Previously in Math 103a

Lots of stuff! But first, about that final:

Monday Mar 19 11:30am - 2:30 pm
Peterson 103 (This room)

Bring blue book (or paper)
OK to bring 1 sheet written on both sides
Final is **cumulative**, but emphasis will be on later part of course.

Back to the two examples we did not finish last time.

Some important ideas in this course:

1. Groups & subgroups. - what is a group, what's not a group.

Ex $\mathbb{R}^*$ is a group - multiplication
$\mathbb{R}_+^*$ is a group - multiplication
$\mathbb{R}_+^*$ is a subgp of $\mathbb{R}^*$ $\quad \mathbb{R}_+^* < \mathbb{R}^*$
$\mathbb{Z}^*$ is not a group (mult'n) since no inverses
$\mathbb{Q}^*$ is a group, $\mathbb{Q}_+^*$ is subgp of $\mathbb{Q}^*$
$\mathbb{Q}^* < \mathbb{R}^*$ subgroup, since contains inverses & products
$\mathbb{R}$ is a group - addition

$\mathbb{R}^* \subset \mathbb{R}$ but is not a subgroup. Why?

Suppose G_1, G_2 groups with $G_1 \subseteq G_2$ as groups.

Then G_1 is a subgp of $G_2 \iff$ the inclusion $i: G_1 \to G_2$ is a homomorphism

$i(g) = g \quad \forall\, g \in G_1$

(Note that i is 1-1, but not onto if $G_1 \neq G_2$)

To say i is a homomorphism means

$$i(g \cdot g') = g \cdot g'$$

(mult in G_2 on the left; mult in G_1 on the right)

i.e. operation is same in G_1 & G_2.

Cyclic groups

G cyclic if $\exists\, a \in G$ with $G = \{a^j : j \in \mathbb{Z}\}$

If $|G| < \infty$, then $\exists\, n > 0$ s.t.

$a^n = e$ & $a^j \neq e$ $\forall j$ with $0 < j < n$.

If $|G| = n$, then $G \approx \mathbb{Z}_n$. If $|G| = \infty$, then $G \approx \mathbb{Z}$

Important facts about orders for G cyclic, finite

(i) $a \in G \Rightarrow |a| \mid |G|$

(ii) $|a| = |\langle a \rangle|$

(iii) For every k for which $k \mid |G|$, there is a unique subgp of order k.

Ex. $G = \mathbb{Z}_{22}$. Find a generator for the subgp of order 11.

Ans If a is a generator of $\mathbb{Z}_{22}$, the subgp of order 11 is generated by $a^{22/\gcd(22,11)} = a^2$. We could take $a = 1$. The multiplication in $\mathbb{Z}_{22}$ is addition mod 22. So for $a = 1$, $a^2 = 1+1 = 2$.

$\mathbb{Z}_n$ has $\phi(n)$ generators, where ϕ is the phi function: $\phi(n) = \#\{k : \gcd(k,n) = 1 \text{ and } 0 < k < n\}$

$\phi(11) = 10$

Cosets & Normal subgroups.

$H \subset G$ subgroup left coset of $a \in G$ = aH

G = disjoint union of cosets

$|G| = (\#\text{ of left cosets}) \times |H|$

G/H = set of left cosets

G/H is a group $\iff$ H is normal in G.

Ex. All subgroups of $U(n)$ are normal.
Reason: $U(n)$ is abelian.

Combining groups

Direct product $G = G_1 \oplus G_2 = \{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$

Ex 1. Give an example of an abelian group that is not cyclic.

Ans. $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is not cyclic, since $|\mathbb{Z}_2 \oplus \mathbb{Z}_2| = 4$, but $(a,b) \in \mathbb{Z}_2 \oplus \mathbb{Z}_2$ has $|(a,b)| = 2$ or 1 (identity)

Ex 2. Give an example of integer $n, m \geq 2$ such that $\mathbb{Z}_n \oplus \mathbb{Z}_m$ is cyclic

Ans. $G = \mathbb{Z}_n \oplus \mathbb{Z}_m$ cyclic if $\exists (a,b) \in G$ with $|(a,b)| = nm = |G|$.

$$|(a,b)| = \text{lcm}(|a|, |b|) = \frac{|a||b|}{\gcd(|a|, |b|)}$$

Need $|a| = n$, $|b| = m$ & $\gcd(n,m) = 1$

Take e.g. $n = 2$, $m = 3$ $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ cyclic, generated by $(1,2)$.

Ex 3. If G is abelian & G contains 2 subgps of order p, with p prime, show that G contains a subgp isomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_p$

Ans. Let H_1, H_2 subgps of order p. since

$H_1 \cap H_2$ is a subgroup whose order divides p and $H_1 \neq H_2$, must have $H_1 \cap H_2 = \{e\}$

$H_1 H_2$ is a subgp of G, and $H_1 \trianglelefteq H_2$ are both normal subgroups of $H_1 H_2$ (why)

By the theorem on internal direct products,

$H_1 H_2 = H_1 \times H_2 \approx H_1 \oplus H_2 \approx \mathbb{Z}_p \oplus \mathbb{Z}_p$

(since $H_1 \approx \mathbb{Z}_p \trianglelefteq H_2 \approx \mathbb{Z}_p$.

Important groups to have as friends

$\mathbb{Z}$	$\mathbb{Z}_n$, $U(n)$	D_n	S_n	$GL(2,\mathbb{R})$
∞ order	$\lvert\mathbb{Z}_n\rvert = n$ $\lvert U(n)\rvert = \phi(n)$	$\lvert D_n\rvert = 2n$	$\lvert S_n\rvert = n!$	∞ order
abelian	abelian	non abelian	non abelian	non abelian

Important stuff $U(p^n) \approx \mathbb{Z}_{p^n - p^{n-1}}$, p odd prime

$U(s,t) \approx U(s) \oplus U(t)$ if $\gcd(s,t) = 1$

Multiplication in D_n: One subgroup is cyclic of order n. what is it?

n elements of order 2 what are they?

what is $Z(D_n)$?

Homomorphisms & isomorphisms,

homomorphism $\varphi : G_1 \longrightarrow G_2$

mapping that preserves operations

φ is an isomorphism if it is also 1-1 & onto

Ex: $G_1 = \mathbb{R}^*$, $G_2 = \mathbb{R}^+$. $\varphi: G_1 \to G_2$

$\varphi(x) = x^2$

is a homomorphism, but not an isomorphism, since $\varphi(-1) = \varphi(1)$.

First isomorphism theorem:

$\varphi: G_1 \to G_2$ homom $\Longrightarrow$

$G_1/\ker\varphi \approx \varphi(G_1)$

Ex: $\mathbb{R}^*/\{1,-1\} \approx \mathbb{R}^+$.

$\mathrm{Aut}(G) = \{$ isomorphisms $G \to G\}$ group under composition

Thm $\mathrm{Aut}(\mathbb{Z}_n) \approx U(n)$.

Ex1. Show that $\mathrm{Aut}(\mathbb{Z}_{12})$ is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Ex2. Describe the automorphism of $\mathbb{Z}_{12}$ determined by $\varphi(1) = 7$.