

Jan 16

Last class summary

Ring: + Abelian group
 x Associative distributive

Sometimes: "unity",
 "inverses" if exists,
 they are unique

Subring: A subset which is
 also a ring (same ops) \Leftrightarrow closed under
 x, -

Zero divisor: $a \cdot b = 0$ but $a \neq 0, b \neq 0$
 (in commutative rings)

Integral domain: commutative w/ unity &
 no zero-divisor
 $(ac = bc, c \neq 0 \Rightarrow a = b)$

Field: +, x both make Abelian group

Claim "Cancellation lemma"

$$ac = bc \quad \& \quad c \neq 0$$

$$\Rightarrow a = b$$

proof: $ac = bc \Rightarrow ac - bc = 0$
 $\Rightarrow (a-b)c = 0$

Claim: A finite integral domain is always
 a field.

(in particular, \mathbb{Z}/p is a field)

(in particular, $\mathbb{Z}/2$ is a field with
 2 elements)

+	0	1
0	0	1
1	1	0

x	0	1
0	0	0
1	0	1

$\mathbb{Z}/19 \Rightarrow$ a field with 19 elements.

under $\mathbb{Z}/19$,

$$8^{-1} = 12 \quad \text{Since } 8 \cdot 12 = 96 = 19 \cdot 5 + 1 \\ \equiv 1 \pmod{19}.$$

Proof of Claim: finite

Assume D is an integral domain
& $0 \neq a \in D$.

Need ~~Now~~ to show that a is invertible.

Consider

$$\{a^1 = a, a^2 = a \cdot a, a^3 = a \cdot a \cdot a, a^4, a^5, \dots\} \\ \subset D$$

There must be repetitions, i.e. $\exists i < j$

$$\text{s.t. } a^i = a^j \Rightarrow 1 = a^{j-i} \\ \Rightarrow \underbrace{a^{j-i-1}}_{a^{-1}} \cdot a = 1$$

Comment: if $n \in \mathbb{Z}$, & $a \in R$ (a general ring)

$$\text{set } na = \begin{cases} \frac{a + a + \dots + a}{n} & n > 0 \\ -\frac{a - a - \dots - a}{n} & n < 0 \\ 0 & n = 0 \end{cases}$$

Def: char R = "characteristic" is the least positive integer n

s.t. $\forall a \in R \quad na = 0$

if none, declare char $R = 0$

Examples:

- ① char $\mathbb{Z}/2 = 2 \quad 2a = a + a$
- ② char $\mathbb{Z}/19 = 19$
- ③ char $\mathbb{Z} = 0 \quad \text{char } \mathbb{Q} = 0$

Jan 16

Lemma: If R has a unity 1 , then
 $\text{Char } R = \text{least positive integer } n$
 s.t. $n \cdot 1 = \underbrace{1 + \dots + 1}_n = 0$

Proof: $na = a + a + \dots + a$
 $= (1 + 1 + \dots + 1)a$
 $= (n \cdot 1)a$

So if $n \cdot 1 = 0$ then $n \cdot a = 0 \forall a$
 $\Rightarrow \text{~~char } R = n~~ (n \cdot 1 = 0)$
 $\Leftrightarrow \forall a \quad na = 0 \quad \square$

Cor: $\text{char } \mathbb{Z}/n = n$

PF: $\underbrace{1 + \dots + 1}_K = K \pmod n$

\Rightarrow least K which is ~~invisible~~ invisible
 by n is n

$\Rightarrow \text{char } \mathbb{Z}/n = n$

Claim: If F is a field,
 then $\text{char } F = 0$ or a prime.

