Thursday
10/17

3.1 G is a group, $N \trianglelefteq G$.

⑤ The order of $gN \in G/N$ is the smallest positive integer n such that $g^n \in N$.

Ex: $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$

$H = \langle r^2 \rangle = \{1, r^2\}$

left cosets	right cosets
$H = \{1, r^2\}$	$H = \{1, r^2\}$
$rH = \{r, r^3\}$	$Hr = \{r, r^3\}$
$sH = \{s, sr^2\}$	$Hs = \{s, r^2s\} = \{s, sr^2\}$
$(sr)H = \{sr, sr^3\}$	$H(sr) = \{sr, r^2sr\} = \{sr, sr^3\}$

$D_8/H =$

order	
order	

$(rH)^2 =$

$sr^3\}$

the left & right cosets are equal

So, $H \trianglelefteq D_8$.

Thus, D_8/H is a group.

$D_8/H = \{H, rH, sH, (sr)H\}$

order of r in D_8 is 4.

order of rH in D_8/H is 2

$rH \neq H$ ← $r \notin H$

$(rH)^2 = r^2H = H$ ← $r^2 \in H$

element	order
H	1
rH	2
sH	2
$(sr)H$	2

} not cyclic of size 4

$D_8/H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

Up to isomorphism there are only two groups of size 4.

$\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$

↑ cyclic

↑ not cyclic

HW 3.1

3(a) Let A be an abelian group and $B \leq A$.
Then $B \trianglelefteq A$ and A/B is an abelian group.

pf: We already proved that since A is abelian, $B \trianglelefteq A$.
So, A/B is a group.

Let $xB, yB \in A/B$ where $x, y \in A$.

Then,

$$(xB)(yB) = (xy)B = (yx)B = (yB)(xB).$$

$xy = yx$ since A is abelian

So, A/B is abelian. □

Propos
and
Then
proof:
Let
Then
Note
so if

Proposition Let G be a group and let $x \in G$ with $|x| = n$.

Then $|x^a| = \frac{n}{\gcd(a,n)}$ with $a \geq 1$.

proof: Let $|x| = n$ and $a \geq 1$.

Let $d = \gcd(a,n)$.

Then $\gcd(\frac{a}{d}, \frac{n}{d}) = 1$.

Note $|x^a| \geq 1$ and $\frac{n}{d} = \frac{n}{\gcd(a,n)} \geq 1$,

so if we show that $|x^a|$ divides $\frac{n}{d}$ and $\frac{n}{d}$ divides $|x^a|$ then $|x^a| = \frac{n}{d}$.

Claim 1: $|x^a|$ divides $\frac{n}{d}$

Note that $\frac{a}{d} = \frac{a}{\gcd(a,n)} \in \mathbb{Z}$ since $\gcd(a,n)$ divides a.

And, $(x^a)^{\frac{n}{d}} = (x^n)^{a/d} = (1)^{a/d} = 1$.

So, $|x^a|$ divides $\frac{n}{d}$. ← Lemma

Claim 2: $\frac{n}{d}$ divides $|x^a|$

Note that $x^{a|x^a|} = (x^a)^{|x^a|} = 1$. ← Lemma

So, $n = |x|$ divides $a|x^a|$.

Thus, $n \mid a|x^a|$. ← $nk = a|x^a|$ where $k \in \mathbb{Z}$; $(\frac{n}{d})k = (\frac{a}{d})|x^a|$; $\frac{n}{d}, \frac{a}{d} \in \mathbb{Z}$ since $d = \gcd(a,n)$

So, $\frac{n}{d} \mid \frac{a}{d}|x^a|$.

Since $\gcd(\frac{n}{d}, \frac{a}{d}) = 1$, this implies that $\frac{n}{d} \mid |x^a|$. ← $a, b, c \in \mathbb{Z}$, $\gcd(a,b) = 1$, $a \mid bc \rightarrow a \mid c$

Lemma

Let G be a group and $y \in G$. If $y^m = 1$, then $|y|$ divides m

pf: By the division alg,

$m = |y| \cdot q + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < |y|$.

