot r', s \cdot s').$$

Similarly, can define $R_1 \times \cdots \times R_n$.

In particular, we can take $S = R$.

<u>Example</u>. $\mathbb{R} \times \mathbb{R}$ is a ring.

Is this the "same" as $\mathbb{C}$?

Def^n. (a) Given rings R and S, a function $\varphi: R \to S$ is a ring homomorphism if

① $\varphi(a+b) = \varphi(a) + \varphi(b)$
② $\varphi(ab) = \varphi(a)\varphi(b)$ $\Big\}\ \forall a,b \in R$
③ $\varphi(1) = 1$

(b) If $\varphi: R \to S$ is a homomorphism (ring map), then S is called an R-algebra via φ.

(c) Let $S \subset R$. We say that S is a subring of R if it is a ring under the same operations, and $1_S = 1_R$.

If $\varphi: S \to R$ is a 1-1 homomorphism, we often identify S with $\varphi(S)$ to consider S as a subring of R.

0 is not a subring of a non-zero ring R!

(d) Let $I \subset R$. We say that I is an ideal in R if:

① $\forall a,b \in I: a+b \in I$
② $0 \in I$
③ $\forall a \in I, \forall a \in R: ra \in I, ar \in I$

mimics subspace def^n in vector space

④ $\forall a \in I: -a \in I$
↳ don't need since our rings have 1

↳ also → quotienting

Since $(R,+)$ is abelian group, $I \trianglelefteq R$, we also want R/I to form a ring.

(Mimick $\mathbb{Z}/n\mathbb{Z}$.)

Consequence: If I is an ideal in R, then the quotient group R/I has a multiplicative structure induced from R.

That is, $\forall a, b \in R$

$$(a+I)(b+I) = (ab+I) \text{ is well defined}$$

elements of R/I

Furthermore, the natural map $\pi : R \to R/I$, $a \mapsto a+I$

is a ring homomorphism with $\ker \pi = I$.

Q: When is an ideal I a subring of R?

24·08·2020

LECTURE - 4

Recall: Let A be a non-empty set. $\mathcal{F}(A, R)$ is a ring under pointwise op.

$A = \mathbb{N}$, $R \to$ any ring; $\mathcal{F}(A, R) \to$ sequences in R

natural subring: eventually 0

$A = \mathbb{N}$, $R = \mathbb{R}$: $\mathcal{F}(\mathbb{N}, \mathbb{Q})$, Convergent seq., bdd seq. } natural subrings

(we saw this closure properties in analysis.)

$A = \mathbb{R}$, $R = \mathbb{R}$: $\mathcal{C}(\mathbb{R})$, $\mathcal{C}^\infty(\mathbb{R})$ $\to$ natural subrings

$A \to$ topological space, $R = \mathbb{R}$ or $\mathbb{C}$: $\mathcal{C}(A,R) \to$ cts functions from A to R.

If $A = R$, $\mathcal{F}(R) = \mathcal{F}(R,R)$.

↳ make it a ring → does composition and addition make it a ring?

if not, modify, put restrictions on R or take subsets (don't modify operations)

Eg. ① $\mathcal{C}([0,1], \mathbb{R})$

Think about what properties they have.

② $D^2 = \{ z \in \mathbb{C} : |z| < 1 \}$.

$H(D^2) \to$ set of analytic functions on D^2.

Def^n Let R be a ring, $a \in R$. We say that

① a is a unit if $\exists b \in R$ s.t. $ab = 1$ and $ba = 1$. $\mathcal{U}(R)$

② a is a zero divisor if $\exists b \in R \setminus \{0\}$ s.t. $ab = 0$ or $ba = 0$. $Z(R)$

[Note that 0 is a zero divisor iff $R \neq 0$.
Also, 0 is a unit iff $R = 0$.]

Q. Ring in which an elt has left inverse but no right

• an element is never a zero div. as well as unit.

