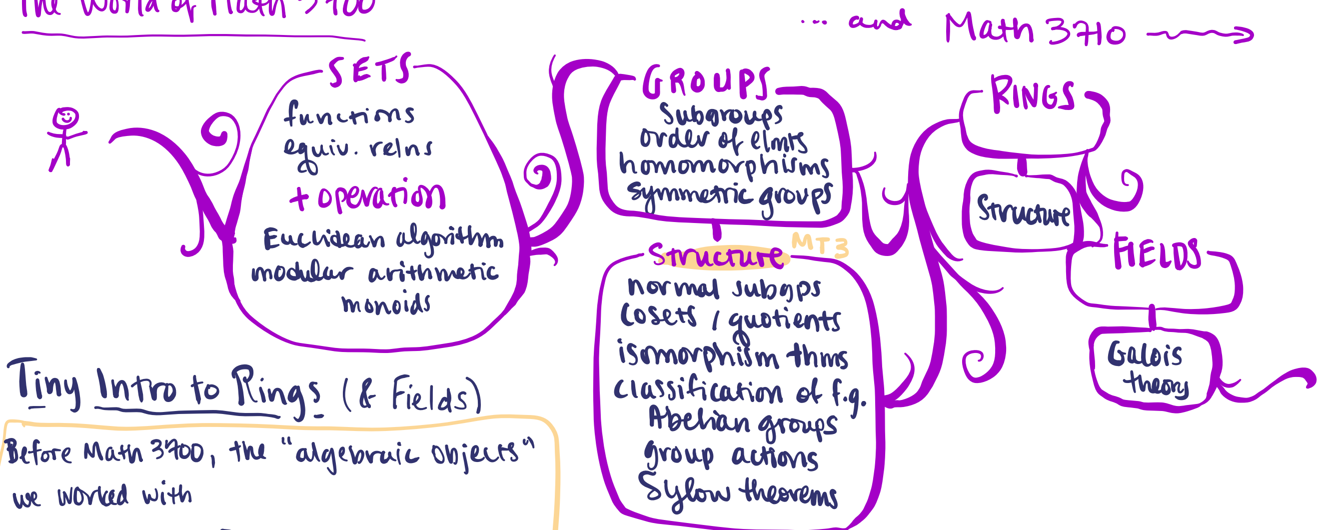
Math 3700

12/06 and 12/08

Today: course overview
tiny intro to rings
review of 3^{rd} half of material

The World of Math 3700



Tiny Intro to Rings (& Fields)

Before Math 3700, the "algebraic objects" we worked with

$$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$$

come w/ two operations: $+$ and $\cdot$

For groups, we only use one operation

$$(\mathbb{Z},+) \quad (\mathbb{Q},+)$$
$$(\mathbb{R},+) \quad (\mathbb{C},+)$$

but we still have

$$(\mathbb{Z},\cdot) \quad (\mathbb{Q},\cdot)$$
$$(\mathbb{R},\cdot) \quad (\mathbb{C},\cdot)$$

which are not groups but monoids.

Idea: A ring R has two operations $+$ and $\cdot$ s.t. $(R,+)$ is an Abelian gp and $(R,\cdot)$ is a monoid, & conditions ...
↪ 0, 1
↪ distribution

Ex. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all rings
So is $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$

Brief History: In 1920s, Emmy Noether gave the axiomatic defns of rings we use today. She revolutionized modern algebra. She is very cool + badass.

Many basic things we can prove about rings will be generalizations of familiar facts:

Ex. In any ring R, $\underbrace{(-1_R)}_{\text{additive inv of } 1_R}\cdot r = \underbrace{-r}_{\text{additive inv of } r}$ for any $r \in R$.

Pf/ Since (additive) inverses are unique in $(R,+)$, it suffices to show $r + (-1_R)\cdot r = 0$.
But $r = 1_R \cdot r$ (as 1_R is the identity of the monoid $(R,\cdot)$) and so

$$\begin{aligned} r+(-1_R)\cdot r &= 1_R\cdot r + (-1_R)\cdot r \\ &= (1_R - 1_R)\cdot r && \text{by distribution} \\ &= 0\cdot r && \text{by defn of additive inverse} \\ &= 0. && \text{Exc.} \end{aligned}$$

$\square$

Note: We already have a name for the "structure" of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$: field.
Fields are special kinds of rings:

$$(\mathbb{Q}\setminus\{0\},\cdot),\ (\mathbb{R}\setminus\{0\},\cdot),\ (\mathbb{C}\setminus\{0\},\cdot) \text{ are groups.}$$

However $\mathbb{Z}$ is not a field since $(\mathbb{Z}\setminus\{0\},\cdot)$ is not a group.

Q. When is $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ a field?

A. $\Leftrightarrow$ When is $(\mathbb{Z}/n\mathbb{Z}\setminus\{0\},\cdot)$ a group
$\Leftrightarrow$ $n=p$ is prime.

Lots of the work we've done for gps will carry over to rings.
But there will be new structures to study ...

Some analogies:

Groups	Rings	Fields
group homomorphism	ring homomorphism	field homomorphism
Subgroups	Subrings	subfields
?	ideals !	(boring)
structure thms	structure thms (for ideals)	(boring)
?	modules Ex. $\mathbb{Z}$-modules = Ab gps Thm. If M is a f.g. $\mathbb{Z}$-module then $M \cong \mathbb{Z}^n \times \mathbb{Z}/p_1^{e_1} \times \dots \times \mathbb{Z}/p_k^{e_k}$	vector spaces (linear algebra) Thm. If V is a fin. dim'l $\mathbb{R}$-v.s. then $V \cong \mathbb{R}^n$ for some n.

Motivation for category theory: Which properties of "algebraic structures" rely on the specific nature of the objects (e.g. rings v.s. fields, all gps v.s. Symmetric groups) and which ones hold "in general"? (+ how can we avoid proving these "general" facts over and over again?)

~ break ~

Gp work/review: Go thru previous hwk assignments and pick 1 problem (or a pt of one problem) that you'd like to discuss together.

Minute sheet:
- How can I help you prepare for MT3?
- Are you planning to take M371?
- What are 3 words you (now) associate w/ the word "algebra"?