And $y^r = y^{m - |y|q} = y^m (y^{|y|})^{-q} = 1(1)^{-q} = 1$.

Since $y^r = 1$ and $0 \leq r < |y|$, we have $r = 0$.

So, $m = |y|q$.

Thus, $|y|$ divides m. ▨

Theorem (Cauchy's Thm for Abelian groups)

If G is a finite abelian group and p is a prime where $p \mid |G|$. Then G contains an element of order p.

Pf: We induct on $|G|$.

Base case: Suppose $|G|=2$. Then $G=\{1, x\}$ where $x \neq 1$.
Then $x^2=1$ (since if $x^2=x$ then $x=1$).
So, x has order 2.
And 2 is the only prime dividing $|G|=2$.

Suppose G is an abelian group with $|G|>2$ and the theorem is true for all abelian groups of size smaller than $|G|$.

Suppose p is a prime with $p \mid |G|$.
We need to find an element of order p in G.

case 1: Suppose $|G|=p$.

Let $x \in G$ with $x \neq 1$.
Then by Lagrange $|x| = |\langle x \rangle|$ divides $|G| = p$.
Since $x \neq 1$, we know $|x| \neq 1$. So, $|x| = p$ (since p is prime its only divisors are 1 and p)

case 2: Suppose $|G|>p$.

Pick any $x \in G$ with $x \neq 1$.

case 2a: Suppose $p \mid |x|$.

So, $|x| = pk$ where $k \geq 1$.

Then $|x^k| = \frac{|x|}{\gcd(|x|,k)} = \frac{pk}{\gcd(pk,k)} = \frac{pk}{k} = p$.

So, $|x^k|$ has order p.

case 2b: Suppose $p \nmid |x|$.

Let $N = \langle x \rangle$.
Since G is abelian, we have that $N \trianglelefteq G$.
So, G/N is a group.
Since G is abelian, we know G/N is abelian,

Since $p \mid |G|$ we get that p divides

$$|G| = \frac{|G|}{|N|} \cdot |N| = \left|G/N\right| \cdot |N|$$

So, $p \mid |G/N| \cdot |N|$ but $p \nmid |N|$.
This implies that $p \mid |G/N|$.

Here we are using this fact:
If p is a prime and $p \mid ab$,
then $p \mid a$ or $p \mid b$. $(a, b \in \mathbb{Z})$

Since $x \neq 1$, we have that

$|N| = |\langle x \rangle| > 1$.

So, $|G/N| = \frac{|G|}{|N|} < |G|$.

Since G/N is abelian and $|G/N| < |G|$ we can apply our inductive hypothesis to get an element $\hat{y} = yN$ of order p from G/N. Here $y \in G$.

So, $\hat{y} = yN$ has order larger than 1

we know $yN \neq N$. So, $y \notin N$

Also, $\hat{y}^p = N$. So, $y^pN = N$.

Thus, $y^p \in N$

Thus, $\langle y^p \rangle \subseteq \langle y \rangle$

but $\langle y^p \rangle \neq \langle y \rangle$.

$\langle y^p \rangle$: contained in N [$y^p \in N$]

$\langle y \rangle$: not contained in N [$y \notin N$]

So, $|y^p| = |\langle y^p \rangle| < |\langle y \rangle| = |y|$.

Thus, $\frac{|y|}{\gcd(|y|, p)} = |y^p| < |y|$.

So, $\gcd(|y|, p) > 1$.

Since p is prime, $\gcd(|y|, p) = 1$ or p.

So, $\gcd(|y|, p) = p$.

Thus, $p \mid |y|$.

Thus, $|y| = pl$ where $l \geq 1$.

Therefore,

$$|y^l| = \frac{|y|}{\gcd(|y|, l)} = \frac{pl}{\gcd(pl, l)} = \frac{pl}{l} = p.$$

$y|$.

So, y^l has order p and $y^l \in G$.