③ a is nilpotent if $\exists n \in \mathbb{N}$ s.t. $a^n = 0$. $N(R)$

Assume $R \neq 0$. Are any of these subrings? Ideals?

can't be subrings, lol
↳ $1 \notin Z(R)$, $N(R)$
$0 \notin \mathcal{U}(R) \to$ not ideal either then

Q. Does the set of units form a group? (under mult. of R) Yes!

Do $N(R)$ and $Z(R)$ form an ideal?

Not in general. Take $R = M_2(\mathbb{R}) \to a = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, b = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$

$a^2 = b^2 = 0$

$(a+b)$ not nilp. or zero div.

Now, suppose $R^{\neq 0}$ is commutative. Do they now form an ideal?

- $N(R)$: $0 \in N(R)$

$a \in N(R)$, $r \in R$. Let $n \in \mathbb{N}$ be s.t. $a^n = 0$.

$$(ra)^n = r^n a^n = 0.$$

$$\therefore ra \in N(R)$$

$a, b \in N(R)$: Let $N = \max(n, m)$ s.t. $a^n = 0 = b^m$.

$$(a+b)^N = \sum \binom{N}{i} a^i b^{N-i} = \sum 0 = 0.$$

Thus, $a+b \in N(R)$.

This shows $N(R)$ is a ideal.

- $Z(R)$: $0 \in Z(R)$ $[R \neq 0]$

Let $a \in Z(R)$, $r \in R$.

suppose $a' \neq 0$ is such that $aa' = 0$.

Then, $(ra)a' = r(aa') = r \cdot 0 = 0$.

$\Rightarrow ra \in Z(R)$. $(a' \neq 0)$

Let $a, b \in Z(R)$. $a', b' \neq 0$ s.t. $aa' = 0 = bb'$.

$(a+b)(a'b') = aa'b' + ba'b'$

$= 0 + bb'a = 0 + 0 = 0.$

Hmm. But bb' could be 0. $=$

ACTUALLY, take $R = \mathbb{Z}/6\mathbb{Z}$.

$2, 3 \in R$ are 0 div.

$2 + 3 = 5$ is not.

Thus, $Z(R)$ is not necessarily an ideal even if R is comm.

25·08·2020

LECTURE - 5

Recall: $Z(R) \cap U(R) = \phi$ (even if $R = 0$)

If $R \neq 0$, then $N(R) \subset Z(R)$.

Q: Is $Z(R) \cup U(R) = R$? → No. Take $R = \mathbb{Z}$.

As an example where true: $R = \mathbb{Z}/n\mathbb{Z}$.

Subsets related to homomorphisms

Let $\varphi : R \longrightarrow S$ be a ring map.

$\ker \varphi := \{ a \in R : \varphi(a) = 0 \} \subset R.$

$$\operatorname{im}\varphi := \{ b \in S : \exists a \in R (\varphi(a) = b)\} \subset S$$
$$= \{\varphi(a) : a \in R\}.$$

$\ker \varphi$ is an ideal of R. [If subring, then $\ker\varphi = R$ AND $S = 0$]

$\operatorname{im}\varphi$ is a subring of S. [If ideal, then $\operatorname{im}\varphi = S$, that is, φ is onto.]

Let $I \subset R$. Then $\varphi(I) \subset S$.

Similarly, if $J \subset S$, then $\varphi^{-1}(J) \subset R$.

Ques. If I is an ideal in R, what can you conclude about $\varphi(I)$?

Ans. $\varphi(I) \underset{\text{ideal}}{\trianglelefteq} \operatorname{im}(\varphi)$? Yes!

In particular, $\varphi(I)$ is an ideal in S if φ is onto.

Eg. If I is an ideal in R, then the natural map

$\pi : R \to R/I$ is onto.

Thus, if $J \subset R$ is an ideal, $\pi(J)$ is an ideal in R/I.

Ques. What does $\pi(J)$ look like?

$$\pi(J) = \{ a + I \in R/I : a \in J\} \overset{\text{def}^n}{=:} \frac{J+I}{I}$$

(just notation for now)

Q. Let $J \subset S$ be an ideal. What can we say about $\varphi^{-1}(J)$?

Ans. $\varphi^{-1}(J)$ is an ideal in R.

