Lecture 2

January 16, 2008
6:00 PM

Ring: $+$: Abelian group
$\times$: Associative & distributive

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

Subring: A subset which is also a ring (same operations)
$\Leftrightarrow$
closed under $\times, -$

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: $+, \times$ both make Abelian.
$\Leftrightarrow$ integral domain in which every $\neq 0$ elem. has an inv.

Claim: "Cancellation lemma"
if $ac = bc$ and $c \neq 0 \Rightarrow a = b$

Proof: if $ac = bc \Rightarrow ac - bc = 0 \Rightarrow (a-b)c = 0$
But $c \neq 0 \Rightarrow a - b = 0 \Rightarrow a = b$ ∎

Claim: A finite integral domain is always a field. (in particular, $\mathbb{Z}/p$ is

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

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

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

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

Proof of claim: Assume D is a finite integral domain and $a \neq 0 \in D$. Need to show that a is invertible. Consider

$\{a^1 = a, a^2 = a \cdot a, a^3 = a \cdot a \cdot a, a^4, a^5, \ldots\} \subseteq D$

There must be repetitions, i.e. $\exists\, i < j$ s.t
$a^i = a^j$

$a^i = a^j$.

$\underbrace{a \cdot a \cdots a}_{i} = \underbrace{a \cdots a}_{j}$

$\Rightarrow 1 = a^{j-i}$

$\Rightarrow \underbrace{a^{j-i-1}}_{a^{-1}} \cdot a = 1$

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

Set $na = \begin{cases} \underbrace{a + \cdots + a}_{n} & n > 0 \\ \underbrace{-a - \cdots - a}_{n} & n < 0 \\ 0 & n = 0 \end{cases}$

Def: Char R = "characteristic of R" is the least positive integer n s.t. $\forall a \in R, na = 0$
If $\nexists$, declare Char R = 0.

Ex: 1. Char $\mathbb{Z}/2 = 2$, $2 \cdot a = a + a$

2. Char $\mathbb{Z}/19 = 19$
3. Char $\mathbb{Z} = 0$
4. Char $\mathbb{Q} = 0$

Lemma: if R has a unity 1, then Char R = the least positive integer n s.t. $n \cdot 1 = \underbrace{1 + \cdots + 1}_{n} = 0$

Proof: $na = \underbrace{a + \cdots + a}_{n} = (\underbrace{1 + \cdots + 1}_{n})a = (n \cdot 1)a$

(1 = unity of the ring)

So if $n \cdot 1 = 0$, then $na = 0 \ \forall a$
$\Rightarrow (n \cdot 1 = 0) \Leftrightarrow \forall a, n \cdot a = 0$ ∎

Cor: Char $\mathbb{Z}/n = n$.

Cor: $\mathrm{Char}\ \mathbb{Z}/n = n$.

Proof: $\underbrace{1+\dots+1}_{k} \equiv k \bmod n$. The least k div. by n is n. Thus $\mathrm{char}\ \mathbb{Z}/n = n$.

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

Proof: Assume F is a field, $\mathrm{char}\ F > 0$.
i.e. assume $n \cdot 1 = 0$ for some n, yet if $0 < k < n$, then $k \cdot 1 \neq 0$.

Now assume by contradiction that n isn't a prime, i.e. $n = k \cdot \ell$ with $k, \ell < n$. Then

$$0 = n \cdot 1 = \underbrace{1+\dots+1}_{n} = \underbrace{\underbrace{(1+\dots+1)}_{k} + \dots + \underbrace{(1+\dots+1)}_{k}}_{\ell} =$$

$$= \ell \cdot (k \cdot 1)$$

But $k < n$, so $k \cdot 1 \neq 0$. Also $\ell < n$, so $\ell \cdot (k \cdot 1) \neq 0$

$\Rightarrow\Leftarrow$

So n is prime.

