**Exercise 2.32:** Construct a Cayley table for $U(12)$.
$U(12) = \{1, 5, 7, 11\}$

```
>> a=[1,5,7,11]
a =

     1     5     7    11

>> b=mod(a'*a,12)
b =

     1     5     7    11
     5     1    11     7
     7    11     1     5
    11     7     5     1

>> diary off
```

| | 1 | 5 | 7 | 11 |
|---|---|---|---|---|
| 1 | 1 | 5 | 7 | 11 |
| 5 | 5 | 1 | 11 | 7 |
| 7 | 7 | 11 | 1 | 5 |
| 11 | 11 | 7 | 5 | 1 |

**Exercise 2.34:** Prove that in a group, $(ab)^2 = a^2b^2$ if and only if $ab = ba$.
Suppose $(ab)^2 = a^2b^2$ for all $a$ and $b$ in some group $G$. Choose $a, b \in G$. Note that $abab = (ab)^2 = a^2b^2 = aabb$, thus $a^{-1}ababb^{-1} = a^{-1}aabbb^{-1}$, so $ab = ba$.
Suppose $ab = ba$. Note that by applying $a$ to the left and $b$ to the right we get, $a^2b^2 = aabb = abab = (ab)^2$.

**Exercise 2.37:** Let $G$ be a finite group. Show that the number of elements $x$ of $G$ such that $x^3 = e$ is odd. Show that the number of elements $x$ of $G$ such that $x^2 \neq e$ is even.
Suppose $x \in G$ such that $x^3 = e$. Note that $(x^2)^3 = (x^3)^2 = e^2 = e$. Note that if $x \neq e$ then $x^2 = xx \neq x$ by the uniqueness of the identity. Note that $(x^2)^2 = x^3x = ex = x$. We have now demonstrated that all the non-identity elements $x$ of $G$ such that $x^3 = e$ come in pairs, thus there are a even number of them, noting that $e^3 = e$ we add one more to this set and conclude that the number of elements $x$ of $G$ such that $x^3 = e$ is odd.
Suppose $x \in G$ such that $x^2 \neq e$. Recall that we can break $G$ up into non-overlapping, other than the identity, cyclic sub-groups. Consider one such sub-group, lets call it $H$.
Suppose $|H| = n$ is even. Suppose $a$ is the generator of this group. Note that $a^0$ and $a^{n/2}$ are the two elements who's square is the identity. There are $n - 2$, witch is even, elements of this sub-group that fulfill $x^2 \neq e$.
Suppose $|H| = n$ is odd. Suppose $a$ is the generator of this group. Note that $a^0$ is the only element who's square is the identity. There are $n - 1$, witch is even, elements of this sub-group that fulfill $x^2 \neq e$.
since none of the elements that fulfill $x^2 \neq e$ we found in the sub-groups are in more than

one sub-group we do not need to worry about over counting, all we need to do is add up the number of elements fulfilling $x^2 \neq e$. The sum of finitely many even numbers is even thus the number of elements $x$ of $G$ such that $x^2 \neq e$ is even.

**Exercise 2.46:** Prove that the set of all rational numbers of the form $3^m 6^n$ , where $m$ and $n$ are integers, is a group under multiplication, lets call it $G$.

(a) Suppose $3^m 6^n \in G$ and $3^{m'} 6^{n'} \in G$. Note that $3^m 6^n 3^{m'} 6^{n'} = 3^{m+m'} 6^{n+n'} \in G$ by the closure of integers under addition. We conclude that $G$ is closed.

(b) Recall that multiplication of rationals is associative.

(c) Note that $1 = 3^0 6^0 \in G$ is the multiplicative identity for rationals.

(d) Suppose $3^m 6^n \in G$. Note that $3^{-m} 6^{-n} \in G$. Note that $3^m 6^n 3^{-m} 6^{-n} = 1$, the identity.

