Thursday
11/7

Last time...

Sylow's Theorem part 1

$|G| = p^\alpha m$ where p is prime, $p \nmid m$, $\alpha \geq 1$.

pf: The proof is by induction on $|G|$.

base case $|G| = 2$ ✓

Let $|G| > 2$.

Suppose theorem is true for all groups of size smaller than $|G|$.

Let p be a prime with $|G| = p^\alpha m$, $p \nmid m$, $\alpha \geq 1$.

$\underline{\text{Case 1: } p \mid |Z(G)|.}$ We finished this case.

$\underline{\text{case 2: } p \nmid |Z(G)|.}$

Let $g_1, g_2, \dots, g_r$ be representatives of the distinct conjugacy classes of G not contained in the center. Then,

$$|G| = |Z(G)| + \sum_{i=1}^{r} \underbrace{\frac{|G|}{|C_G(g_i)|}}_{\text{size of conjugacy class containing } g_i}$$

There must be some i with $1 \le i \le r$ where $p \nmid \dfrac{|G|}{|C_G(g_i)|}$.

This is because if p did divide $\dfrac{|G|}{|C_G(g_i)|}$ for all i,

then p would divide

$$|Z(G)| = |G| - \sum_{i=1}^{r} \frac{|G|}{|C_G(g_i)|}.$$

p would divide these terms.

$|G| = p^\alpha m$

For this i, let $H = C_G(g_i)$.

Since $H \leq G$, by Lagrange, $|H| = p^\beta k$ where $0 \leq \beta \leq \alpha$ and $k | m$.

Note that $\frac{|G|}{|H|} = p^{\alpha-\beta}\left(\frac{m}{k}\right)$.

But $p \nmid \frac{|G|}{|H|}$, so $\alpha - \beta = 0$.

So, $\beta = \alpha$ and $|H| = p^\alpha k$ where $k | m$.

Note also that $|H| \neq |G|$ because if so then $g_i \in Z(G)$ because its conjugacy class would have size $1 = \frac{|G|}{|H|} = \frac{|G|}{|C_G(g_i)|}$.

conjugacy class of g is $\{xgx^{-1} \mid x \in G\}$

$g \in G$. $g \in Z(G)$ iff the congugacy class of g has size 1.

Summary so far, $H = C_G(g_i) \leq G$, $|H| = p^\alpha k < p^\alpha m = |G|$.

Using the inductive hypothesis on H, we get a sylow p-subgroup of H, call it P. That is, $P \leq H$ with $|P| = p^\alpha$. Since $H \leq G$, we have $P \leq G$. So, P is a Sylow p-subgroup of G. $\blacksquare$

4550

HW 9

2 (kind of)

$G = \mathbb{Z}_4 \times \mathbb{Z}_4$

$H = \langle(\bar{1},\bar{1})\rangle = \{(\bar{0},\bar{0}),(\bar{1},\bar{1}),(\bar{2},\bar{2}),(\bar{3},\bar{3})\}$ ← $(\bar{0},\bar{0})+H$

$(\bar{1},\bar{0})+H = \{(\bar{1},\bar{0}),(\bar{2},\bar{1}),(\bar{3},\bar{2}),(\bar{0},\bar{3})\}$ ← order 4

$\boxed{(\bar{3},\bar{0})+H =}$ $(\bar{0},\bar{1})+H = \{(\bar{0},\bar{1}),(\bar{1},\bar{2}),(\bar{2},\bar{3}),(\bar{3},\bar{0})\}$ ← $[(\bar{0},\bar{1})+H]+[(\bar{0},\bar{1})+H] = (\bar{0},\bar{2})+H \neq H$ order 4

$(\bar{2},\bar{0})+H = \{(\bar{2},\bar{0}),(\bar{3},\bar{1}),(\bar{0},\bar{2}),(\bar{1},\bar{3})\}$ ← order 2

$\mathbb{Z}_4 \times \mathbb{Z}_4 / H = \{(\bar{0},\bar{0})+H, (\bar{1},\bar{0})+H, (\bar{2},\bar{0})+H, (\bar{3},\bar{0})+H\}$

order 1, order 4, order 2, order 4

Make a homomorphism $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_4 \longrightarrow \mathbb{Z}_4$
that's onto with $\ker(\varphi) = H$.