Quotient Rings

"generalization of $\mathbb{Z} \longmapsto \mathbb{Z}/n$" $= \mathbb{Z}/n\mathbb{Z}$

"Forgetting multiples of n"

"Forgetting $n\mathbb{Z}$"

Def: A subring A of a ring R is called "an ideal" if

$$\forall\, a \in A, \forall\, r \in R,\ a \cdot r \text{ and } r \cdot a \in A$$

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

$$\begin{array}{ccccc} 5 & \cdot & 18 & = & 90 \\ \cap & & \cap & & \cap \\ \mathbb{Z} & & 6\mathbb{Z} & & 6\mathbb{Z} \end{array}$$

$R = \mathbb{Z}[x] = \{7x^3 - 3x^2 + 2x - 28\}$

1. $\mathbb{Z} \subset \mathbb{Z}[x]$ a subring but not an ideal indeed $7x^3 \notin \mathbb{Z}$
2. Yet $\{$polynomials with constant term $= 0\} = \{7x^3 + 2x^2 - 7x + 0\}$
$= x \cdot \mathbb{Z}[x]$
if $p \in x \cdot \mathbb{Z}[x]$ & $q \in \mathbb{Z}[x]$
Then $p = x \cdot f$ for some f
so $p \cdot q = x \cdot f \cdot q = x \cdot (f \cdot q) \in x \cdot \mathbb{Z}[x]$

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

3. Let $A_3 = \{$all polynomials with even const. term$\}$

- Ex: Show A_3 is an ideal.

Given R a ring, $r_1, r_2 \in R$ and $A \in R$ an ideal

Declare "$r_1 \sim_A r_2$" $\Leftrightarrow$ $r_1 - r_2 \in A$

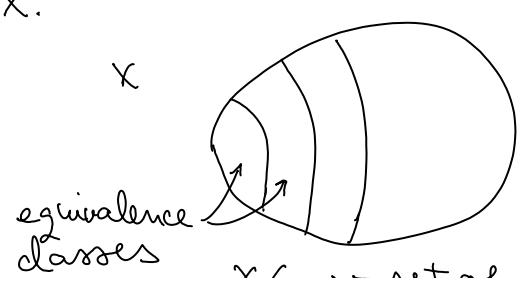
↑ is equivalent to mod A

Claim: $\sim_A$ is an "equivalence relation"

1. $r \sim r$ — reflexivity
2. $r_1 \sim r_2 \Rightarrow r_2 \sim r_1$ — symmetry
3. $r_1 \sim r_2, r_2 \sim r_3 \Rightarrow r_1 \sim r_3$ — transitivity

All 3 facts follow from A is closed under "$-$", and it contains 0.

Suppose $\sim$ is an equivalence relation on any set X.



Two items are equiv. if they are in the same "chunk".

classes $X/\sim$:= set of all "chunks"
:= set of all equivalence classes

if $x \in X$, denote its equivalence class by $[x]$
$[x] = \{y : y \sim x\}$

if $A \subset R$ is an ideal, denote $R/\sim_A$ by R/A.

$R/A = \{[r] : r \in R\}$
$[r] = \{r' : r - r' \in A\}$
$= r + A$

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

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

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

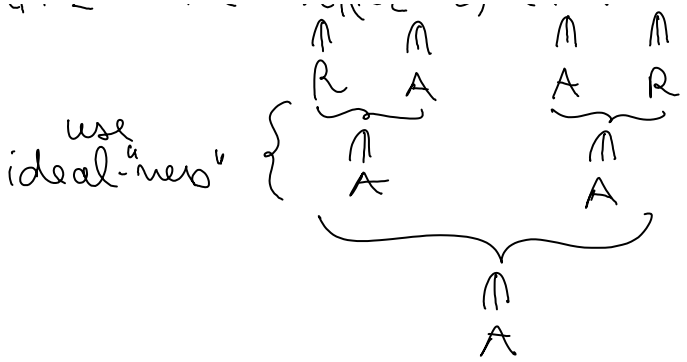
(may not be well-defined, to prove later)