**Exercise 2.51:** List the six elements of $GL(2, Z_2)$. Show that this group is non-Abelian by finding two elements that do not commute. (This exercise is referred to in Chapter 7.)

```
>> a=[0,1;1,0]
a =

     0     1
     1     0

>> b=[0,1;1,1]
b =

     0     1
     1     1

>> a*b
ans =

     1     1
     0     1

>> b*a
ans =

     1     0
     1     1

>>
>> diary off
```

Note that these two matrices above do not commute.
The elements in this group are, $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$.

**Exercise 2.54:** Suppose that in the definition of a group $G$, the condition that for each element $a$ in $G$ there exists an element $b$ in $G$ with the property $ab = ba = e$ is replaced by the condition $ab = e$. Show that $ba = e$. (Thus, a one-sided inverse is a two-sided inverse.) Suppose $a \in G$. There exists $b \in G$ such that $ab = e$. There exists $c \in G$ such that $bc = e$. Note $ab = e$ apply $c$ to the right and obtain $(ab)c = ec$ thus $a(bc) = c$ so $a = c$, thus $ba = bc = e = ab$.

**Exercise 3.32:** If $H$ and $K$ are subgroups of $G$, show that $H \cap K$ is a subgroup of $G$. (Can you see that the same proof shows that the intersection of any number of subgroups of $G$, finite or infinite, is again a subgroup of $G$?)

(a) Closure. Suppose $a, b \in H \cap K$. Note that $a, b \in H$, thus $ab \in H$ and likewise for $K$ thus $ab \in H \cap K$.

(b) Associativity is preserved to the subset.

(c) The identity is in both $H$ and $K$ and thus is in $H \cap K$.

(d) Suppose $a \in H \cap K$. Note $a \in H$ thus $a^{-1} \in H$, and likewise with $K$, thus $a^{-1} \in H \cap K$.

**Exercise 3.64:** Compute $|U(4)|$, $|U(10)|$, and $|U(40)|$. Do these groups provide a counterexample to your answer to Exercise 62? If so, revise your conjecture. Note that $|U(4)| = |\{1, 3\}| = 2$. Note that $|U(10)| = |\{1, 3, 7, 9\}| = 4$. Note that $|U(40)| = |\{1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31,$ 16.

**Exercise 3.65:** Find a cyclic subgroup of order 4 in $U(40)$.
Note that $< 3 >= \{3, 9, 27, 1\}$.

**Exercise 3.66:** Find a noncyclic subgroup of order 4 in $U(40)$.
Note that $\{1, 9, 11, 19\}$ is non cyclic and that every element is its own inverse. Below i have a table demonstrating closure, this is a noncyclic subgroup of order 4.

```
>> a=[1,9,11,19]
a =

     1     9    11    19

>> mod(a'*a,40)
ans =

     1     9    11    19
     9     1    19    11
    11    19     1     9
    19    11     9     1

>> diary off
```

**Exercise 3.71:** Let $G = GL(2,\mathbb{R})$ and $H = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| a \text{ and } b \text{ are non-zero integers} \right\}$ under the operation of matrix multiplication. Prove or disprove that $H$ is a subgroup of $GL(2,\mathbb{R})$.
It is not a subgroup since $H$ is not a group. The inverse to $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$, $\begin{bmatrix} 1/2 & 0 \\ 0 & 1/2 \end{bmatrix}$ is not in $H$.

**Exercise 3.79:** Let $G = GL(2,\mathbb{R})$.

(a) Find $C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right)$

Let $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ a & b \end{bmatrix} = \begin{bmatrix} a+b & a \\ c+d & c \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$. We now see that $C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right) = \left\{ \begin{bmatrix} a & b \\ b & d \end{bmatrix} \middle| \text{where } a = b + d \right\} \cap GL(2,\mathbb{R})$.

(b) $C\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right) = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \right\} \cap GL(2,\mathbb{R})$

(c) All multiples of identity are in $Z(G) = a\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ where $a \in \mathbb{R} - \{0\}$.