Lecture 2

Chapter 3

Def: Let G be a group.
The order of G is the number elements in G
$|G|$ — the order of G.
Note, we can have $|G|=\infty$

$|\mathbb{Z}_n|=n$
$|D_n|=2n$
$|U(n)|=$ # of numbers in $\{0,1,\cdots,n-1\}=\varphi(n)$ that are relatively prime.

not the same

$\mu_n=\{x\in\mathbb{C}\mid x^n=1\}$
$|\mu_n|=n$

example: $\mu_4=\{1,-1,i,-i\}$

Def: The order of an element $g\in G$ is the least positive integer n s.t. $g^n=e$.

If no such n exists, we say that g has infinite order.

Examples:
R_{180} in D_4

$|R_{180}|=2$

What is $|9|$ in $\mathbb{Z}_{13}$? $|9|=13$ $\underbrace{9+9+\cdots+9}_{13\text{ times}}\equiv 0 \bmod 13$

In D_n, all reflections have order 2.

What is $|3|$ in $U(5)$?
$3^1=3\neq 1 \bmod 5$
$3^2=4\neq 1 \bmod 5$
$3^3=2\neq 1 \bmod 5$
$3^4=81\neq 1 \bmod 5$

So $|3|=4$
problem of finding prime elements.
Fix p a prime #, find $k\in\mathbb{Z}_p$ s.t. $|k|=p-1$, $|U(p)|=p-1$

Infinite order:

$\mathbb{Z}$: $|\text{identity}|=1$ by convention

Every non-identity element has infinite order.
$\mathbb{R}^*$ under multiplication. What are the orders of elements?

Claim: only $+1$ & -1 have finite order in $\mathbb{R}^*$.

Pf: $(0,1), (1,\infty)$
$(-1,0), (-\infty,1)$

Let $x \in \mathbb{R}^*$, and suppose x has finite order. Then $x^n = 1$ for some n. Then $x^n - 1 = 0$

But we know that ± 1 are the only roots of unity in $\mathbb{R}$.

What are finite order elements in $\mathbb{C}^*$

$\{\pm 1, \pm i, \cdots\}$ all nth roots of unity for any n.

$\mu_\infty = \{e^{2\pi r} \mid r \in \mathbb{Q}\}$ → this is a group.

Def: (subgroup)
Let G be a group and let $H \subseteq G$. We say H is a subgroup of G if H is a group under the multiplication operation coming from G.
Notation: $H \leq G$ (Compare this w/ the notion of subspace.

Classify all subgroup of $\mathbb{Z}$.
① $\mathbb{Z} \leq \mathbb{Z}$
② $\{e\} \leq \mathbb{Z}$
③ ~~$\mathbb{N} \leq \mathbb{Z}$~~ ? It does not have inverse.

④ evennumbers $= 2\mathbb{Z}$

~~$\mathbb{Z}_n \leq \mathbb{Z}$~~ ? The multiplication is not the operation coming from $\mathbb{Z}$.
Same reason : ~~$U(n) \leq \mathbb{Z}$~~

~~$\{-1, 1\} \leq \mathbb{Z}$~~ There isn't $0 \in \{+1, -1\}$
Multiplication is different.
⑤ $n\mathbb{Z} = \{\text{all multiply of } n\}$

Theorem: All subgroups of $\mathbb{Z}$ look like either $n\mathbb{Z}$ for $n \geq 1$ or are $\{0\}$.

Proof: Sps $S \leq \mathbb{Z}$ and $S \neq n\mathbb{Z}$ and $S \neq \{0\}$. Since $S \neq \{0\}$, there is some $x \in S$ s.t. $x \neq 0$.

Taking inverses if necessary, we may assume $x > 0$. therefore, S has at least one positive element.

Let k be the least positive elements of S.
I claim that $S = k\mathbb{Z}$.
Sps $S \neq k\mathbb{Z}$. Then $\exists r \in S$. s.t. r is not a multiple of k.
But we know $r \equiv S \bmod k$ where $0 < S \leq k-1$
Thus $S = r + m \cdot k$ Thus $S \in S$.
But $S < k$, which contradicts the fact that k is the least positive integer in S.

Thm (One-step subgroup test)
Let G be a group, and let $H \leq G$. Then H is a subgroup of G iff
$H \neq \emptyset$
$\forall a, b \in H,\ ab^{-1} \in H$.