Proof: 1. $+_{R/A}$ is "well-defined"
If $[r_1] = [r_1']$ & $[r_2] = [r_2']$, then
$[r_1 + r_2] = [r_1' + r_2']$
mini-proof: $[r_1] = [r_1'] \iff r_1 \sim r_1' \iff r_1 - r_1' \in A$
similarly $\iff r_2 - r_2' \in A$
is $r_1 + r_2 \sim r_1' + r_2'$?
Check $r_1 + r_2 - (r_1' + r_2') \stackrel{?}{\in} A$

$= \underbrace{(r_1 - r_1')}_{\in A} + \underbrace{(r_2 - r_2')}_{\in A} \Rightarrow (r_1 + r_2) - (r_1' + r_2') \in A$

2. Multiplication is well-defined
Same as addition
Given $r_1 - r_1' \in A$, $r_2 - r_2' \in A$
study $r_1 r_2 - r_1' r_2' = r_1(r_2 - r_2') + (r_1 - r_1')r_2'$
$\in R \cdot A$, $\in A \cdot R$

use "ideal-ness" $\{$ $\in A$, $\in A$



$[r_1]+[r_2] \stackrel{?}{=} [r_2]+[r_1]$

$\|$

$[r_1+r_2] = [r_2+r_1]$

$-[r] = [-r]$

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

Examples:

1. $A = \{0\}$ $R/\{0\} = R$ $r_1 - r_2 \in \{0\}$ $r_1 - r_2 = 0$ $r_1 = r_2$
2. $A = A$ $R/R = \{0\}$ $r_1 - r_2 \in A = R$
3. $n\mathbb{Z}$ $\mathbb{Z}/n\mathbb{Z} =$ $r_1 \sim r_2 \iff r_1 - r_2 \in n\mathbb{Z}$
   $= \{[0], [1], \ldots, n-1\}$ $r_1 - r_2$ is a multiple of n
   $= \mathbb{Z}/n$ $r_1 \bmod n = r_2 \bmod n$
4. Let R be a commutative ring, $a \in R$.
   $aR = \{a \cdot r : r \in R\} =: \langle a \rangle$ "ideal generated by a"

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

Proof: 1. $ar_1 + ar_2 = a(r_1 + r_2) \Rightarrow \langle a \rangle$ is closed under add.

2. $(a \cdot r_1) \cdot r_2 = a(r_1 \cdot r_2)$
   $\in$ $\in$
   A R

So $R/\langle a \rangle$ is always a ring.

Ex: 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. $R = \mathbb{Z}[x]$ $A = \langle x \rangle = \{xf : f \in R\}$

$= \{$polys with 0 as a const. term$\}$

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

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

Claim: $x^2 + 19 \sim 19$
$x^2 + 19 - 19 = x^2 \in \langle x \rangle$

$R[x]/\underbrace{\langle x^2+1 \rangle}_{A,\sim} = \mathbb{C}$

Claim: Any $f \in R[x]$ is equiv. to a linear f'n
$\forall f \; \exists \; a, b \in \mathbb{R}$ s.t. $f \sim ax + b$

2. $ax + b = cx + d$ iff $a = c$, $b = d$

Proof of 2: $ax + b \sim cx + d$

$\Leftrightarrow ax + b - (cx + d) \in A$
$\Leftrightarrow (a - c)x + (b - d) \in A =$ multiples of $1 + x^2$
$\Leftrightarrow (a - c)x + (b - d) = 0$
$\Rightarrow a = c$, $b = d$

Proof of 1: $x^2 \sim -1$
$x^2 - (-1) = x^2 + 1 \in A$
$x^2 f \sim -f$
$x^2 f - (-f) = x^2 f + f = (x^2 + 1) f \in A$
$28x^4 - 3x^3 + \pi x^2 - ex + 2$

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

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

$$\mathbb{R}[x]/\langle 1+x^2\rangle = \{[a+bx]\}$$

$$[a+bx][c+dx] = [(a+bx)(c+dx)]$$

$$= [ac + (bc+ad)x + bdx^2]$$

$$= [(ac-bd) + (bc+ad)x]$$

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