Lec 8/21

Wednesday, August 21, 2019 11:30

HW due Weds, leave it in mailbox of Dr. Edmonds. (30 %)

2 midterms, 4 quizzes, all in recitation. (28 %, 12 %)

Take-home final (probably 48 hrs) (30 %)

<u>More monoids</u>

<u>Def</u>: a monoid has an assoc. binary op. w/ identity. $(M, *, e)$

<u>Ex</u>: $(\mathbb{Z}, \cdot, 1)$ (not a group)

<u>Def</u> let $(M,*,e)$ be a monoid. A submonoid of M is a subset of M that contains e and is closed under $*$.

If N is a submonoid of $(M, *, e)$, then $(N, *, e)$ is a monoid.

eg: $(\mathbb{N}, \cdot, 1) \leq (\mathbb{Z}, \cdot, 1)$

$A^B = A^{\curvearrowright B}$

<u>Ex</u> Let S be a non-empty set.

then $M(S) = S^S$ is a monoid under composition. id = e.

A submonoid of $M(S)$ is called a monoid of transformations.

Def a monoid $(M, *, e)$ is finite if M is finite.

$|M|$ is the "order" of the monoid

ex: $M(S) = |S|^{|S|}$.

Def Let $(M, *, e)$ be a monoid. Then $m \in M$ is invertible if $\exists\, n \in M$ s.t. $nm = e = mn$. n is unique, so call it m^{-1}!

↳ "a unit"

Ex Let $(M, *, e)$ be any monoid.

Then e is invertible w/ inverse e.

Let $m \in M$ be invertible. Then m^{-1} is also invertible.

Def a group is a monoid where every element is invertible.

Ex $(\mathbb{Z}, +, 0)$ vs $(\mathbb{Z}, \cdot, 1)$.

Ex Let S be a non-empty set. Let $U(M(S))$ = invertible transformations of S. (bijections).

Then $U(M(S))$ is a group.

also called the symmetric group of S.

In fact, $U(M)$ is always a group when M is a monoid.

Ex: the group $S_2 = U(M(\{1,2\}))$ has 2 elements: 1 and σ.

$\sigma^2 = 1$.

Def Let M be a monoid (in particular, consider a group)

Then a subgroup of M is a submonoid which is a group.

Prop: Let M be a monoid, let $G \subseteq M$. Then G is a subgp of M iff

(i) $1 \in G$

(ii) $\forall g_1, g_2 \in G$, $g_1 g_2 \in G$

(iii) $\forall g \in G$, $g^{-1} \in G$.

Prop if M is a group, $\overset{\overset{\emptyset}{\neq}}{G} \subseteq M$ is a subgp iff

$\forall x, y \in G$, $y^{-1} x \in G$.