If we do this then $\mathbb{Z}_4 \times \mathbb{Z}_4 / H = \mathbb{Z}_4 \times \mathbb{Z}_4 / \ker(\varphi) \cong \operatorname{im}(\varphi) = \mathbb{Z}_4$.

Let $\varphi(\bar{a}, \bar{b}) = \bar{a} - \bar{b} = \bar{a} + \overline{-b}$.

Then $\ker(\varphi) = H$.

φ is a homomorphism since

$$\varphi((\bar{a},\bar{b}) + (\bar{x},\bar{y})) = \varphi(\bar{a}+\bar{x}, \bar{b}+\bar{y}) = (\bar{a}+\bar{x}) - (\bar{b}+\bar{y})$$
$$= \bar{a} - \bar{b} + \bar{x} - \bar{y}$$
$$= \varphi(\bar{a},\bar{b}) + \varphi(\bar{x},\bar{y}).$$

$(\bar{3},\bar{0}) + H =$

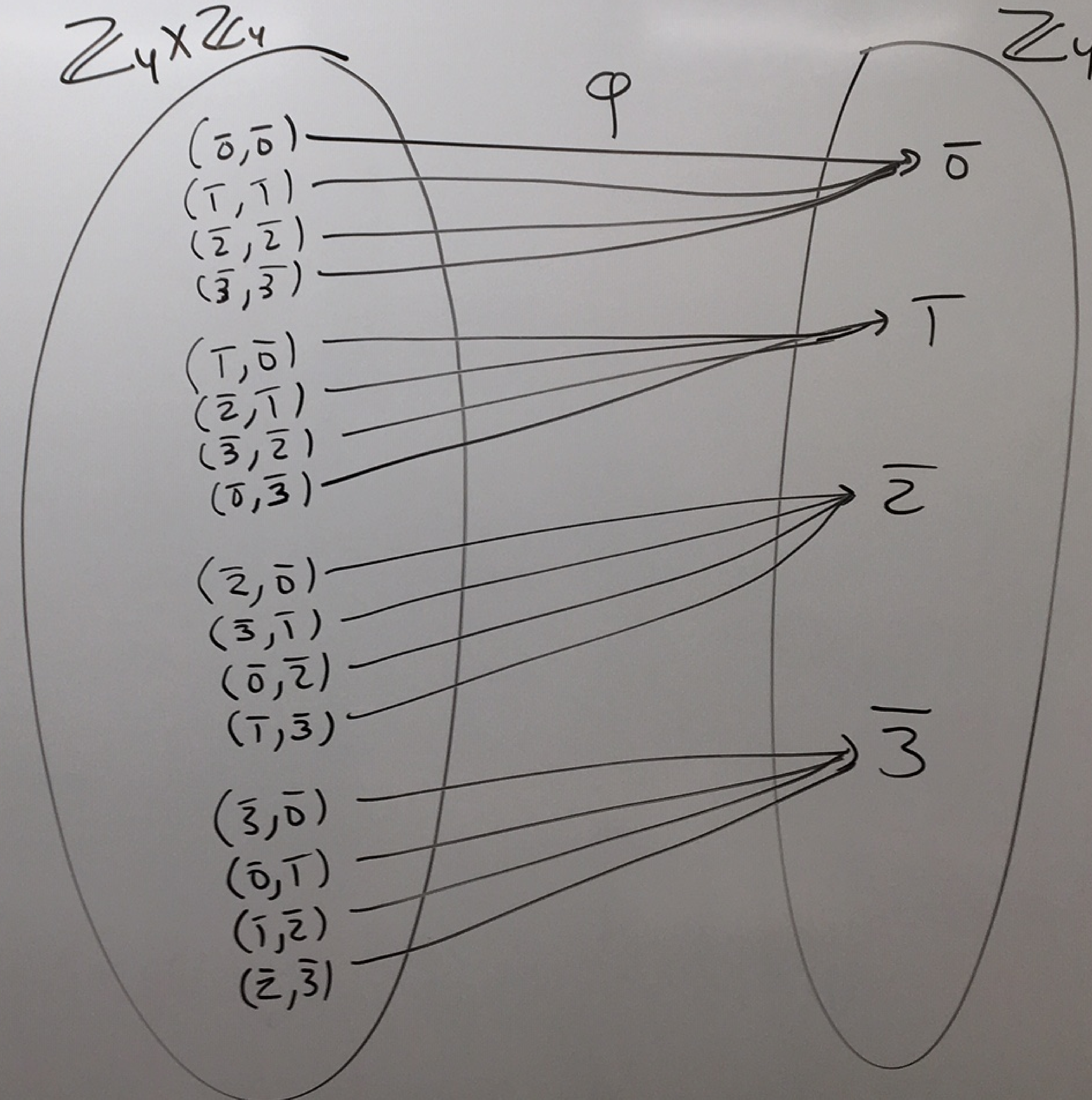
φ is onto

$\varphi(\bar{0},\bar{0}) = \bar{0}$

$\varphi(\bar{1},\bar{0}) = \bar{1}$

$\varphi(\bar{2},\bar{0}) = \bar{2}$

$\varphi(\bar{3},\bar{0}) = \bar{3}$



3.3

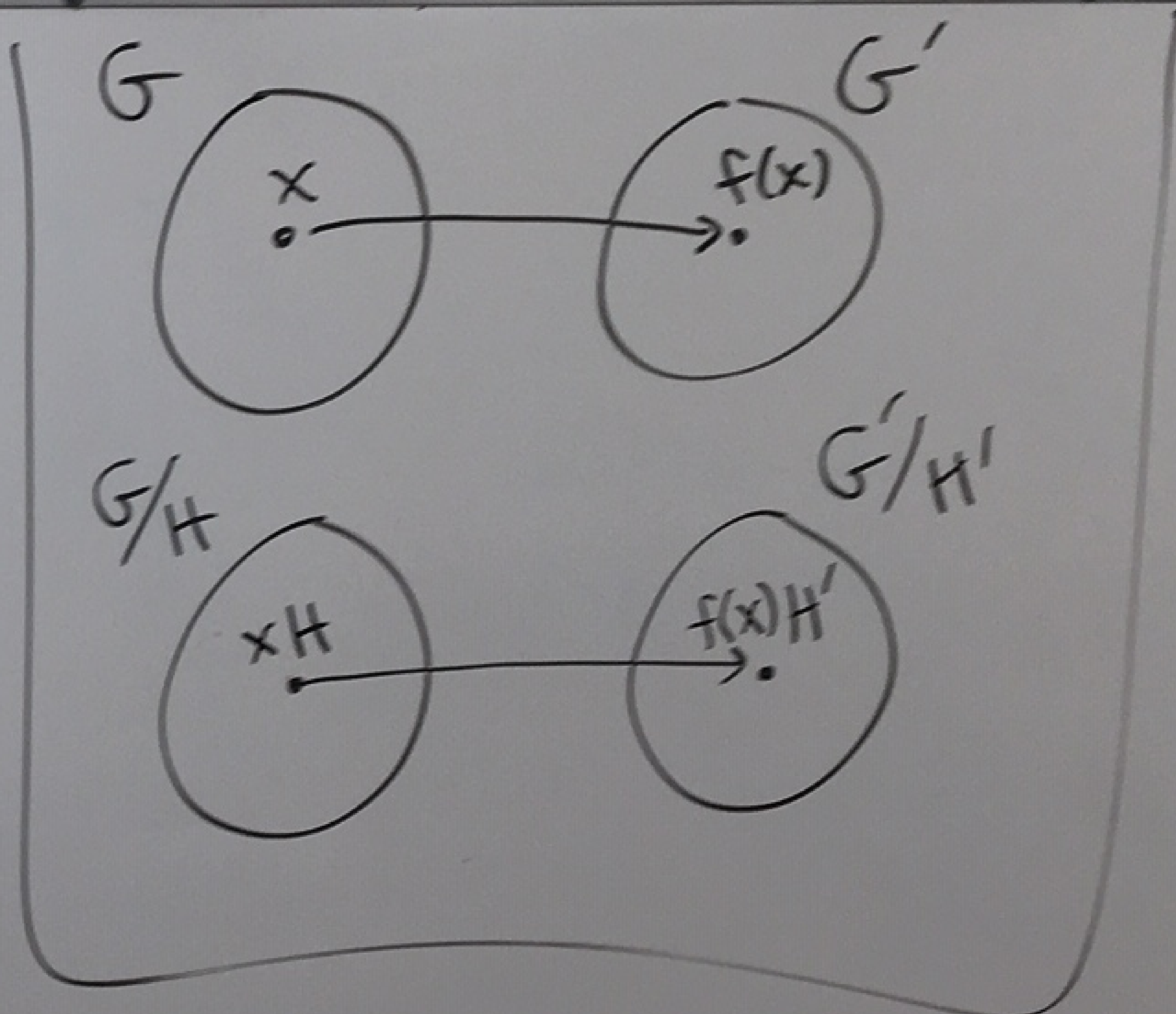
c) G, G' are groups, $H \trianglelefteq G$, $H' \trianglelefteq G'$

