Lecture 10
quiz next week (up to and including ch. 9)
Today: Normal subgroups & factor groups (ch 9)
Next week: Homomorphisms (ch 10)
Group

Normal Subgroups & factorgroups
"Building new groups from old groups"
What we want: Given a group G and $H \leq G$, want to form a group "G/H" that behaves like "G modulo H".
E.g. $G = \mathbb{Z}$
$H = n\mathbb{Z}$
$H \leq G$
We want G/H to be the integers mod n.
Unfortunately, this cannot work for all subgroups.
We need H to be a normal subgroup for this to work.

Def'n: Let G be a group, and let $H \leq G$. We say that H is a normal subgroup of G if $\forall a \in G$, $aH = Ha$.
(each left coset = the corresponding right coset)

Warning: $aH = Ha$ does not mean $ah = ha$ $\forall h \in H$.
Rather $\forall h \in H$, $\exists h' \in H$ s.t. $ah = h'a$
Remark: $h' = aha^{-1}$

Thm: $H \leq G$ is a normal subgroup iff $\{xhx^{-1} \mid h \in H\} = xHx^{-1} \subseteq H$ $\forall x \in G$

Proof: See the Book.

Remark: In the lecture on cosets we saw that $xHx^{-1} = H \iff xH = Hx$

Notation: If H is a normal subgroup we write $H \triangleleft G$

E.g. ① If G is abelian, every subgroup is normal.
Let $H \leq G$, Then $aH = \{ah \mid h \in H\} = \{ha \mid h \in H\} = Ha$
(since G is abelian)

② Let G be a group, then $Z(G) \triangleleft G$
$\forall a \in G$, $aZ(G) = \{ah \mid h \in Z(G)\} = \{ha \mid h \in Z(G)\} = Ha$
(b/c $h \in Z(G)$)

③ Let $S \leq D_n$ given by $S = \{\text{all rotations}\} = \{R_0, R_{\frac{360}{n}}, \cdots, R_{\frac{360(n-1)}{n}}\}$
In fact $S \triangleleft D_n$
Why is this true?
Let's check that $xSx^{-1} \subseteq S$ $\forall x \in D_n$
If x is a rotation, then xSx^{-1} is a set of rotations
So $xSx^{-1} \subseteq S$
If x is a reflection, what can we say about xSx^{-1}?
$xSx^{-1} = \{xrx^{-1} \mid \text{where } r \text{ is a rotation}\} \subseteq S$.
↳ also rotation!

④ Consider $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$ → $\{A \in Mat_{n\times n} \mid \det(A) \neq 0\}$
$\{A \in Mat_{n\times n} \mid \det(A) = 1\}$ = $\{A \in Mat_{n\times n} \mid A^{-1} \text{ exists}\}$

Claim: $SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$

Let $X \in GL_n(\mathbb{R})$. we want to prove $XSL_n(\mathbb{R})X^{-1} \subseteq SL_n(\mathbb{R})$

Proof: Every element of $XSL_n(\mathbb{R})X^{-1}$ is of the form XAX^{-1} for $A \in SL_n(\mathbb{R})$

Then $\det(XAX^{-1}) = \det(X)\det A \det(X)^{-1} = \det(A) = 1$

So $XAX^{-1} \in SL_n(\mathbb{R})$ where $A \in SL_n(\mathbb{R})$.

If $K \subseteq H$, what is HK?
So $HK \subseteq H$ and $H \subseteq HK$
So $HK = H$

Prop:
Sps $H \trianglelefteq G$, $K \leq G$, Let $HK = \{hk \mid h \in H, k \in K\}$
Then $HK \leq G$

Proof: Existence of inverse:
Suppose: $hk \in HK$.
Then $(hk)^{-1} = k^{-1}h^{-1}$
$= (k^{-1}h^{-1}k)k^{-1} \in H$
Since H is normal

