

SOLUTIONS TO HW #10

Chapter 12

10.

Example 8. The only element of $\{0\}$ is 0, and $0 - 0 = 0$, $0 \cdot 0 = 0 \Rightarrow \{0\}$ is a subring of R . Let $a, b \in R$. Then $a - b \in R$ and $a \cdot b \in R$ since R is a ring, so R is a subring of itself.

Example 9. The following subtraction and multiplication tables show that $\{0, 2, 4\}$ is a subring of $\mathbb{Z}/6\mathbb{Z}$:

-	0	2	4
0	0	4	2
2	2	0	4
4	4	2	2

×	0	2	4
0	0	0	0
2	0	4	2
4	0	2	4

Example 10. Let $a, b \in n\mathbb{Z}$, so that $a = pn$, $b = qn$. Then $a - b = (p - q)n \in n\mathbb{Z}$ and $ab = pn(qn) = (pnq)n \in n\mathbb{Z}$. Hence $n\mathbb{Z}$ is a subring of \mathbb{Z} .

Example 11. Let $a + bi, c + di \in \mathbb{Z}[i]$, where $a, b, c, d \in \mathbb{Z}$. Then $(a + bi) - (c + di) = (a - c) + (b - d)i \in \mathbb{Z}[i]$, since $a - c, b - d \in \mathbb{Z}$. Also, $(a + bi)(c + di) = (ac - bd) + (ad + bc)i \in \mathbb{Z}[i]$, since $ac - bd, ad + bc \in \mathbb{Z}$. Hence $\mathbb{Z}[i]$ is a subring of \mathbb{C} .

Example 12. Let $f, g \in \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f(0) = 0\}$. Then $(f - g)(0) = f(0) - g(0) = 0 - 0 = 0$, and $(fg)(0) = (f(0))(g(0)) = 0 \cdot 0 = 0$, so this is a subring of the ring of real-valued one-variable functions.

Example 13. $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} - \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} a - c & 0 \\ 0 & b - d \end{pmatrix}$ is a matrix of the required form. Similarly, $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix}$, also a matrix with integer entries.

18. Let $a \in R$ and $S = \{x \in R \mid ax = 0\}$, $b, c \in S$. Then $a(b - c) = ab - ac = 0 - 0 = 0$ by the distributivity property, so that $b - c \in S$. Also, $a(bc) = (ab)c = 0 \cdot c = 0$ by associativity, so $bc \in S$, and hence S is a subring of R .

20. If A is an element of $M_2(\mathbb{Z})$, we consider the equation $AB = I$. Basic properties of determinants tell us that the only way for this equation to be true is if $\det(A)\det(B) = \det(I) = 1$. That means that $\det(A)$ (and incidentally $\det(B)$ also) has to be a unit in the ring \mathbb{Z} . We know from previous homework that the units in \mathbb{Z} are 1 and -1 . Hence the elements of $M_2(\mathbb{Z})$ that have multiplicative inverses are those with determinant 1 or -1 .

30. Suppose that there is a positive power $n > 1$ such that for all x in a ring R , $x^n = x$. And suppose that, given some $a \in R$, there exists $m > 0$ such that $a^m = 0$. We want to show that a must be equal to 0. We consider three cases.

Case 1 ($n = m$): $a = a^n = a^m = 0$, and we are done.

Case 2 ($n > m$): $a = a^n = a^m a^{(n-m)} = 0 \cdot a^{(n-m)} = 0$.

Case 3 ($n < m$): Notice that since $a = a^n$, $a = \underbrace{a \cdots a}_n = \underbrace{a^n \cdots a^n}_n = a^{n^n}$. Since we can do this arbitrarily often, notice that there exists $k > 1$ in the form of repeated exponentiation of n such that $k > m$, and $a^k = a^n = a$. Hence this case reduces to Case 2, so we are done.

Chapter 13

4. The zero divisors in $\mathbb{Z}/20\mathbb{Z}$ are $\{2, 4, 5, 6, 8, 10, 12, 14, 15, 16, 18\}$ because all of these numbers have a common factor with 20 other than 1. The units are $\{1, 3, 7, 9, 11, 13, 17, 19\}$, and these numbers are all relatively prime to 20.

10.

$$\frac{1}{2} = 1 \cdot 2^{-1} = 1 \cdot 4 = 4.$$

$$-\frac{2}{3} = (-2) \cdot (3)^{-1} = 5 \cdot 5 = 25 = 4.$$

$$\sqrt{-3} = x \Rightarrow -3 = x^2 \Rightarrow 4 = x^2 \Rightarrow 2 = x \text{ or } 5 = x.$$

$$-\frac{1}{6} = (-1) \cdot (6)^{-1} = 6 \cdot 6 = 36 = 1.$$

12. We can use the information in Problem 4. Take, for example, 2 and 5. They are zero divisors in $\mathbb{Z}/20\mathbb{Z}$, but $2 + 5 = 7$, and 7 is not a zero divisor in $\mathbb{Z}/20\mathbb{Z}$ (in fact, it is a unit). It is a very important fact that if $a \in R$, then a cannot simultaneously be a zero divisor and a unit.