Due 4/9:
G1 (present): page 150: 1, 7, 8
G2 (present): page 150: 3, 6, 9, 12, 14 (me: 3, 14)
All (turn in): page 150: 17, 19, 29, 36 (me)
Due 4/11:
Present: page 167: 20
All (turn in): page 167: 1, 22

Page 150

Exercise 3

Let H = {0, ± 3, ± 6, ± 9...}. Rewrite the condition $a^{-1}b \in H$ given in property 6 of the lemma on page 139 in additive notation. Assume that the group is Abelian. Use this to decide whether or not the following cosets of H are the same.

Property 6: $aH = bH$ iff $a^{-1}b \in H$
Rewritten: $a + H = b + H$ iff $a^{-1} + b \in H$

   a. **11 + H and 17 + H**: $-11 + 17 = 6 \in H$, so yes.

   b. **-1 + H and 5 + H**: $1 + 5 = 6$ mem H, so yes.

   c. **7 + H and 23 + H**: $-7 + 23 = 16 \notin H$, so no.

Exercise 14

Let C^* be the group of nonzero complex numbers under multiplication and let H = {a + bi $\in$ C^* : $a^2 + b^2 = 1$}. Give a geometric description of the cosets (3 + 4i)H and (c + di)H.
Well,
$(3 + 4i)H = \{(3 + 4i)h : h \in H\}$
$(3 + 4i)H = \{(3 + 4i)(a + bi) : a + bi \in C^*, a^2 + b^2 = 1\}$
$(3 + 4i)H = \{3a + 4ai + 3bi - 4b: a + bi \in C^*, a^2 + b^2 = 1\}$
$(3 + 4i)H = \{3a + (4a + 3b)i - 4b: a + bi \in C^*, a^2 + b^2 = 1\}$
thus,
$(c + di)H = \{ca + (da + cb)i - db: a + bi \in C^*, a^2 + b^2 = 1\}$
$(c + di)H = \{(ca - db) + (da + cb)i: a + bi \in C^*, a^2 + b^2 = 1\}$
It looks like the subset H just indicates the elements that create a unit circle.
When we multiply by some real constant > 1, we just get a coset that represents a bigger circle.
When we multiply by some complex constant (e.g. 2i), we just get a coset that represents a flipped circle (where x, y becomes y, x), and if the complex constant has a scaling factor (e.g. 2), then the circle grows by that factor.
As far as the description of a coset with a positive real and positive complex part, I think it transforms it into an ellipse.

Exercise 17

Let G be a group with |G| = pq: p, q are prime. Prove that every proper subgroup of G is cyclic.
Let H be a proper subgroup of G.
Since G is finite, |H| divides |G|.

Case:

i) |H| = 1: Then H is cyclic by default.

ii) |H| ≠ 1: Then by the fundamental theorem of arithmetic, |H| = t: t ∈ {p, q}

   Notice: |H| > 1.

   Let h ∈ H: h ≠ e.

   Then $1 < |<h>| \leq |H|$.

   Since H is finite, $|<h>|$ divides |H|.

   Since |H| is prime, its factors are only 1 and |H|.

   Since $|<h>| \neq 1$, this implies that $|<h>| = |H|$.

   Hence, H must be cyclic.

Exercise 19

Compute 5^{15} mod 7 and 7^{13} mod 11.

Fermat's Little Theorem: For every integer a and prime p, a^p mod p = a mod p

$$5^{15} \mod 7 = 5^3 * 5^5 \mod 7$$

Exercise 29

Let |G| = 33. What are the possible orders for the elements of G? Show that G must have an element of order 3.

Well, if |G| = 33, then for g ∈ G, |g| must be some factor of 33: 1, 3, 11, or 33.
If |g| = 1, then g is the identity, which exists in every group.
|g| cannot be 33, since that's the size of the group. The maximum order for an element is n − 1 where n is the size of the group.
So the possible orders are 1, 3, and 11.
Let's suppose this group contains elements only of orders 1 and 11. In order for there to be 33 elements, there has to be more than one element of order 11.
However, the moment there are two elements of order 11, we can look at their cross product and see that we get more than 33 elements - a contradiction.
So, we must have an element of order 3.

Exercise 36

Let G be a group and |G| = 21. If g ∈ G and g^{14} = e, what are the possibilities for |g|?

Well, since g is a generator for H, a cyclic subgroup of G, that means that |H| must be a factor of |G|.
Since |G| = 21 and 14 doesn't divide 21, |H| must be some factor of both 21 and 14, but lower than 14.
Those possibilities are: 1, 7

Exercise 20

Find a subgroup of $\mathbf{Z}_{12} \bigoplus \mathbf{Z}_{18}$ that is isomorphic to $\mathbf{Z}_9 \bigoplus \mathbf{Z}_4$.

Well, we know that $Z_9 \bigoplus Z_4$ is isomorphic to Z_{36} since 9 and 4 don't share any common factors (by Theorem 8.2).

So, let's just pick two elements with orders 4 and 9.

I think 3 from Z_{12} will work for an order of 4, and 2 from Z_{18} will work for an order 9.

So our generator becomes $(3, 2) \in Z_{12} \bigoplus Z_{18}$, and the group isomorphic to $Z_9 \bigoplus Z_4$ is simply $< (3, 2) >$

Exercise 22

Determine the number of elements of order 15 and the number of cyclic subgroups of order 15 in $\mathbf{Z}_{30} \bigoplus \mathbf{Z}_{20}$.

By Theorem 8.1, the number of elements of order 15 is the number of elements $(a, b) \in Z_{30} \bigoplus Z_{20}$ such that $15 = |(a, b)| = \text{lcm}(|a|, |b|)$

Case:

  i) $|a| = 1$, $|b| = 15$ - in this case there are 1 * 3 = 3

 ii) $|a| = 15$, $|b| = 1$ - in this case there are 15 * 1 = 15

iii) $|a| = 15$, $|b| = 15$ - in this case there are 15 * 3 = 45

 iv) $|a| = 3$, $|b| = 5$ - in this case there are 3 * 5 = 15

  v) $|a| = 5$, $|b| = 3$ - in this case there are 5 * 1 = 5

So the sum of all of those is 83.

The number of cyclic subgroups of order 15 in $Z_{30} \bigoplus Z_{20}$ is going to be $\frac{83}{\phi(15)}$