MATH 369 Fall 2025 - Class Notes

9/15/2025

Scribe: Dona Aldossary

Summary: Groups, and subgroups and their axioms of closure, associativity, identity and inverses. Discovering new ways to prove associativity that are easier.

Notes: Proving associativity is annoying, so we can find an easier way to get associativity for free by looking at a group that we know is already associative
Example: $(\mathbb{Z}_4, +)$

$+$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

What if we went and threw out a bunch of things? (expect the identity since it still needs to be closed to be a group)
Lets say 1 doesn't exist, then it is no longer closed, since when we add $3 + 2$ we get 1: $\{\mathbb{Z}_4 \backslash [1]_4\}$ not a group since it is not closed because $[3]_4 + [2]_4 = [1]_4$

$+$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$		$[2]_4$	$[3]_4$
$[1]_4$				
$[2]_4$	$[2]_4$		$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$		$[1]_4$	$[2]_4$

Now lets say 3 doesn't exists, we are left we 4 entries, $[0]_4, [2]_4$ and it is closed since we have the identity 0, and associative since the group is associative. So what is left has identity, associativity and is closed, and everything in it has an inverse, so the smaller collection of things form its own group, a subgroup.
So $\{[2]_4, [2]_4\}$ form a group, which is a subgroup of $(\mathbb{Z}_4, +)$

$+$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$		$[2]_4$	
$[1]_4$				
$[2]_4$	$[2]_4$		$[0]_4$	
$[3]_4$				

Definiiton: $H \subseteq G$ is a subgroup of G if its elements form a group using the same operation as G

Given a group G and a subset $H \subseteq G$ how do we check if H forms a subgroup?
We have to check the four axioms, but now we get the associativity for free, so the properties we need to check are that:

- identity is in H
- H is closed under the operation
- and every element of H has an inverse in H

But there is a simpler way to check this using the 2 criteria subgroup test
Proposition - 2 Criteria Subgroup Test: $H \subseteq G$ is a subgroup if and only if:

- H is nonempty
  - prove that something exists in the subset
- If $a, b \in H$ then $ab^{-1} \in H$
  - this uses all three properties (identity, inverse, and closed) for this to be true

Proof:
If H is a subgroup, we need to show that both properties hold:
Since H is a group $e \in H$, so H is nonempty
Since H is a group, if $a, b \in H$ then $b^{-1} \in H$ and since H is closed, $ab^{-1} \in H$

Now suppose $H \subseteq G$ (subset) that is nonempty and if $a, b \in H$ then $ab^{-1} \in H$:
We get associativity for free from G
Since H is nonempty, we can pick one element from H and called it b
b has an inverse $b^{-1} \in G$
Picking b to be both of these elements a and b we are guaranteed that $bb^{-1} = e \in H$
So H has an identity

Suppose $b \in H$, we need to show that $b^{-1} \in H$
Pick $a = e$, so $ab^{-1} = eb^{-1} = b^{-1} \in H$
So every element has an inverse in H

Last we need to show that if $a, b \in H$ then $ab \in H$
b has an inverse $b^{-1} = c \in H$
So we are gaurenteed that $ac^{-1} = a(b^{-1})^{-1} = ab$
So $ab \in H$
Proposition: If $H \subseteq G$ is finite then H is a subgroup if and only if:

- H is nonempty
- and $ab \in H$ for all $a, b \in H$

Proof: All we need to prove is that if $a \in H$ then $a^{-1} \in \mathbb{N}$
Consider $a^1, a^2, a^3, \ldots$ (infinite powers of a)
All of these powers of a are in H by closure
Since H is finite there must be two equal things in this list such that $a^m = a^n$ for some $m < n$ by the pigeon hole principle
By cancellation (cancelling m times) we get:
$e = a^{n-m}$
$a^{-1} = a^{n-m-1}$
$(a^{n-m-1})a^1 = a^1 a^{n-m-1} = a^{n-m} = e$
So $a^{-1} \in H$
So H is closed under inverses
Since $n > m, n - m > 0, n - m - 1 > -1, n - m - 1 \geq 0$
Problem: Suppose G is a group and $a \in G$ is some element of G what is the smallest subset of G containing a that forms a subgroup
Example: $\{\mathbb{Z}_{20}, +\}$
lets test $a = 15$:
The subgroup has to have identity $[0]_{20}$ and itself $[15]_{20}$
Since $15's$ inverse $[5]_{20}$ it also has to be in the subgroup
The subgroup has to be closed so $[5]_{20} + [5]_{20} = [10]_{20}$ has to be in the group
$\{[0]_{20}, [5]_{20}, [10]_{20}, [15]_{20}\}$ form a subgroup of $\mathbb{Z}_{20}$ and this seems to be the smallest one containing $[15]_{20}$
Proposition: If G is a group and $a \in G$ then the subset consisting of $\{a^1, a^2, \ldots, a^k\}$ and $\{a^{-1}, a^{-2}, \ldots, a^{-k}\}$ and $\{e\}$ equivalently $H = \{a^k | k \in \mathbb{Z}\}$ forms a subgroup of G
Proof: We can use the 2 criteria subgroup test:
Show that H is nonempty:
$a^1 \in H$
So H is nonempty
Now suppose that c, d are any two elements of H
We need to show that $cd^{-1} \in H$:
$c = a^m$ for some $m \in \mathbb{Z}$ and $d = a^n$ for some $n \in \mathbb{Z}$
$d^{-1} = a^{-1} = (a^{-1})^n \in H$
So $cd^{-1} = a^m a^{-n}$
Where a^m is a m times and a^{-n} is a^{-1} n times
So we get a^{m-n}, $m - n \in \mathbb{Z}$
And $a^{m-n} \in H$
So H is a subgroup by the 2 criteria subgroup test
Definiton: If G is a group and $a \in G$ then $< a >= \{a^k | k \in \mathbb{Z}\}$ of G generated by cyclic subgroup by a
Example: $(\mathbb{Z}, +)$, $a = 7$, What is $< 7 >$?
$< 7 >= \{7k | k \in \mathbb{Z}\}$ is the cyclic subgroup generated by 7

If we can find $a \in G$ such that $G =< a >$ then we call G a cyclic group

If $a \in G$ and $a^m = e$ for some $m > 0$ we call m the order of a
If no such m exists we say a has infinite order
If a has infinite order m then $| < a > | = m$
Definition: If G is any finite group, we call $|G|$ the order of G
Example: $G = S_4$, If A, B, C, D are the corners of a square rotating that square clockwise gives us the permutation call it, σ:

$$\sigma = \begin{pmatrix} A & B & C & D \\ B & D & A & C \end{pmatrix} \in S_4 \ , \qquad | < \sigma > | = 4, \qquad \sigma^4 = e \ , \qquad < \sigma > \subseteq S_4$$

$< \sigma >$ is a group of order 4 consisting of all possible rotations in the plane that return the corners to the orginal square