Proof:
"$\Rightarrow$" Assume H is a subgroup
Then $H \neq \emptyset$ because $e \in H$
Also $\forall a, b \in H,\ ab^{-1} \in H$. This is b/c first $b^{-1} \in H$ as H is closed under taking inverses, and then $ab^{-1} \in H$ as H is closed under multi.

"$\Leftarrow$" Assume $\forall a, b \in H$ that $ab^{-1} \in H$ & H & $H \neq \emptyset$.
Let $x \in H$ (which is possible since $H \neq \emptyset$)
Then $x(x^{-1}) \in H$, i.e. $e \in H$

Sps $x \in H$, then setting $a = e$, $b = x$, we see that $x^{-1} \in H$.

Sps $x \in H$, $y \in H$, then setting $a = x$, $b = y^{-1}$, we get $ab \in H$. ∎

Thm (2-Step subgroup test)
Let G be a group, $H \leq G$, then $H \leq G$ iff
$H \neq \emptyset$
$\forall a, b \in H,\ ab \in H$
$\forall c \in H,\ c^{-1} \in H$

Proof: $\Rightarrow$ easy
$\Leftarrow$ Assume $H \neq \emptyset$
$\forall a, b \in H, ab \in H$ and $\forall c \in H,\ c^{-1} \in H$.

Since $H \neq \emptyset$, take any $x \in H$ & will have $x^{-1} \in H$. And $x(x^{-1}) \in H$
So...

∎

Thm (Finite subgroup test)
Assume in addition to the previous assumptions that H is a finite set. Then $H \leq G$ iff $\forall a, b \in H,\ ab \in H$, $H \neq \emptyset$. We can take $x \in H$ and look at its powers.

$$\{x^n \mid n \in \mathbb{N}\} \subseteq H$$

But H is a finite set.
So $x^n = x^m$ for some $n \neq m$.
$x^{n-m} = e$ where $n > m$
$x \cdot (x^{n-m-1}) = e$, so $x^{-1} = x^{n-m-1}$

Def: Let $a \in G$. Define $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$

Thm: $\langle a \rangle \leq G$
- $a^n \cdot a^m = a^{m+n}$ closed multi.
- $(a^n)^{-1} = a^{-n} = (a^{-1})^n$
- $e = a^0$

Def: The center of G is $Z(G)=\{a\in G \mid \forall x\in G, ax=xa\}$

Thm: $Z(G)\leq G$

Proof: $Z(G)\neq\emptyset$ because $e\in Z(G)$

Sps $a,b\in Z(G)$, let $x\in G$ and we want to show that $(ab)x=x(ab)$

But we know $abx=axb=xab$

($b\in Z(G)$ over the first $=$, $a\in Z(G)$ over the second $=$)

Finally, we want to show that $a^{-1}\in Z(G)$, i.e. $\forall x\in G, a^{-1}x=xa^{-1}$.

We know that $ax=xa$

Multiplying on the left by a^{-1} we get $x=a^{-1}xa$.

Multiplying on the right by a^{-1}, we get $xa^{-1}=a^{-1}x$.

The centralizer of a in G.

Def: Let $x\in G$, define the centralizer $C(x)$ by $C(x)=\{a\in G \mid xa=ax\}$

Thm: $C(x)\leq G$

Practice problems

Ch3: (8th ed/7th)

(28/14), (34/20), (36/22), (37/23), (38/24), (52/36), (55/39), (61/45), (68/52)

Cyclic groups (Ch4)

Def: Say G is cyclic if $\exists a\in G$ s.t. $G=\langle a\rangle$, we say a is a generator for G.

Examples: $\mathbb{Z}_n=\langle 1\rangle=\langle n-1\rangle$

$\mathbb{Z}=\langle 1\rangle=\langle -1\rangle$

Ex: Show $U(8)$ is not cyclic

Thm (for when $a^i=a^j$ in cyclic group) — criteria

Assume $G=\langle a\rangle$.

If G is finite, then $a^i=a^j$ iff $i=j$

If G is finite, then $G=\{e,a,a^2,\cdots,a^{n-1}\}$ and $a^i=a^j$ iff $i\equiv j \bmod n$.

In particular, $|G|=n$.

Corollary: $|\langle a\rangle|=|a|$

Cor: $a^k=e$ iff $n\mid k$ i.e. $k\equiv 0 \bmod n$

Prop: baby thm
Thm: provable thm
Lema : helper thm
Cor : immediate consequence of thm