In particular, if K is an ideal in R/I, then $\pi^{-1}(K)$ is an ideal in R.

$$J = \pi^{-1}(K) = \{a \in R : a + I \in K\}.$$

Moreover, $\pi(J) = K$. ($\because \pi$ is onto.)

I.e., $K = \dfrac{J+I}{I}$.

In particular, J contains $\pi^{-1}(\{0\}) = \ker \pi$.

In this case : $\ker \pi = I \subset J$.

Thus, $J + I = J$ and hence

$$K = \frac{J+I}{I} = J/I.$$

Thus, every ideal of R looks like J/I where J is an ideal of R containing I.

Thm. The ideals in R/I are in 1-1 correspondence with ideals in R containing I.

$$\left\{\begin{matrix}\text{ideals in}\\ R/I\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{ideals in } R\\ \text{containing } I\end{matrix}\right\}$$

$$K \longmapsto \pi^{-1}(K)$$

$$J/I = \pi(J) \longleftarrow J$$

27·08·2020

LECTURE - 6

Recap: Let $I, J \subset R$ be ideals with $I \subset J$.

If $\pi : R \longrightarrow R/I$ is the natural map, then

$\pi(J) = \{a + I : a \in J\}$. This is denoted by J/I.

Q. What happens if $I \not\subset J$? Then, $\pi(J) = \pi(J+I)$.

Moreover, $I \subset J + I$. Thence, $\pi(J) = (J+I)/I$.

[If $I \subset J$, then $J + I = J$.]

Few constructions:

Defn. Let I, J be ideals in R. Then,

① (sum) $I + J := \{a \in R \mid \exists i \in I, \exists j \in J : a = i + j\}$

$= \{i + j \mid i \in I, j \in J\}$,

② (intersection) $I \cap J$,

$IJ = \{a \in R \mid \exists i \in I, \exists j \in J : a = ij\}$ ✗

would want this

* construct example s.t. this is not an ideal

(product) 3 $IJ := \{a_1b_1 + \cdots + a_nb_n \mid a_i \in I, b_i \in J, n \in \mathbb{N}\}$

$= \{a \in R \mid \exists n \in \mathbb{N}, \exists a_1, \ldots, a_n \in I, \exists b_1, \ldots, b_n \in J, a = a_1b_1 + \cdots + a_nb_n\}$,

4 $I : J := \{a \in R \mid aJ \subset I\}$

are ideals of R.

Example. $R = \mathbb{Z}$, $I = 6\mathbb{Z}$, $J = 3\mathbb{Z}$.

Find $I : J$.

$I : J = 2\mathbb{Z}$.

This is sort of divisibility.

Def^n. (Radical) $I \subset R$ ideal.

5 $\sqrt{I} = \{a \in R \mid \exists n \in \mathbb{N} \, (a^n \in I)\}$.

Is this an ideal?

Ex. $R = \mathbb{Z}$. $I = 8\mathbb{Z}$

$\sqrt{I} = ?$ $\sqrt{I} = 2\mathbb{Z}$.

Observation. $\sqrt{0} = N(R)$ $\rightarrow$ also called nilradical of R

Thus, we don't expect $\sqrt{I}$ to be ideal if R non-commu.

However, if R is commutative, then $\sqrt{I}$ does form an ideal. (Similar proof as earlier for $N(R)$)

Remark. The first four ideals are ideals always.

$\sqrt{I}$ is ideal if R is commutative.

Can't expect anything in non-commutative.

⑥ Let $a \in R$. Let $I \subset R$ be an ideal s.t. $a \in I$.

R is an ideal containing a

Then, $\forall r, s \in R \ (ras \in I)$.

$$a \in \{ras \mid s, r \in R\} \subset I.$$

In fact, for all $n \in \mathbb{N}$, $r_1, \dots, r_n \in R$, $s_1, \dots, s_n \in R$,

$$r_1 a s_1 + \dots + r_n a s_n \in I.$$

Moreover, $\{r_1 a s_1 + \dots + r_n a s_n \mid n \geq 1, r_i \in R, s_i \in R\}$ is actually an ideal.