Existence of identity $e = e \cdot e \in HK$

Closure under multiplication.
Let $h, h' \in H$, $k, k' \in K$
Then $hkh'k' = h \cdot \underbrace{kh'k^{-1}}_{\in H \text{ b/c } H \text{ is normal}} kk^{-1} = (h \cdot kh'k^{-1}) \cdot (kk')$
($h \cdot kh'k^{-1} \in H$, $kk' \in K$)

∎

Factorgroups:
Let $H \trianglelefteq G$, then the set G/H $(G/H = \{\text{left cosets of } H\} = \{aH \mid a \in G\})$
$= \{Ha \mid a \in G\}$
$= \{\text{right cosets}\}$
when H is normal

is a group under the following multiplication rule:
$\forall a, b \in G \quad (aH) \cdot (bH) = abH$

According to this definition: if $aH = a'H$ and $bH = b'H$, then $(aH)\cdot(bH) = (a'H)\cdot(b'H)$

$abH \overset{?}{=} a'b'H$

So is it true that $abH = ab'H$?
If not, this def'n is not "well-defined", i.e. it doesn't make sense.

Complex numbers: $z \in \mathbb{C}^*$, let $S = \{z \in \mathbb{C}^* \mid |z| = 1\}$ s.t. $|z| = 1$.
Then we know $z = \exp(i\theta)$ for some $\theta \in \mathbb{R}$
Then define $\varphi: S^1 \to \mathbb{R}$ by $\varphi(z) = \theta$ when $z = \exp(i\theta)$
it's one-to-many b/c $\exp(i\theta) = \exp(i(\theta + 2\pi))$, φ is not "well-defined".

Prop: Let $H \trianglelefteq G$, $a, a' \in G$, $b, b' \in G$ s.t. $aH = a'H$, $bH = b'H$. Then $abH = a'b'H$.
i.e. the multiplication in G/H is well-defined.

Proof: Since $aH=a'H$, $a\in a'H$
i.e. $a=a'h_1$ for some $h_1\in H$
Similarly, $b=b'h_2$ for some $h_2\in H$
So $ab=a'hb'h_2=a'b'\underbrace{(b')^{-1}h_1b'}_{H \text{ since } H \text{ is normal}}h_2\in a'b'H$ ∎

This is equivalent to $abH=a'b'H$.

This only works because $H\lhd G$. If not, the multiplication isn't well-defined.

In fact, $H\lhd G$ is equivalent to the multiplication in G/H being well defined.

(non) E.g: Let $G=D_4$, $H=\{R_0, V\}$.
Then $H\leq G$, but H is not normal.
And check that the proposition fails for G/H.
(The mult. will no longer be well-defined).

So we proved that the multiplication in G/H is well-defined. We still need to prove that it's a group.

Proof:
- eH is the identity in G/H because $aH\cdot eH=aeH=aH$ (identity)
- $(aH)^{-1}=a^{-1}H$ ($a^{-1}H\cdot aH=a^{-1}aH=eH=H$) (inverse)
- $(aHbH)cH=abHcH=abcH=aHbcH=aH(bHcH)$ (associability)

E.g:
$4\mathbb{Z}\lhd\mathbb{Z}$
$=\{4k\mid k\in\mathbb{Z}\}$
$=\{\dots,-8,-4,0,4,8,\dots\}$

What does $\mathbb{Z}/4\mathbb{Z}$ look like?
$\mathbb{Z}/4\mathbb{Z}=\{\text{left cosets of } 4\mathbb{Z}\}$
$=\{0+4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z}\}$
analagous to the "aH" notation for additive groups
$=\{\dots-4,0,4,8,\dots\}$
$\{\dots1,5,9,\dots\}$
$\{\dots2,6,10,\dots\}$
$\{\dots3,7,11,\dots\}$

What is $(1+4\mathbb{Z})+(2+4\mathbb{Z})$? $=3+4\mathbb{Z}$
analagous to $aH\cdot bH$

