Exercise 4.13: I started by looking at the elements of $< 21 >$ and $< 10 >$, there intersection is $\{18, 12, 6\}$ as shown below. Next I tested $< 18 >= \{18, 12, 6\}$ so 18 is a generator for the intersection of these two.

```
>> a=1:1:20
a =

 Columns 1 through 16:

    1    2    3    4    5    6    7    8    9   10   11   12   13   14
 15   16

 Columns 17 through 20:

   17   18   19   20

>> [a;mod(a*21,24);mod(a*10,24)]
ans =

 Columns 1 through 16:

    1    2    3    4    5    6    7    8    9   10   11   12   13   14
 15   16
   21   18   15   12    9    6    3    0   21   18   15   12    9    6
 3    0
   10   20    6   16    2   12   22    8   18    4   14    0   10   20
 6   16

 Columns 17 through 20:

   17   18   19   20
   21   18   15   12
    2   12   22    8

>> mod(18*a,24)
ans =

 Columns 1 through 16:

   18   12    6    0   18   12    6    0   18   12    6    0   18   12
 6    0

 Columns 17 through 20:

   18   12    6    0

>> diary off
```

Examining the $< a^{21} > \cap < a^{10} >$ described in the book we note that this is identical to Z_{24} with $a = 1$, thus by symmetry we can say $< a^{21} > \cap < a^{10} >=< a^{18} >$ and more in general $< a^m > \cap < a^n >=< a^i >$ if and only if $< m > \cap < n >=< i >$.

Exercise 4.15: 1. Closure.

Suppose $a, b \in H$. Note that there must exist some naturals k, j such that $|a|k = 12$ and $|b|j = 12$. Note that $(ab)^{12} = a^{12}b^{12} = a^{|a|k}b^{|b|j} = e$, thus $|ab|$ divides 12, and so we have closure.

2. Suppose $a \in H$ and $b \in< a >$. Note that there exists some natural i such that $a^i = b$. Note that $b^{12} = (a^i)^{12} = (a^{12})^i = e^i = e$, thus $|b|$ divides 12. We conclude $< a >\subseteq H$ and since $a^{-1} \in< a >$ we know $a^{-1} \in H$.

By the two step subgroup test we conclude H is a subgroup of G.

Nowhere did I use any special properties of 12 and thus this is completely expandable to replacing the 12 with any natural number.

Exercise 4.20: Suppose there is no element that generates the entire group. Select $a \in G$ where $a \neq e$. Note that $a^{35} = e$, thus $|a| \mid 35$. Note that there are only two possibilities eater $|a| = 5$ or $|a| = 7$.

Suppose all non identity elements have order 5. Suppose $a \in G - \{e\}$ and $b \in G- < a >$. Suppose there exists $c \in< a > \cap < b > -\{e\}$. Note that since 5 is prime c must be a generator of both $< a >$ and $< b >$ thus $< b >=< a >$, a contradiction, we conclude that no such c exists so, $< a > \cap < b >= \{e\}$. Noting that there is no overlap between subgroup cycles other than the identity we can conclude that there are exactly $\frac{35-1}{4}$ cyclic sub groups, -1 for the identity and $/4$ since each sub group has 4 non-identity elements that appear in no other cycle. We note that $\frac{35-1}{4}$ is not a natural number, a contradiction with it being the exact number of cyclic sub groups, we conclude that not all non identity elements have order 5.

A very similar proof holds for 7, and since $\frac{35-1}{6}$ is also not a whole number we conclude that not all non identity elements have order 7.

We can now conclude that there must be at least one element of order 5 and one element of order 7. Let $|a| = 5$ and $|b| = 7$. Note that $ab \in G$. Suppose $|ab| = 5$. Note that $e = (ab)^5 = a^5b^5 = eb^5 = b^5$ and so $|b| = 5$ a contradiction. The same follows for 7 and thus we conclude $|ab| \neq 5$ and $|ab| \neq 7$, this is impossible since 5 and 7 are the only possibilities for $|ab|$. We conclude the negation of our first supposition and conclude that there is a element that generates the entire group, thus G is cyclic.

The same would hold for 33 as well as any other semi-prime.

Exercise 4.33: See attached

Exercise 4.41: Note that ab is a group element thus $(ab)^{|ab|} = a^{|ab|}b^{|ab|} = e$. Since $b^{|ab|} = a^{-|ab|} \in< a >$ and $b^{|ab|} \in< b >$ we can conclude $b^{|ab|} = e$ and $a^{|ab|} = e$, this means

$|ab|$ is a multiple of $|a| = m$ and $|b| = n$, or $\text{lcm}(m, n) \leq |ab|$. Let $n = \text{lcm}(m, n)$. Note that $(ab)^n = a^n b^n = ee = e$, thus $|ab| \leq \text{lcm}(m, n)$. We are forced to conclude that ab has order of the least common multiple of m and n.

As a counter example to prove that it is necessary that a and b commute, consider D_3, the symmetries of a triangle. The rotations are order 3 and the reflections are order 2. The only shared element between the cyclic group containing the first rotation and the cyclic group containing the first reflection is the identity. The LCM of the group containing the rotation and the group containing the reflection is 6 however there are no elements with order 6.

Exercise 4.64: Suppose $c \in < a > \cap < b > -\{e\}$. Note that $|c| \mid |a|$ and $|c| \mid |b|$, a contradiction since $1 < |c|$, and $|a|$ and $|b|$ are relatively prime.