Lecture 1

① Course Info: See class website, syllabus, calendar

② HW01 due this Friday at 11:59pm:

will ask you to recall prereq topics from 150ab, 250a and review some important ones for 250b

③ Goal: Cover material from Chp 6 & 8 in Rotman, mostly linearly. Fill in gaps as needed. Will cover some other stuff at the end.

<u>Recall</u>. A category $\mathcal{C}$ consists of

collection of objects $Ob(\mathcal{C})$ $\quad X, Y$

and structure-preserving maps $Mor(\mathcal{C})$ $\quad Mor(X,Y)$

these Mor / Hom sets can be enriched in other categories

Rings: $(R, +, \cdot)$ where

- $(R,+)$ is an abelian group ($\Rightarrow 0 \in R$)
- there is a multiplicative identity $1 \in R$ and multiplication is associative

  ie $(R-\{0\}, \cdot)$ is a monoid
- Distributive: $a(b+c) = ab + ac$,

  $(b+c)a = ba + ca \quad \forall\ a,b,c \in R$

<u>Rmk</u>. If $1=0$, then the whole thing collapses and we have $R = \{0\}$, the <u>zero ring</u>.

<u>Rmk</u> If mult. is comm, then we have a commutative ring.
$\rightsquigarrow$ commutative algebra is a whole course

We will ~~not~~ assume R is commutative.

Eg. Many important non-comm rings:

① ⓐ $Mat_n(\mathbb{C})$ where $n \geq 2$

ⓑ or for that matter, $Mat_n(k)$ where k is any nonzero commutative ring (eg. fields) $(n \geq 2)$

ⓒ or even $Mat_n(R)$ where R is noncomm $(n \geq 1)$

② Group ring: $(G, \cdot)$ = a group.

$\mathbb{Z}G = \mathbb{Z}[G] = \{ \sum_{g \in G} a_g g \mid$ only finitely many $a_g \neq 0 \}$

Rotman

where multiplication is like polynomial mult:

eg. $(3x+2y)(x+y) = 3x^2 + 3xy + 2yx + 2y^2$

here $x^2, xy, yx, y^2 \in G$.

③ Polynomials! k - not nec. comm. ring. Then $k[x]$ also is noncomm (why is this obvious?)

not "proof by intimidation"; rather, should be a quick answer once you figure it out

④ $End(A)$ where A is an abelian group

eg. $End(\mathbb{Z}^2) \cong Mat_2(\mathbb{Z})$.

Some important structures:

defn. <u>Subring</u>: $S \subset R$ that has the same $0, 1$ as S, and is closed under $+, \cdot$. $\Rightarrow$ also a ring.

defn. <u>Center</u> $Z(R)$ = elements that (obv. multiplicatively) comm. w/ all others.

Eg. Scalar matrices in $M_n(k)$, when k is commu.

<u>Claim</u> $Z(R)$ is a subring (Prove this — this is 150-level proof)

Eg. $S = \{a+ib \mid a,b \in \mathbb{Z}\} \subset \mathbb{C}$

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

is a ring ... but not a subring of $\mathbb{C}$.

What is 1_S?

$ac + (ad+bc)i = c + di$ iff $a=1, b=0$ ✓ same 1

But multiplication is not the same!

Eg. $R = \mathbb{Z} \times \mathbb{Z}$. $1_R = (1,1)$.

$S = \{(n,0)\} \cong \mathbb{Z}$ but $1_S = (1,0)$.

So S is not a subring of R.

Easier to think of all this by morphisms:

S is a subring of R iff there is an injective ring hom / ring map $i : S \hookrightarrow R$.

defn. A ring hom $\varphi: R \longrightarrow S$ is a set map where $(+, \cdot, 1)$ are respected.

$\varphi(a+b) = \varphi(a) + \varphi(b)$, $\varphi(ab) = \varphi(a)\varphi(b)$, $\varphi(1_R) = 1_S$.

Obvious consequence: $\varphi(0) = 0$. Why? (group hom. condition)

$\rightsquigarrow$ this gives us the notion of ring isom- (hom + bij), endo-, auto-morphisms; kernel, image...

Subrings are **not to be confused with** ideals.

defn. Let I be an additive subgroup of R.

① I is a left ideal if $\forall a \in I, r \in R$, $ra \in I$

ie $R \cdot I \subset I$, ie. $\exists$ action by R on left

② I is a right ideal if $\forall a \in I, r \in R$, $ar \in I$

ie $I \cdot R \subset I$, ie $\exists$ action by R on the right

③ I is a 2-sided ideal if both $IR, RI \subset I$

ie there is left and right action by R.

eg. $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} r & 0 \\ s & 0 \end{bmatrix} = \begin{bmatrix} * & 0 \\ * & 0 \end{bmatrix} \Rightarrow Re_1$ is a left ideal

$\rightsquigarrow \left\{\begin{bmatrix} * & 0 \\ * & 0 \end{bmatrix}\right\}$ and $\left\{\begin{bmatrix} 0 & * \\ 0 & * \end{bmatrix}\right\}$ are left ideals

OTOH, $\left\{\begin{bmatrix} * & * \\ 0 & 0 \end{bmatrix}\right\}$ and $\left\{\begin{bmatrix} 0 & 0 \\ * & * \end{bmatrix}\right\}$ are right ideals

What are the two-sided ideals?

$\hookrightarrow$ only $\{0\}$ and $Mat_2(\mathbb{R})$

$\Rightarrow$ no proper two-sided ideals

Why are ideals "more important" than subrings?

<u>defn.</u> If I is a 2-sided ideal, then R/I is a <u>quotient ring</u>

$$R/I = \{ r+I \mid r \in R \}$$

- addition is clearly ok
- $(r+I)(s+I) = rs + rI + sI + I^2 = rs + I$

Is this <u>well-defined</u>?

if $r \sim r'$, $s \sim s'$, then $r - r', s - s' \in I$.

$$rs - r's' = rs - rs' + rs' + r's'$$
$$= r(s-s') + (r-r')s' \in I.$$

Think back to <u>normal</u> subgroups...

The canonical/natural map: $\pi: R \longrightarrow R/I$
$$r \longmapsto r+I$$

Next time: Modules.