Thm 21 $U_n = \{ a \mid a \in \mathbb{Z}_n \text{ and } a^{-1} \in \mathbb{Z}_n \text{ s.t. } a \cdot a^{-1} = 1 \}$

Things we know:

- $\mathbb{Z}_n$ is closed under $\cdot$
- $1 \in \mathbb{Z}_n$ and $1 \cdot a = a \cdot 1 = a$: 1 is the mult. identity
- $\cdot$ is associative in $\mathbb{Z}_n$

- $\cdot$ is associative in U_n because it is associative in $\mathbb{Z}_n$

The mult. identity, 1, is its own inverse:

$1 \cdot 1 = 1$

So $1 \in U_n$

Let $a, b \in U_n$

so $a^{-1}, b^{-1} \in \mathbb{Z}_n$ s.t.

$a \cdot a^{-1} = 1$, $b \cdot b^{-1} = 1$

so $a^{-1} \cdot b^{-1} \in \mathbb{Z}_n$

and

$ab(a^{-1}b^{-1}) = 1$

So $ab \in U_n$

Let $a \in U_n$

then $a^{-1} \in \mathbb{Z}_n$ s.t.

$a \cdot a^{-1} = 1$

so a^{-1} has an inverse: a

so $a^{-1} \in U_n$

Thm 25: Let order of a be k

$a^n = e$

Let $gcd(n,k) = d$

then $d = nu + kv$

$a^d = a^{nu+kv}$

$= a^{nu} \cdot a^{kv}$

$= (a^n)^u \cdot (a^k)^v$

$= e \cdot e = e$

$a^d = e$

k is the order of a

so if $a^d = e$ and $d > 0$

then $\boxed{k \leq d}$

d is the greatest Common divisor

$d \leq d$

$d | k$

$\boxed{d \leq k}$

$d = k$

$d | n$, so $\boxed{k | n}$

34.5 Given groups G, H and a homomorphism $f: G \to H$

then $f(e_G) = e_H$

(e_G: Identity for G; e_H: identity for H.)

So if $a \in G$

$e_G \cdot a = \boxed{a \cdot e_G = a}$

so $f(a \cdot e_G) = f(a)$

$\to f(a) \cdot f(e_G) = f(a)$

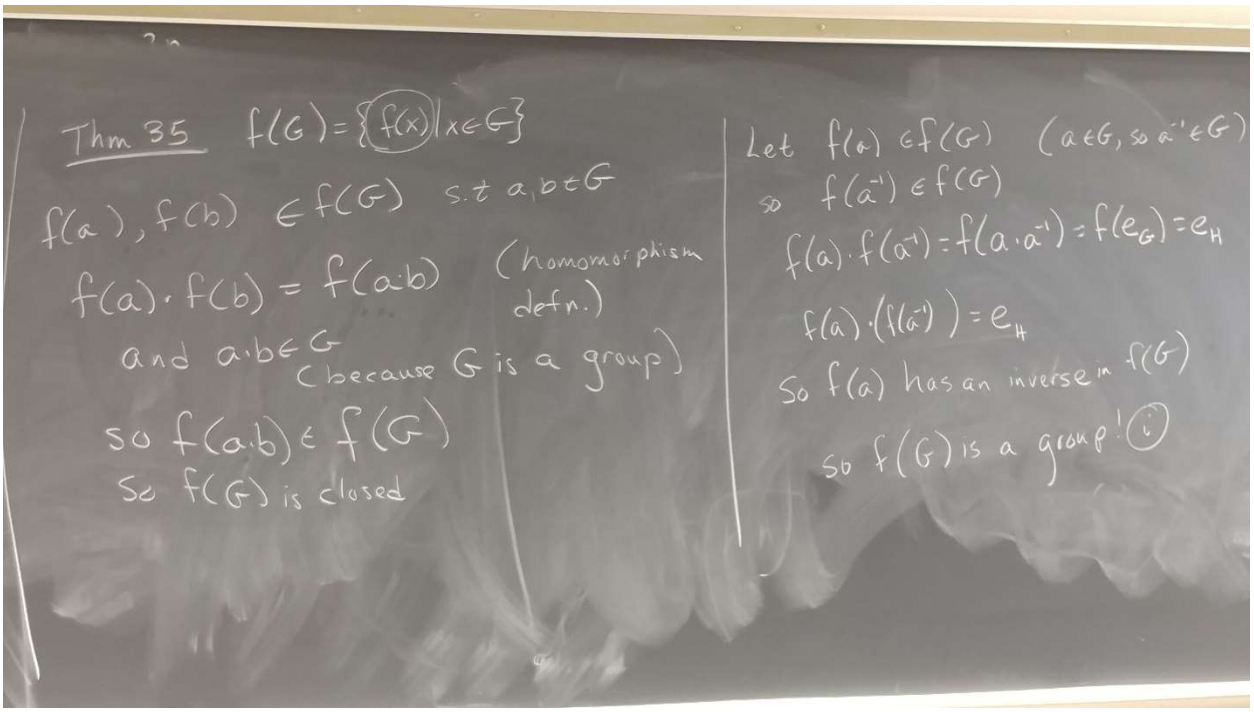
notice $f(a) \in H$

$\to$ so $(f(a))^{-1} \in H$

so $(f(a))^{-1} \cdot (f(a)) \cdot f(e_G) = (f(a))^{-1} \cdot (f(a))$

$e_H \cdot f(e_G) = e_H$

$f(e_G) = e_H$


Thm 35 $f(G) = \{f(x) \mid x \in G\}$
$f(a), f(b) \in f(G)$ s.t $a, b \in G$
$f(a) \cdot f(b) = f(a \cdot b)$ (homomorphism defn.)
and $a \cdot b \in G$ (because G is a group)
so $f(a \cdot b) \in f(G)$
So $f(G)$ is closed
Let $f(a) \in f(G)$ ($a \in G$, so $a^{-1} \in G$)
so $f(a^{-1}) \in f(G)$
$f(a) \cdot f(a^{-1}) = f(a \cdot a^{-1}) = f(e_G) = e_H$
$f(a) \cdot (f(a^{-1})) = e_H$
So $f(a)$ has an inverse in $f(G)$
so $f(G)$ is a group! (i)