Ungraded.

§1.11 - 1 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
The elements are $([a]_2, [b]_4)$
which has order n, when r is the
smallest integer s.t. $ar \equiv 0 \bmod 2$
$br \equiv 0 \bmod 4$

So: order 1 $([0]_2, [0]_4)$
order 2 $([1]_2, [0]_4), ([0]_2, [2]_4)$
$([1]_2, [1]_4)$.

The other 4 elements have order 4

§1.11-3 The order of $(2,6)$ in $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.
Smallest $r > 1$. $(2r, 6r) = (0,0)$.
$2r \equiv 0 \bmod 4$
$6r \equiv 0 \bmod 12$; by inspection, $r = 2$.

§1.11-5 The order of $(8,10)$ in $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$
Again, $8r \equiv 0 \bmod 12$, $10r \equiv 0 \bmod 18$.
So $12 \mid 8r$, $18 \mid 10r$. If $\frac{10r}{18} = \frac{5r}{9}$
is an integer, then $9 \mid r$, and $8 \cdot 9 \equiv 0 \bmod 12$,
so $r = 9$.

§1.13-7 $\phi: \mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}$. $\phi(1) \neq [1]_7$
$\phi(1) = [4] \Rightarrow \phi(25) = 100 \bmod 7 = [2]_7$.
$\ker \phi = \{x : \phi(x) = [0]_7\}$
$= \{x : 4x \equiv 0 \bmod 7\} = \{x : x \equiv 0 \bmod 7\}$
$= 7\mathbb{Z}$.

§1.13-9 $\phi: \mathbb{Z} \to S_8$
so $\phi(1) = (1426)(257) = (142576)$
(tricky!) So $\phi(1)$ is a cycle of order 6
and so $\phi(6) =$ identity. $\phi(n) =$ identity
$\iff 6 \mid n$, so $\ker \phi = 6\mathbb{Z}$.
$\phi(20) = (142576)^{20} = (142576)^{3 \cdot 6 + 2}$
$= (142576)^2 = (127)(456)$

Math 417
HW 6
Due 3/8/19

1. §1.10-37
Actually a big deal
There are two parts.

1) Suppose $a \in G$ and $a \neq e$.
Then $\langle a \rangle$ is a bigger subgroup than $\{e\}$
By hypothesis. This means that
$\langle a \rangle$ must be all of G. This is
true for all $a \in G$, $a \neq e$.
Thus G must be a cyclic group.

2) Suppose G is a cyclic group
of order n, and $n = rs$, $r, s > 1$.
Then $G = \{e, a, a^2, \ldots, a^{rs-1}\}$
and $\langle a^r \rangle = \{e, a^r, a^{2r}, \ldots, a^{(s-1)r}\}$
is a proper subgroup, which
is impossible by hypothesis.
Thus n must be prime.

3) Suppose G is an infinite group.
We still know it's cyclic, so it's
$\{e, a, a^{-1}, a^2, a^{-2}, \ldots\}$
already $\{e, a^2, a^{-2}, a^3, a^{-3}, \ldots\}$
is a proper subgroup
I will not "count" 3), since we
really haven't talked about
infinite groups. If you got this
part, it will be $\frac{1}{4}$ pt extra credit

2a. §1.11-2 $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
elements are $([a]_3, [b]_4)$. Its
order is the smallest positive integer
r so that $ra \equiv 0 \bmod 3$, $rb \equiv 0 \bmod 4$.

$(0,0) \to 1$ $(1,0) \to 3$ $(2,0) \to 3$
$(0,1) \to 4$ $(1,1) \to 12$ $(2,1) \to 12$
$(0,2) \to 2$ $(1,2) \to 6$ $(2,2) \to 6$
$(0,3) \to 4$ $(1,3) \to 12$ $(2,3) \to 12$

4-generators: $([a]_3, [b]_4)$ if $a = 1$ or 2
$b = 1$ or 3

2. ord of $(2,3)$ in $\mathbb{Z}_6 \times \mathbb{Z}_{15} = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$. We could use the previous argument. (smallest r so that $2r \equiv 0 \bmod 6$, $3r \equiv 0 \bmod 15$ or just write out multiples

$(2,3), (4,6), (6,9), (8,12), (10,0),$
$(0,3), (2,6), (4,9), (6,12), (8,0),$
$(10,3), (0,6), (2,9), (4,12), (6,0)$

order $= 15$.

3a. I'll take powers of $[2]_{11}$

$1, 2, 4, 8, 16 \equiv 5, 10, 20 \equiv 9, 18 \equiv 7,$
$14 \equiv 3, 6, 12 \equiv 1$ ✓

so $\{1,2,4,8,5,10,9,7,3,6\}$ is the set of powers of 2 and is $(\mathbb{Z}/11\mathbb{Z})^*$

3b. The order of 2^k is $\frac{10}{\gcd(k,10)}$

so 2^k is a generator if $\gcd(k,10) = 1$ i.e. $k \equiv 1, 3, 7, 9$. Reading from the list, $2^1 = 2$, $2^3 = 8$, $2^7 \equiv 7$, $2^9 \equiv 6$

These are the generators of $(\mathbb{Z}/11\mathbb{Z})^*$.