Proof: Assume $\text{char } F > 0$
 ie, assume $n \cdot 1 = 0$ for some n , yet
 if $0 < k < n$, then $k \cdot 1 \neq 0$

Now assume by contrary, that n isn't
 a prime, ie $n = k \cdot l$ with $k, l < n$,
 then $0 = n \cdot 1 = \underbrace{1 + \dots + 1}_{n=k \cdot l} = \underbrace{(1 + \dots + 1)}_k + \underbrace{(1 + \dots + 1)}_k + \dots + \underbrace{(1 + \dots + 1)}_k_l$
 $= l \cdot (k \cdot 1)$

but $k < n$ so $k \cdot 1 \neq 0$ and $l < n$ so
 $l \cdot (k \cdot 1) \neq 0 \Rightarrow \text{so } n \text{ is prime.}$

Quotient rings

"generalization of $\mathbb{Z} \mapsto \mathbb{Z}/n = \mathbb{Z}/n\mathbb{Z}$ "
"forgetting multiples of n "
"forgetting $n\mathbb{Z}$ "

Definition: A subring A of a ring R is called
"an ideal" if $\forall a \in A \quad \forall r \in R$
 $a \cdot r \in A$ and $r \cdot a \in A$

Examples: $6\mathbb{Z}$ is an ideal in \mathbb{Z} .

$$\begin{array}{ccc} 5 & \cdot & 18 \\ \uparrow & & \uparrow \\ \mathbb{Z} & & 6\mathbb{Z} \end{array} = 90 \quad \uparrow \\ \mathbb{Z} \quad 6\mathbb{Z}$$

$R = \mathbb{Z}[x] = \{7x^3 - 3x^2 + 2x - 20\}$
 $\mathbb{Z} \subset \mathbb{Z}[x]$ a subring but
not an ideal, indeed

$$7 \cdot x^3 \notin \mathbb{Z}$$

yet {polynomials with constant term $= 0$ }

$$= \{7x^3 + 2x^2 - 7x + 0\}$$

$$= x \cdot \mathbb{Z}[x]$$

if $p \in x\mathbb{Z}[x]$ & $q \in \mathbb{Z}[x]$

then $p = x \cdot f$ for some f

$$p \cdot q = x \cdot f \cdot q = x \cdot (f \cdot q) \in x \cdot \mathbb{Z}[x]$$

so $x\mathbb{Z}[x]$ is indeed an ideal.

$A_3 = \{\text{polynomials with even constant term}\}$

Ex: A_3 is an ideal.

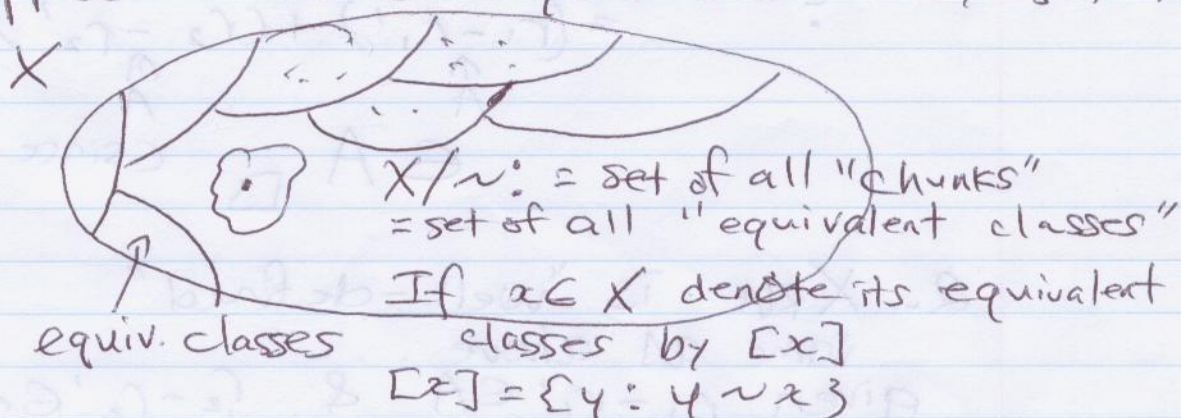
Jan 16

Declare " $r_1 \sim_A r_2$ " , $r_1, r_2 \in R$
 (Given R - a ring , $A \subset R$ an ideal)
 $\Leftrightarrow r_1 - r_2 \in A$.

