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 ∈ 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 ∈ H}
(3 + 4i)H = {(3 + 4i)(a + bi) : a + bi ∈ C^*, $a^2 + b^2 = 1$}
(3 + 4i)H = {3a + 4ai + 3bi - 4b: a + bi ∈ C^*, $a^2 + b^2 = 1$}
(3 + 4i)H = {3a + (4a + 3b)i - 4b: a + bi ∈ C^*, $a^2 + b^2 = 1$}
thus,
(c + di)H = {ca + (da + cb)i - db: a + bi ∈ C^*, $a^2 + b^2 = 1$}
(c + di)H = {(ca - db) + (da + cb)i: a + bi ∈ 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.
I think the cosets scale it by ||c + di||.

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) $|H| \neq 1$: Then by the fundamental theorem of arithmetic, $|H| = t$: $t \in \{p, q\}$

Notice: $|H| > 1$.

Let $h \in H$: $h \neq e$.

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, $a^p \equiv a \bmod p$.
And, if a is not divisible by p, then $a^{p-1} \equiv 1 \bmod p$ (which is 1)
Also, if a and n are relatively prime, then $a^{\phi(n)} \bmod n \equiv 1$ (from problem 18 in the book)

$$\begin{aligned} 5^{15} \mod 7 &= (5^7)(5^7)5^1 \mod 7 \\ &\equiv (5)(5)5 \mod 7 \text{ (by Fermat's Little Theorem)} \\ &\equiv 125 \mod 7 \\ &= 6 \end{aligned}$$

$$\begin{aligned} 7^{13} \mod 11 &= (7)^3(7)^{10} \mod 11 \\ &\equiv 7^3(1) \mod 11 \text{ (by Fermat's Little Theorem)} \\ &\equiv 147 \mod 11 \\ &= 4 \end{aligned}$$

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 $g \in G$, $|g|$ 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

Page 167

Exercise 1

Prove that the external direct product of any finite number of groups is a group.
Let G_1, G_2, ... G_n be a finite collection of groups.
Then $G_1 \bigoplus G_2 \bigoplus ... \bigoplus G_n = \{(g_1, g_2, ... g_n) : g_i \in G_i\}$
and $(g_1, g_2, ... , g_n)(g_1', g_n', ... , g_n') = (g_1g_1', g_2g_2', ... , g_ng_n')$
Denote $D = \{(g_1, g_2, ... g_n) : g_i \in G_i\}$
Want to show that D is a group on the group product operation.
Closure:
Let a, b ∈ D.
So:
$a = (g_1, g_2, ... , g_n)$
$b = (g_1', g_2', ... , g_n')$
and
$ab = (g_1g_1', g_2g_2', ... , g_ng_n')$
Since $g_ig_i' \in G_i$ for i = 1, 2, .. n by definition of a group,
$(g_1g_1', g_2g_2', ... , g_ng_n') \in D$
Associativity:
Let a, b, c ∈ D.
So:
$a = (g_1, g_2, ... , g_n)$
$b = (g_1', g_2', ... , g_n')$
$c = (g_1'', g_2'', ... , g_n'')$
$(ab)c = (g_1g_1', g_2g_2', ... , g_ng_n')(g_1'', g_2'', ... , g_n'')$
$(ab)c = (g_1g_1'g_1'', g_2g_2'g_2'', ... , g_ng_n'g_n'')$
$(ab)c = (g_1, g_2, ... , g_n)(g_1'g_1'', g_2'g_2'', ... , g_n'g_n'') = a(bc)$
Identity:
Let $e = (e_1, e_2, ... , e_n)$ and let $a \in D$: $a = (g_1, g_2, ... , g_n)$
Notice:
$ae = (g_1, g_2, ... , g_n)(e_1, e_2, ... , e_n) = (g_1, g_2, ... , g_n)$
$ea = (e_1, e_2, ... , e_n) = (g_1, g_2, ... , g_n) = (g_1, g_2, ... , g_n)$
Hence, D contains an identity element: e
Inverse:
Let $a \in D$: $a = (g_1, g_2, ... , g_n)$
Define $a^{-1} = ({g_1}^{-1}, {g_2}^{-1}, ... , {g_n}^{-1})$
Notice:
$aa^{-1} = (g_1, g_2, ... , g_n)({g_1}^{-1}, {g_2}^{-1}, ... , {g_n}^{-1}) = (g_1{g_1}^{-1}, g_2{g_2}^{-1}, ... , g_n{g_n}^{-1}) = (e_1, e_2, ... , e_n) = e$
$a^{-1}a = ({g_1}^{-1}, {g_2}^{-1}, ... , {g_n}^{-1})(g_1, g_2, ... , g_n) = ({g_1}^{-1}g_1, {g_2}^{-1}g_2, ... , {g_n}^{-1}g_n) = (e_1, e_2, ... , e_n) = e$
Hence, all elements of D have an inverse.
Hence, D is a group on the group product operation.

Exercise 20

Find a subgroup of $Z_{12} \bigoplus Z_{18}$ that is isomorphic to $Z_9 \bigoplus Z_4$.
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 $Z_{30} \bigoplus Z_{20}$.
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 = lcm(|a|, |b|)
Since the orders have to have a LCM of 15, we only have to choose numbers such that the orders are less than 15 and factors of 15.
In other words, we can only choose elements from Z_{30} and Z_{20} with orders of 1, 3, 5, and 15.
So,
from Z_{30}: 1:(e), 3:(10, 20), 5:(6, 12, 18, 24), 15:(2, 4, 8, 14, 16, 22, 26, 28)
from Z_{20}: 1:(e), 3:(), 5:(4, 8, 12, 16), 15:()
Case:

i) |a| = 15, |b| = 1 - in this case there are 8 * 1 = 8

ii) |a| = 15, |b| = 3 - in this case there are 8 * 0 = 0

iii) |a| = 15, |b| = 5 - in this case there are 8 * 4 = 32

iv) |a| = 15, |b| = 15 - in this case there are 8 * 0 = 0

v) |a| = 5, |b| = 3 - in this case there are 15 * 0 = 0

vi) |a| = 5, |b| = 15 - in this case there are 4 * 0 = 0

vii) |a| = 3, |b| = 5 - in this case there are 2 * 4 = 8

viii) |a| = 3, |b| = 15 - in this case there are 0 * 0 = 0

ix) |a| = 1, |b| = 15 - in this case there are 1 * 0 = 0

So the sum of all of those is 48.
The number of cyclic subgroups of order 15 in $Z_{30} \bigoplus Z_{20}$ is going to be $\frac{48}{\phi(15)} = 6$