	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$0+4\mathbb{Z}$	$4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$1+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$4\mathbb{Z}$
$2+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$4\mathbb{Z}$	$1+4\mathbb{Z}$
$3+4\mathbb{Z}$	$3+4\mathbb{Z}$	$4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$

This looks like $\mathbb{Z}_4$ Caley Table

We want to prove $\mathbb{Z}/4\mathbb{Z}\simeq\mathbb{Z}_4$

Define: $\varphi:\mathbb{Z}/4\mathbb{Z}\longrightarrow\mathbb{Z}_4$
$\varphi(k+4\mathbb{Z})=k \pmod 4$

Ex: verify that φ is an isomorphism.

Proposition: Let $n \geq 0$, then $\varphi: \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}_n$ defined by $\varphi(k+n\mathbb{Z}) = k \bmod n$ is an isomorphism.

E.g. Consider $S \lhd D_n$ given by $S = \{\text{all rotations}\}$
What does D_n/S look like?
First of all.
$$|D_n/S| = \frac{|D_n|}{|S|} = 2$$

Recall: If $H \leq G$, then $|G/H| = \frac{|G|}{|H|}$
$= |G:H|$
index # of left cosets

We know that D_n/S must be cyclic of order 2.
$D_n/S = \{S, \overrightarrow{rS} \mid r \text{ is any reflection}\}$ (→ all reflection)
Then $S \cdot S = S$
$S \cdot rS = rS$
$rS \cdot S = rS$
$rS \cdot rS = r^2 S = S$

$K = \{R_0, R_{180}\} \lhd D_4$ (in fact, $K = Z(D_4)$)

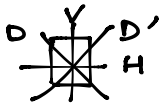
$D_4/K = \{K, R_{90}K, HK, DK\}$
$= \{K, R_{90}K, V''K, D''K\}$
$R_{270}K = R_{270}\{R_0, R_{180}\} = \{R_{270}, R_{90}\}$

	K	$R_{90}K$	HK	DK
K	K	$R_{90}K$	HK	DK
$R_{90}K$	$R_{90}K$	K	DK	HK
HK	HK	DK	K	$R_{90}K$
DK	DK	HK	$R_{90}K$	K

$HK \cdot R_{90}K = H R_{90} K$

What is HR_{90}?

$$\begin{matrix}1&2\\4&3\end{matrix} \xrightarrow{R_{90}} \begin{matrix}2&1\\3&4\end{matrix} \xrightarrow{H} \begin{matrix}1&4\\2&3\end{matrix} = D$$



Look at the § in the book (ch 9) to get a feel for the Cayley tables of factor groups.

Since every group of order 4 is isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ ($\simeq U(8)$)
D_4/K must be isomorphic to one of them.
But D_4/K has no element of order 4.
So $D_4/K \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$ ($\simeq U(8)$)

Applications
Fact: If $H \leq G$, and $|G:H| = 2$ then $H \lhd G$.

Proof: Since $|G:H| = 2$
H has two left cosets: H and $G - H = \{g \in G \mid g \notin H\}$
This is clearly the same as the two right cosets.

Proposition: A_4 has no subgroup of order 6. (Converse of Lagrange's thm is false).

$$|A_4| = 4!/2 = 12$$

Proof: Suppose $H < A_4$ with $|H| = 6$.
Then $|A_4 : H| = 2$, so $H \triangleleft A_4$
So A_4/H has order 2, i.e. $A_4/H \approx \mathbb{Z}_2$.
So everything squares to the identity in A_4/H.
$\forall \alpha \in A_4$, $(\alpha H)^2 = H$
$$(\alpha H)^2 = \alpha^2 H$$
So $\forall \alpha \in A_4$, $\alpha^2 \in H$. All squares of elements $\in H$. Look at the Caley Table for A_4 (Ch5) and you will see that A_4 has 9 squares.
So $9 < 6$, which is a contradiction.