Claim \sim_A is an "equiv. relation"

1. $r \sim r$
 2. $r_1 \sim r_2 \Rightarrow r_2 \sim r_1$
 3. $r_1 \sim r_2, r_2 \sim r_3 \Rightarrow r_1 \sim r_3$
- } A is closed under $-$ & contains 0

Suppose \sim is an equiv. rel. on any set X

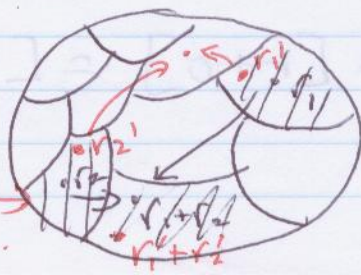


If $A \subset R$ is an ideal, denote R/\sim_A by R/A
 $R/A = \{[r] : r \in R\}$
 $[r] = \{r' : r' - r \in A\}$
 $= r + A$

$r' - r \in A$
 $r' - r = a \in A$
 $r' = r + a$
 $r' \in r + A$

Theorem: If $A \subset R$ is an ideal in a ring then R/A is a ring under

1. $0_{R/A} = [0] = A$
2. $+_{R/A} : [r_1] + [r_2] := [r_1 + r_2]$
 $(r_1 + A) + (r_2 + A) := (r_1 + r_2) + A$



Same applies for $\times_{R/A}$

may result in this chunk

If "well-defined" see next pg.

$$3. \text{XRIA} : [r_1] \cdot [r_2] := [r_1 \cdot r_2]$$

Proof: 1. $+_{RIA}$ is "well-defined"

If $[r_1] = [r_1']$ & $[r_2] = [r_2']$
 then $[r_1 + r_2] = [r_1' + r_2']$

Proof: $[r_1] = [r_1'] \Leftrightarrow r_1 \sim r_1'$

$$\Leftrightarrow r_1 - r_1' \in A$$

$$\Leftrightarrow r_2 - r_2' \in A$$

IS $r_1 + r_2 \sim r_1' + r_2'$?

$$A \ni r_1 + r_2 - (r_1' + r_2')$$

$$= (r_1 - r_1') + (r_2 - r_2')$$

$$\uparrow A$$

$$\uparrow A$$

$$\in A$$

□

(since A is subring)

2. XRIA is "well-defined"

same as above

given $r_1 - r_1' \in A$ & $r_2 - r_2' \in A$

study $r_1 r_2 - r_1' r_2'$

$$r_1 r_2 - r_1' r_2' = r_1(r_2 - r_2') + (r_1 - r_1')r_2'$$

$$\underbrace{\uparrow R \quad \uparrow A}$$

$$\underbrace{\uparrow A \quad \uparrow R}$$

def'n of an ideal

$$\underbrace{\uparrow A \quad \uparrow A}_{\uparrow A}$$

$$\begin{aligned} [r_1] + [r_2] &\stackrel{?}{=} [r_2] + [r_1] \\ &= [r_1 + r_2] = [r_2 + r_1] \end{aligned} \quad \square$$

$$-[r] := [-r]$$

$$[r] + [0] = [r + 0] = [r]$$

Jan 16

Examples 1. $A = \{0\}$ $R/\{0\} = R$

$$r_1 - r_2 \in \{0\} \rightarrow r_1 - r_2 = 0 \Rightarrow r_1 = r_2$$

$$2. A = R \quad R/R = \{0\}$$

$$r_1 - r_2 \in A \Rightarrow r_1 - r_2 \in R$$

3. $n\mathbb{Z}$ $\mathbb{Z}/n\mathbb{Z}$ is a ring

$$r_1 \sim r_2 \Leftrightarrow r_1 - r_2 \in n\mathbb{Z}$$

 $r_1 - r_2$ is a multiple of n

$$(r_1 \bmod n) = (r_2 \bmod n)$$

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], [2], \dots, [n-1]\} = \mathbb{Z}/n$$