$f: G \to G'$ is a homomorphism

with $f(H) \subseteq H'$.

Prove there exists a homomorphism

$g: G/H \to G'/H'$.



<u>proof:</u> Define $g: G/H \to G'/H'$

where $g(xH) = f(x)H'$.

Let's show that g is well-defined and g is a homomorphism.

g is well-defined

Let $xH, yH \in G/H$ with $xH = yH$.

We need to show that $g(xH) = g(yH)$.

Since $xH = yH$ we have $y^{-1}x \in H$.

Since $f(H) \subseteq H'$, we have $f(y^{-1}x) \in H'$.

So, $f(y)^{-1} f(x) \in H'$.

Thus, $f(x)H' = f(y)H'$.

And therefore, $g(xH) = g(yH)$.

$aH = bH$
iff
$b^{-1}a \in H$
iff
$a \in bH$

g is a homomorphism

Let $xH, yH \in G/H$. Then,

$$\begin{aligned} g((xH)(yH)) &= g((xy)H) \\ &= f(xy)H' \\ &= f(x)f(y)H' \\ &= (f(x)H')(f(y)H') \\ &= g(xH)g(yH). \end{aligned}$$

f is a homomorphism

3.3

c) (

proo

wh

Theorem: Let G be a group with $|G| = p^{\alpha} m$ where p is prime, $\alpha \geq 1$, $p \nmid m$.

Let n_p be the number of Sylow p-subgroups of G.

1. Let P be a Sylow p-subgroup of G. Then $P \trianglelefteq G$ iff $n_p = 1$.
2. If G is abelian, then $n_p = 1$.

pf:

1. Let P be a sylow p-subgroup of G. Then by part 2 of Sylows theorem the set of all Sylow p-subgroups is $S = \{ gPg^{-1} \mid g \in G \}$.

   $P \trianglelefteq G$ iff $gPg^{-1} = P$ for all $g \in G$
   iff $S = \{P\}$
   iff $n_p = 1$.

2. Let P be a sylow p-subgroup. If G is abelian, then $P \trianglelefteq G$. By part 1, $n_p = 1$. $\blacksquare$