HW 6

Charles Liu
Elementary Modern Algebra - Dr. Ben Clark
March 26th, 2025

---

1. Let R be a ring with unity 1 and with elements a, b, c. Prove the following

(a) $a(b-c) = ab - ac$

Theorem. $a(b-c) = ab - ac$

Proof:

$a(b-c) = a(b+(-c)) = ab + a(-c) = ab - ac$

(b) $(-1)(-1) = 1$

Lemma. $a \cdot 0 = 0$

We can find that $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$.

However, we also know that $a \cdot 0 = a \cdot 0 + 0$

So $a \cdot 0 = 0$.

Theorem. $(-1)(-1) = 1$

Proof:

We can find that $(-1)(1+(-1)) = (-1)(0) = 0$ by the above Lemma.

On the other hand, we can distribute to get $(-1)(1) + (-1)(-1) = 0$.

So $-1 + (-1)(-1) = 0$, and $(-1)(-1) = 1$.

---

2. Find an integer n that shows that the rings $\mathbb{Z}_n$ need not have the following properties.

(a) $a^2 = 0$ implies that $a = 0$ or $a = 1$.

Take $n = 4$

$\mathbb{Z}_4$

We know that $a = 2 \in (\mathbb{Z}_4, +, \cdot)$

$a^2 = 4 \bmod 4 = 0$

(b) $ab = 0$ implies $a = 0$ or $b = 0$.

Take $n = 6$
Take $a = 2, b = 3$. $ab = 0$ but neither a, b are 0.

---

3. Show that the two properties from the previous exercise hold when n is prime.

a) If $a^2 = 0$, then $n|a^2$. Since n is prime, $n|a$. This means either $a = 0$ or $a = 1$.
b) If $ab = 0$, then $n|ab$. Since n is prime, $n|a$ or $n|b$. This means $a = 0$ or $b = 0$.

---

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

Theorem. A ring that is cyclic under addition is commutative.
Proof:
Take $a, b \in R$. Let $c \in R$ be the element that cyclically generates R under addition.

We can find two integers, $n_1, n_2 \in \mathbb{Z}$, such that
$a = n_1 c$ and $b = n_2 c$.

This means

$$\begin{aligned} ab &= (n_1 c)(n_2 c) \\ &= (c + \ldots + c)(c + \ldots + c) \\ &= c^2 + c^2 \ldots + c^2 \\ &= n_1 n_2 c^2 \\ &= n_2 n_1 c^2 \\ &= n_2 c(c + c \ldots + c) \\ &= (n_2 c)(n_1 c) \\ &= ba \end{aligned}$$

So commutativity holds.

---

5. Suppose that a and b belong to a commutative ring R with unity. If a is a unit of R and $b^2 = 0$, show that $a + b$ is a unit of R.

Proof:

Since a is a unit of R, a^{-1} exists in R.

Take $c = a^{-1} - ba^{-2}$.

Since the ring is commutative and $b^2 = 0$, we can solve that

$(a+b)(a^{-1} - ba^{-2}) = aa^{-1} - aba^{-2} + ba^{-1} - b^2a^{-2} = 1.$

Thus, $c = (a+b)^{-1}$ and $a + b$ is a unit.