SOLUTION KEY
Produced by: Kyle Dahlin

Problems:
Chap 12: 2, **6**, 18, 22, **23**, 31, 44, **50**

Problem 12.2. The ring $\{0, 2, 4, 6, 8\}$ under addition and multiplication modulo 10 has a unity. Find it.

Solution:
6 is the unity of this ring since $6 \times 2 = 2$, $6 \times 4 = 4$, $6^2 = 6$, and $6 \times 8 = 8$ modulo 10. ■

Problem 12.6. Find an integer n that shows that the rings $\mathbb{Z}_n$ need not have the following properties that the ring of integers has.

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 $b = c$

Is the n you found prime?

Solution:
Consider the group $\mathbb{Z}_6$. The element 3 has the property that $3^2 = 3$ but it is not equivalent to 0 or 1. The pair $(2, 3)$ has the property $2 \times 3 = 0$ but neither are the 0 element. Finally the triplet $(2, 3, 4)$ has the property that $3 \times 2 = 3 \times 4 = 0$ with $3 \neq 0$ and $2 \neq 4$.

$n = 6$ is composite. ■

Comment: Problem **12.7** has you show that the three properties listed above *do* indeed hold when n is prime.

Problem 12.18. Let a belong to a ring R. Let $S = \{x \in R | ax = 0\}$. Show that S is a subring of R.

Solution:
We will use Theorem 12.3, the Subring Test. Clearly $0 \in S$ so S is not empty. Let x and y in S. Since $a(xy) = (ax)y = 0y = 0$, $xy \in S$. Next, since $a(x - y) = ax - ay = 0 - 0 = 0$, $x - y \in S$. Thus S is a subring of R. ■

Problem 12.22. 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.

Solution:
Let e denote the unity of R and let a and b be arbitrary elements of $U(R)$. We must first show that multiplication of R induces a binary operation on $U(R)$. There exists $x, y \in R$ such that $ax = e$ and $by = e$. Then $(ab)yx = aex = ax = e$, so that $ab \in U(R)$. This operation is automatically associative and has an identity because it inherits those properties from multiplication on R. Now suppose that $za = e$. Then $z = ze = zax = ex = x$. Hence a has a unique multiplicative inverse. Thus $U(R)$ is a group under the multiplication it inherits from R. ■

Problem 12.23. Determine $U(\mathbb{Z}[i])$.

Solution:
The unity of $\mathbb{Z}[i]$ is $1 = 1 + 0i$. Let $a + bi \in U(\mathbb{Z}[i])$ and suppose that $x + yi$ is its inverse. Then we must have that $(a + bi)(x + yi) = 1$, equivalently:

$$(ax - by) + (ay + bx)i = 1 + 0i$$

Now notice that the complex conjugates of $a+bi$ and $x+yi$ exhibit the same property since:

$$(a - bi)(x - yi) = (ax - by) - (ay + bx)i = 1 - 0i$$

Therefore $(a + bi)(a - bi)(x + yi)(x - yi) = 1$ and $(a^2 + b^2)(x^2 + y^2) = 1$. Since a, b, x, y are all integers, this can only be true if $a^2 + b^2 = x^2 + y^2 = 1$. Furthermore, the only integer solutions to $a^2 + b^2 = 1$ are $a = \pm 1, b = 0$ and $a = 0, b = \pm 1$.

Thus $U\mathbb{Z}[i] = \{1, -1, i, -i\}$. ■

Comment: Alternatively, to do this problem without using conjugation or the norm on $\mathbb{Z}[i]$(neither of which have been defined in this course), you can proceed as follows.

The system of equations $ax - by = 1$, $ay + bx = 0$ can be written as:

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

By Cramer's Rule, this system has a solution if and only if $a^2 + b^2 \neq 0$ and the solution is given by:

$$x = \frac{a}{a^2 + b^2}, y = -\frac{b}{a^2 + b^2}.$$

Since $x, y \in \mathbb{Z}$, we must have that $a^2+b^2 \mid a$ and $a^2+b^2 \mid b$. But in $\mathbb{Z}$, $a^2+b^2 \geq \max\{|a|, |b|\}$, with equality if and only if $a = 0, b = \pm 1$ or $a = \pm 1, b = 0$ or $a = b = 0$. In the case that $a = b = 0$, then $a^2 + b^2 = 0$ and $a + bi$ is not a unit, by the condition above. Therefore $U\mathbb{Z}[i] = \{1, -1, i, -i\}$.

Problem 12.31. Give an example of ring elements a and b with the properties that $ab = 0$ but $ba \neq 0$.

Solution:
Let $a = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $b = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ in $M_2(\mathbb{Z})$, the ring of two-by-two matrices over the integers with the usual addition and matrix multiplication. Then $ab = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and $ba = a \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.
■

Comment: When seeking (counter) examples related to commutativity, two-by-two matrices are often a good place to start.

Problem 12.44. Suppose that there is a positive even integer n such that $a^n = a$ for all elements a of some ring. Show that $-a = a$ for all a in the ring.

Solution:
Suppose that $n = 2k$ for some positive integer k. Then since $(-1)^2 = 1$, we get that $(-a)^2 = a^2$ and finally that $a = a^{2k} = (a^2)^k = ((-a)^2)^k = (-a)^{2k} = -a$. ∎

Problem 12.50. Suppose that R is a ring and that $a^2 = a$ for all a in R. Show that R is commutative.

Solution:
Let a and b in R. Then $a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$ and hence $ab + ba = 0$. By Problem **12.44**, $ba = -ba$. Hence $ab = ba$ and R is commutative. ∎