3c. A generator for $C_{10} = (\mathbb{Z}/10\mathbb{Z})$ is $[1]_{10}$; in an isomorphism, it maps to a generator

ϕ_1	ϕ_2
$[0]_{10} \to [1]_{11}$	$\to [1]_{11}$
$[1]_{10} \to [2]_{11}$	$\to [8]_{11}$
$[2]_{10} \to [4]_{11}$	$\to [9]_{11}$
$[3]_{10} \to [8]_{11}$	$\to [6]_{11}$
$[4]_{10} \to [5]_{11}$	$\to [7]_{11}$
$[5]_{10} \to [10]_{11}$	$\to [10]_{11}$
$[6]_{10} \to [9]_{11}$	$\to [3]_{11}$
$[7]_{10} \to [7]_{11}$	$\to [2]_{11}$
$[8]_{10} \to [3]_{11}$	$\to [5]_{11}$
$[9]_{10} \to [6]_{11}$	$\to [7]_{11}$

I'll pick ϕ_2 as the one that sends the generator to the generator you could also pick $[7]_{11}$ or $[6]_{11}$ here

---

4. As one more class let's check $a \circ b = a + b - ab$ is a group.

$3 \circ b = a + 3 - 3a = 3 - 2a$.

Identity $= 0$, $3 \circ 3^{-1} = 0 \Rightarrow 3^{-1} = \frac{3}{2}$

$\frac{3}{2} \circ b = \frac{3}{2} - \frac{1}{2}b$

Powers of 3

$3, 3 \circ 3 = -3, 3 \circ -3 = 9, 3 \circ 9 = 15,$
$3 \circ (-15) = 33, 3 \circ 33 = -63, \ldots$

$3^{-1} = \frac{3}{2}$, $\frac{3}{2} \circ \frac{3}{2} = \frac{3}{4}$, $\frac{3}{2} \circ \frac{3}{4} = \frac{9}{8}$,
$\frac{3}{2} \circ \frac{9}{8} = \frac{15}{16}$.

Discussion. Certainly the powers of 3^{-1} seem to be going to 1.

$\frac{3}{2} = 1 + \frac{1}{2}$ $\frac{3}{4} = 1 - \frac{1}{4}$, $\frac{9}{8} = 1 + \frac{1}{8}$, $\frac{15}{16} = 1 - \frac{1}{16}$

and you may notice.

$3 = 1 + 2$, $-3 = 1 - 4$, $9 = 1 + 8$, $-15 = 1 + 16$.

The pattern seems to be $1 - (-2)^n$.

We saw (in class) that

$(1-a) \circ (1-b) = (1-a) + (1-b) - (1-a)(1-b)$
$= 1 - a + 1 - b - 1 + a + b - ab = 1 - ab$.

so $(1 - (-2)^n) \circ (1 - (-2)^m) =$
$(1 - (-2)^{m+n})$

and this is the group!

---

5. Suppose $G = C_p = \langle a \rangle$ and $H = C_q = \langle b \rangle$ and ϕ is a homomorphism from G to H. What is $\phi(a)$?

$\phi(a) = b^i$ for some i, because $\phi(a) \in H$.

Because ϕ is a homomorphism, $\phi(a^k) = (b^i)^k = b^{ki}$ for all k. In particular, $\phi(a^p) = b^{pi}$. But $a^p = e_G$ and $\phi(e_G) = e_H$, so $b^{pi} = e_H \Rightarrow q \mid pi$. But p, q are diff. primes, so $q \mid i$ and $\phi(a) = b^i = e_H$.

; cont'd. Thus, the only group homomorphism for C_6 to C_4 is the trivial or "boring" one.

6a. Since H is a normal subgroup of G, $gH = Hg$. That is,

$g\{e, a, b\} = \{e, a, b\}g$

as sets.

$\{g, ga, gb\} = \{g, ag, bg\}$.

If $ga \neq ag$, then we must have $ga = bg$, because ga has to be in Hg and that's the only choice.

6b. $H = \{e, a\}$ is a normal subgroup of G if and only if, for every $g \in G$, $gH = Hg$; that is

$\{g, ga\} = \{g, ag\}$.

That is, if and only if $ga = ag$.

Notes on LCM.

Given positive integers m, n, the least common multiple of m, n $LCM(m, n)$ is the smallest integer r such that $m \mid r$ and $n \mid r$. What follows are two approaches to prove.

$$LCM(m, n) = \frac{mn}{\gcd(m, n)}$$

(i). Let $g = \gcd(m, n)$, so $m = gm'$, $n = gn'$ for integers m', n'.

Claim $\gcd(m', n') = 1$.

Pf. If $k \mid m'$ and $k \mid n'$, then $m' = km''$, $n' = kn''$ and $m = gkm''$, $n = gkn''$, so $gk \mid m, n$ but g was the greatest common divisor, so $gk \leq g \Rightarrow k = 1$.

Now suppose $m \mid r$ and $n \mid r$. Since $m \mid r$, $r = mt$ for integer $\Rightarrow r = gm't$. But $n \mid r$, so $r = n \cdot u = gn'u$, so

$gm't = gn'u \Leftrightarrow m't = n'u$.

but $m' \mid m't$, so $m' \mid n'u$ and $\gcd(m', n') = 1 \Rightarrow m' \mid u \Rightarrow u = m'v$

$\Rightarrow r = gn'u = gn'm'v$.

The smallest value is found by taking $v = 1$, so $LCM(m, n) = gn'm'$

$= \frac{(gn')(gm')}{g} = \frac{m \cdot n}{g}$. ✓

(ii) $a \mid b \Leftrightarrow \nu_p(a) \leq \nu_p(b)$ for all primes p. So $g \mid m, n \Leftrightarrow \nu_p(g) \leq \nu_p(m), \nu_p(n)$, so the largest g has $\nu_p(g) = \min(\nu_p(m), \nu_p(n))$. Similarly, $m, n \mid r \Leftrightarrow \nu_p(r) \geq \nu_p(m), \nu_p(n) \Rightarrow \nu_p(LCM) = \max(\nu_p(m), \nu_p(n))$ and $\nu_p(g) + \nu_p(LCM) = \min + \max$

But $\min(r, s) + \max(r, s) = r + s$