■

Thm: If $G/Z(G)$ is cyclic, then G is abelian.
Proof: If G is abelian, what is $G/Z(G) \Rightarrow G/Z(G)$ is the one-element group
If G is abelian, $Z(G) = G$

Suppose $G/Z(G)$ is cyclic with generator $aZ(G)$.
That means all cosets $xZ(G) = a^n Z(G)$ for some $n \in \mathbb{Z}$. In particular, every element $x \in G$ is equal to $a^n z$ for some $n \in \mathbb{Z}$, $z \in Z(G)$
So let $x, y \in G$, pick $n, m \in \mathbb{Z}$, $z, z' \in Z(G)$ s.t. $x = a^n z$, $y = a^m z'$
We want to prove $xy = yx$.
LHS $= xy = a^n z a^m z' = a^n a^m z z'$ (because $z \in Z(G)$)
RHS $= yx = a^m z' a^n z = a^m a^n z z' = a^n a^m z z' =$ LHS ■

Thm: (Cauchy's Thm for Abelian Group)
Let G be a finite abelian group and let p be a prime number diverging $|G|$.
Then $\exists$ an element of G with order p.

Pf: If $|G| = 2$, then the thm is obvious.
Assume $|G| > 2$, and for induction we'll assume the thm holds for any abelian group of strictly smaller order. (strong induction)
Let $x \in G$, s.t. $x \neq e$. Then $|x| = n > 1$.
Let $n = qm$ where q is some prime.
Then $|x^m| = q$ (So the theorem holds for at least one prime.)
So if $p = q$, we're done. So assume $p \neq q$.
Let $H = \langle x^m \rangle$. Then $H \triangleleft G$ because G is abelian.
And $|G/H| = |G|/q$. Since $p \neq q$, p divides $|G/H|$.
By induction, $\exists\, aH \in G/H$ of order p.
So $a^p \in H$.
If $a^p = e$, then $|a| = p$, and we are done.
otherwise, a^p is a non-identity element in H, which has order q.
So a^p generates H, So $(a^p)^q = e$, and not for any lower power.
So $(a^p)^q = e$, and not for any lower power.
So $|a^q| = p$

■

About HW 2

Classify all finite subgroups of $\mathbb{C}^*$.

1st thing: If $S \leq \mathbb{C}^*$, and $|S|$ is finite, then all elements of S must have finite order.

So if $x \in S$. Then $x^n = 1$ for some $n \in \mathbb{Z}$. That means $x = e^{2\pi i \frac{k}{n}}$ for some $k, n \in \mathbb{Z}$

Sps $|S| = n$, then every element of $x \in S$ must satisfy $x^n = 1$.

So if $|S| = n$, then every element x is of the form $e^{2\pi i k/n}$ where $k \in \{0, 1, 2, \cdots, n\}$

($e^{2\pi i k/n}$: nth root of unity)

$S \subseteq \{e^{2\pi i 0/n}, e^{2\pi i 1/n}, \cdots, e^{2\pi i (n-1)/n}\}$

So $S = \{e^{2\pi i \frac{0}{n}}, \cdots, e^{2\pi i \frac{n-1}{n}}\}$ and this is a subgroup (μ_n) ∎

Let $m, n \geq 1$, $m, n \in \mathbb{Z}$

What's $\langle m \rangle \cap \langle n \rangle$?

$\langle m \rangle = m\mathbb{Z} = \{\text{multiples of } m\}$

$\langle n \rangle = n\mathbb{Z} = \{\text{multiples of } n\}$

We know that $\langle m \rangle \cap \langle n \rangle = \langle k \rangle = k\mathbb{Z}$ (can choose $k \geq 0$)

$x \in m\mathbb{Z} \cap n\mathbb{Z}$ iff x is a multiple of m & a multiple of n.

For all non-trivial subgroup of $\mathbb{Z}$, the generator is the least positive element.

So the generator of $\langle m \rangle \cap \langle n \rangle$ is the least positive integer that is both ....

i.e. $\text{lcm}(m, n)$