HW #7

7.5 #6

- Identity: $(0,\bar{0}) \in H$.
- Inverse: if $(a,b) \in H$, then its inverse is $(-a,-b)$. This lives in H since $a \equiv b \pmod 2$
$\Rightarrow -a \equiv -b \pmod 2$.
- Closure: $a \equiv b \pmod 2$, $c \equiv d \pmod 2 \Rightarrow a+c \equiv b+d \pmod 2$.

H is abelian of order 8, so it's either

~~$\mathbb{Z}_8$~~ (but no elts of order 8) or $\mathbb{Z}_4 \times \mathbb{Z}_2$ or ~~$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$~~ (but $(1,1) \in H$ has order 4)

$\therefore H \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

7.5 #7 $\mathbb{Z}_{p^\alpha} \cong G_1 \times G_2$, then

$|G_1| = p^k$, $|G_2| = p^{\alpha-k}$.

An element $(g_1,g_2) \in G_1 \times G_2$ has order

$$\begin{aligned} \operatorname{ord}(g_1,g_2) &\le \operatorname{lcm}(\operatorname{ord}(g_1), \operatorname{ord}(g_2)) \\ &\le \operatorname{lcm}(p^k, p^{\alpha-k}) = p^{\max(k,\alpha-k)} \end{aligned}$$

So for $G_1 \times G_2$ to have an element of

order $p^{\pm\alpha}$, we need $\max(k, q-k) = q$.

$\Rightarrow k = 0$ or q.

$\Rightarrow |G_1| = p^q$ and $|G_2| = 1$ OR vice versa.

$\Rightarrow G_1 \cong \mathbb{Z}_{p^q}$, $G_2 \cong \{e\}$ OR vice versa.

7.5 #8 Note that $\left(g^{(p-1)/2}\right)^2 \equiv 1 \ (p)$, since

$g \in \mathbb{Z}_p^\times$ and $|\mathbb{Z}_p^\times| = p-1$.

$\Rightarrow g^{(p-1)/2} \equiv \pm 1 \ (p)$.

But g generates $\mathbb{Z}_p^\times \Rightarrow \text{ord}(g) = p-1$.

$\therefore g^{(p-1)/2} \equiv -1 \ (p)$.

7.5 #10 $G = \mathbb{Z}_a \times \mathbb{Z}_b$.

$M = \langle (1,1) \rangle$.

Let $H = \langle \left(\frac{a}{d}, \frac{b}{d}\right) \rangle$ where $d = \gcd(a,b)$.

Then • $|H| = d$

• $|M| = \text{lcm}(a,b)$.

- What is $H \cap M$?

$$H \cap M = \left\{ \left(N'\frac{a}{d}, N'\frac{b}{d}\right) \;\middle|\; N'\frac{a}{d} = N'\frac{b}{d} + kb \right\}$$

$$\Rightarrow N'\left(\frac{a-b}{d}\right) = kb$$

$$\Rightarrow N' = \frac{kbd}{a-b} \quad \text{if } a \neq b,$$

$d \mid (a-b)$, $d^2 \nmid (a-b)$, $d^2 \mid kbd \Rightarrow d \mid N'$.

$$\therefore \left(N'\frac{a}{d}, N'\frac{b}{d}\right) = (0,0) \in (\mathbb{Z}_a \times \mathbb{Z}_b).$$

So $H \cap M = \{(0,0)\}$.

- $|H||M| = d \cdot \mathrm{lcm}(a,b) = ab$.

$\therefore G \cong H \times M$.

7.6 #1 (a) $g[a,b]g^{-1} = [gag^{-1}, gbg^{-1}] = (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1})$

$$= gabg^{-1}b^{-1}g^{-1}$$

$$= g[a,b]g^{-1}.$$

(b) N' generated by $[a,b]$ for $a, b \in N$.

So $g[a,b]g^{-1} = [\underbrace{gag^{-1}}_{\in N}, \underbrace{gbg^{-1}}_{\in N}] \in N' \Rightarrow N'$ normal.

7.6 #2 Any finite group has a composition series.

Conversely, suppose G abelian has a composition series

$$G = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_n$$

s.t. $N_i \trianglelefteq N_{i-1}$, N_{i-1}/N_i simple, $N_n = \{e\}$.

G abelian $\Rightarrow N_{i-1}/N_i$ abelian.

Claim: A simple abelian group $\tilde{G}$ is iso to $\mathbb{Z}_p$.

Pf: Let $e \neq x \in \tilde{G}$. If $\langle x \rangle \leq \tilde{G}$, it's a nontrivial normal subgroup, which contradicts that $\tilde{G}$ is simple.

$\therefore \tilde{G} = \langle x \rangle$.

If x has infinite order, then $\tilde{G} \cong \mathbb{Z}$ which is not simple. $\Rightarrow x$ has order n, and $\tilde{G} \cong \mathbb{Z}_n$. Subgroups of $\mathbb{Z}_n$ correspond to divisors of n. Hence $\tilde{G}$ simple $\Rightarrow n = p$ prime. //

So $\exists\, |N_{i-1}/N_i| = p_i$.

$\therefore |G| = p_1 p_2 \cdots p_n$.

7.6 #9

Let $G = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_n = \{e\}$ with N_i/N_{i+1} abelian. Then $N_{n-1}/N_n \cong N_{n-1}$ is abelian, and normal in G by #1.

7.6 #10

Consider

$$G \supseteq G' \supseteq G'' \supseteq G''' \supseteq \cdots$$

Since G is finite, at some stage we have

$G^{(n)} = G^{(n+1)}$ $\quad G^{(n)} \trianglelefteq G$ by #1.