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 $a \neq 1$
$\implies a^2 = pa$
$\implies a^2 = p^2 \notin \mathbb{Z}_p$

$$\Rightarrow\!\Leftarrow$$

$\therefore a = 0$ 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.) $ab = ac,\ a \neq 0 \implies b = c$
$a^{-1} \in \mathbb{Z}_p$
$\implies a^{-1}ab = a^{-1}ac$, as $\mathbb{Z}_p$ is a field and so every non-zero element in a unit.
$\implies b = c$
$\therefore b = c$

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:

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

Proof.
$ab = ca, a \neq 0 \implies b = c,$
$\implies a^{-1}ab = a^{-1}ca,$
$\implies b = a^{-1}ca,$
$\implies b = a^{-1}ac,$
$\implies b = c$
$\therefore ab = ba$, and R is commutative

Q.E.D.

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