Adam Jump
MATH 385
HW #1

**Chapter 13 Problems:** $3, 6, 7, 8, 9, 12, 17, 19, 21, 22, 23, 40, 46, 48, 54$

7. Show that the three properties listed in Exercise 6 are valid for $\mathbb{Z}_p$, where p is prime.

   To reiterate, those properties are:

   **a.** $a^2 = a$ implies $a = 0$ or $a = 1$.

   **b.** $ab = 0$ implies $a = 0$ or $b = 0$.

   **c.** $ab = ac$ and $a \neq 0$ imply $b = c$.

   *Proof.*

   **(a.)** B.W.O.C. Assume $a^2 \mod_p = a$ and $a \neq 0$ and $a \neq 1$
   $\implies a^2 = (p+1)a$
   $\implies ap + a \mod_p = 0 + a = a$
   however $p + 1 \notin \mathbb{Z}_p$

   $\Rightarrow\!\Leftarrow$

   $\therefore a = 0$ or $a = 1$

   **(b.)** B.W.O.C. Assume $a \neq 0$ and $b \neq 0$
   $\implies a \cdot b = k \cdot p$, for $k \in \mathbb{N}$
   $\implies a$ or $b = p \notin \mathbb{Z}_p$

   $\Rightarrow\!\Leftarrow$

   $\therefore a = 0$ or $b = 0$

   **(c.)** $ab = ac,\ a \neq 0 \implies b = c$
   $\implies ab = ac$
   $\implies ab - ac = 0$
   $\implies a(b - c) = 0$
   and we know that $a \neq 0$
   $\implies b - c = 0$
   $\therefore b = c$

Q.E.D.

8. Show that a ring is commutative if it has the property that $ab = ca$ implies $b = c$ when $a \neq 0$. This is actually a chain of implications of the form:

$$ab = ca, a \neq 0 \implies b = c \implies R \text{ is commutative}$$

What we need to show is that for any arbitrary element $x \in R$, $ax = xa$.

*Proof.*
We know that $ab = ca, a \neq 0 \implies b = c$.
Using $b = c$,
$\implies ab = ac$ however, by our assumption, $ab = ca$, this implies that,
$ab = ca = ac$
$\therefore ca = ac$, which shows $R$ is commutative.

Q.E.D.

17. Show that a ring that is cyclic under addition is commutative.

*Proof.*
Let $R = \langle a \rangle, |R| = n, n_1, n_2 < n,$ and $, n_1 < n_2$ for $n_1, n_2 \in \mathbb{Z}$
which means $R = \{i \cdot a \in R \mid i \in [n]\}$,
$(n_1 \cdot a) + (n_2 \cdot a)$
$\implies (a + \cdots + a) + (a + \cdots + a)$
which by associativity implies,
$\implies (n_1 - (n_1 - n_2)) \cdot a + (n_2 - (n_2 - n_1)) \cdot a$

Q.E.D.

22. Let $R$ be a commutative ring with unity and let $U(R)$ denote the set of units of $R$. Prove that $U(R)$ is a group under the multiplication of $R$. (This group is called the *group of units of R*.) Let $a, b \in U(R)$,
$a^{-1}, b^{-1} \in U(R)$, by definition *unit*,
Show $a \cdot b^{-1} \in U(R)$,

*Proof.*
We know that $a, a^{-1}, b, b^{-1} \in U(R)$.
This implies that $a \cdot b^{-1} \cdot b \cdot a^{-1} \in R$,
$\implies a \cdot 1 \cdot a^{-1}$,
$\implies a \cdot a^{-1} = 1$,
$\implies a \cdot b^{-1} \in U(R)$,
$\therefore U(R) \leq R$

Q.E.D.