Let R be a ring & commutative, and let $a \in R$. Define $aR = \{a \cdot r : r \in R\}$

$=: \langle a \rangle$: ideal generated by a

Claim $\langle a \rangle$ is an ideal:

pf: 1. $ar_1 + ar_2 = a(r_1 + r_2)$

$\Rightarrow \langle a \rangle$ is closed under addition

$$2. (a \cdot r_1) \cdot r_2 = a(r_1 \cdot r_2)$$

$$\begin{matrix} \uparrow & & \uparrow \\ A & & R \end{matrix} \quad \text{associativity}$$

$$r_2 \cdot (a \cdot r_1) = a \cdot (r_1 \cdot r_2)$$

$\therefore R/\langle a \rangle$ is always a ring!

Examples: 1. $R/\langle 1 \rangle = R/R = \{0\}$

$$2. R/\langle 0 \rangle = R/\{0\} = R$$

$$3. \mathbb{Z}/\langle 7 \rangle = \mathbb{Z}/7\mathbb{Z}$$

$$4. R = \mathbb{Z}[x] \quad \text{polynomials by variable } x.$$

$$A = \langle x \rangle = \{xf : f \in R\}$$

$= \{ \text{polynomials with zero constant term} \}$

$$R/\langle x \rangle = \{[p]\}$$

\uparrow
equivalence
classes
of polynomials

Claim: Any $p \in \mathbb{Z}[x]$ is equivalent to a constant
and constants are never equivalent to each other
So, $R/\langle x \rangle = \mathbb{Z}$.

$$x^2 + 19 \sim 19 \quad \text{indeed } x^2 + 19 - 19 = x^2 \in \langle x \rangle$$

real # $\rightarrow \mathbb{R}[x] / \langle x^2 + 1 \rangle \stackrel{\sim}{=} \mathbb{C}$ complex #.

Claim: 1. any $f \in \mathbb{R}[x]$ is equivalent to a linear function $\forall f \exists a, b \in \mathbb{R}$ s.t. $f \sim ax + b$

2. $ax + b \sim cx + d \Leftrightarrow a = c, b = d$

Pf of 2: $ax + b \sim cx + d \Rightarrow (ax + b) - (cx + d) \in A$
 $\Leftrightarrow (a - c)x + (b - d) \in A = \text{multiples of } 1 + x^2$
 $\Leftrightarrow (a - c)x + (b - d) = 0 \Leftrightarrow a - c = 0 = b - d$

Pf of 1: $x^2 \sim -1 \quad x^2 - (-1) = x^2 + 1 \in A$
 $x^2 f \sim -f \quad x^2 f - (-f) = x^2 f + f = (x^2 + 1)f \in A$

$$28x^4 - 3x^3 + \pi x^2 - ex + 2$$

$$\underbrace{(28x^2 - 3x + \pi)}_f x^2 - ex + 2$$

$$\sim -28x^2 + 3x - \pi - ex + 2$$

$$\sim 28x + 3x - \pi - ex + 2 \quad \text{linear}$$

$$\mathbb{R}[x] / \langle 1 + x^2 \rangle = \{[a + bx]\} \quad \begin{array}{l} \star \text{ understand it} \\ \star \text{ as a set,} \\ \text{NOT a ring} \end{array}$$

$$\begin{aligned} [a + bx] \cdot [c + dx] &= [(a + bx)(c + dx)] \\ &= [ac + (bc + ad)x + bd x^2] \\ &= [(ac - bd) + (bc + ad)x] \end{aligned} \quad \leadsto \underline{x^2 f \sim -f}$$

$$\star (a + bi)(c + di) = (ac - bd) + (bc + ad)i$$