This is the smallest ideal of R containing a.

Notation: $\langle a \rangle \to$ ideal generated by a.

If R is commutative, then $\langle a \rangle = \{ra : r \in R\}$, also denoted Ra.

Let $a_1, a_2 \in R$. What is $\langle a_1, a_2 \rangle$? (Nothing about commutativity.)

$$\langle a_1, a_2 \rangle = \langle a_1 \rangle + \langle a_2 \rangle.$$

More generally, if $a_1, \dots, a_n \in R$, then

$$\langle a_1, \dots, a_n \rangle = \langle a_1 \rangle + \dots + \langle a_n \rangle.$$

If R is commutative, then
$a \in \langle a_1, \dots, a_n \rangle \iff \exists r_1, \dots, r_n \in R \ (r_1 a_1 + \dots + r_n a_n = a)$

(Resembles linear span from linear algebra.)

We say I is finitely generated if
$\exists a_1, \dots, a_n \in R$ s.t. $I = \langle a_1, \dots, a_n \rangle$.

and I is cyclic (or principal) if $\exists a \in R$ s.t. $I = \langle a \rangle$.

Some special classes of ideals: $0 \neq R$ commutative

Q1 When is R a field? $U(R) = R \setminus \{0\}$. (works even if $R = 0$.)

I is maximal if $I \neq R$ & $I \subsetneq J \Rightarrow I = J$.
$\hphantom{I \text{ is maximal if } I \neq R \text{ \& } I \subsetneq} \llcorner$ ideal

Q2. When is R a domain? $Z(R) = \{0\}$.

I is a prime ideal if $ab \in I \Rightarrow a \in I$ or $b \in I$

<u>Q3.</u> When is R reduced? $N(R) = \{0\}$.

I is radical if $I = \sqrt{I}$.

(Then R/I becomes reduced.)

31·08·2020

LECTURE - 7

- We'll pretty much stick commutative rings.

Especially when dealing with $M_n(R)$, $R[x]$, $R[[x]]$, prime or radical ideals, R is assumed to be commutative.

- Let $a \in R$. Do you think $1-a$ is a unit?

Well, $1 + a + a^2 + \dots$ seems like a nice candidate.

If $a \in \mathcal{N}(R)$, then the above sum will make sense and will be correct.

If R is comm., then $\forall r \in R$, $\forall a \in \mathcal{N}(R)$, $1 + ra \in \mathcal{U}(R)$.

- If $\varphi : R \longrightarrow S$ is a ring map, then $R/\ker\varphi \simeq \varphi(R)$.

In fact, the map
$$\tilde{\varphi} : R/\ker\varphi \longrightarrow S$$
$$\bar{a} \longmapsto \varphi(a)$$
is a well-defined one-one homo. and onto its image, giving the isomorphism.

Let $I \subset R$, $\varphi : R \to S$ ring map. Does φ factor through R/I?

I.e., $\exists\, \tilde{\varphi}$ s.t.

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "\pi"'] \arrow[dr, phantom, "\circlearrowleft"] & S \\ R/I \arrow[ur, dashed, "\tilde{\varphi}"'] & \end{tikzcd}$$

Works if $0 \subseteq I \subseteq \ker \varphi$.

"Same" proof as of first iso. theorem.

- R comm

$I = \langle a_1, \dots, a_n \rangle$, $J = \langle b_1, \dots, b_m \rangle$

$$IJ \subset I \cap J \subset I + J$$

$IJ = \langle a_i b_j \mid 1 \le i \le n,\ 1 \le j \le m \rangle$

$I+J = \langle a_1, \dots, a_n, b_1, \dots, b_m \rangle$.

equality almost impossible

$$\begin{tikzcd} & I+J \arrow[dl, dash] \arrow[dr, dash] & \\ I \arrow[dr, dash] & & J \arrow[dl, dash] \\ & I \cap J \arrow[d, dash] & \\ & IJ & \end{tikzcd}$$

$I+J$ → smallest ideal containing both

$I \cap J$ → largest ideal contained in both

this shows why $I + J = I \cap J$ is possible iff $I = J$.