Math 320 Homework 11

Joseph C. McGuire

November 15, 2018

For each ring R given in Problems 89 - 93, complete the following items (a) - (c). Justify all answers for Problems 89 - 91. For Problems 92 and 93, you need only justify answers of "no".

(a.) Find char(R).

(b.) Is R an integral domain?

(c.) Is R a field?

(89.) $\mathbb{Z}_{11}$

(a.) By Theorem 13.3, we have the order of 1 under addition is the char(R). Since |1| under addition is 11, we have $char(R) = 11$.
(b.) Yes, since 1 is the unity of the ring and we have no such elements $a \not\equiv 0(\text{mod } 11)$ and $b \not\equiv 0(\text{mod } 11)$, where $ab \equiv 0(\text{mod p})$. Since that would mean ab = pk, for some $k \in \mathbb{Z}$, meaning p divides ab, hence by Euclid's Lemma either $a \equiv 0(\text{mod p})$ or $b \equiv 0(\text{mod p})$, which would be a contradiction. Hence $\mathbb{Z}_{11}$ has no zero divisors. Thus $\mathbb{Z}_{11}$ is an integral domain
(c.) Yes, by Theorem 13.2. Since Z_{11} is a finite integral domain, we have $\mathbb{Z}_{11}$ is also a field.

(90.) $\mathbb{Z}_2 \oplus \mathbb{Z}_5$

(a.) By Theorem 13.3, we have the order of $(1, 1)$ under addition is the char($Z_2 \oplus Z_5$). Hence by Theorem 8.1, $char(R) = |(1, 1)| = LCM(|1|, |1|)$, in their respective rings under addition, hence $char(R) = LCM(2, 5) = 10$. Thus $char(R) = 10$.
(b.) No, by the contrapositive of Theorem 13.4, since $char(R) = 10$ and not a prime or 0, we have $\mathbb{Z}_2 \oplus \mathbb{Z}_5$ is not an integral domain.
(c.) No, since the ring is not an integral domain it can't be a field.

(91.) $\mathbb{Z}_5[i]$, where the operations are complex number addition and multiplication; remember that $i^2 = -1$. (<u>Hint</u>: $(3+4i)(3+i)$.)

(a.) Note that here 1 is still the unity element, since $ai * 1 = ai$ for all $a \in \mathbb{Z}_5$. Hence, we will use Theorem 13.3 again to find the characteristic: $1+1+1+1+1 = 5 \equiv 0(\text{mod } 5)$. Hence $|1| = 5 = char(R)$.
(b.) No, since we have $3+4i \neq 0$ and $3+i \neq 0$, but $(3+4i)(3+i) = 5+15i = 0+0i = 0$, so we have non-zero zero divisors, hence $Z_5[i]$ isn't an integral domain.
(c.) No, since our ring isn't an integral domain it can't be a field.

(92.) $\mathbb{Z}_3[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}_3\}$, where addition and multiplication are defined as with ordinary real numbers, and where coefficient arithmetic is done modulo 3.

(a.) Note that here we have the unity of 1, since $1 = 1 + 0\sqrt{2}$. So we will use Theorem 13.3 to find the char(R). Note that here since $1+1+1 = 3 \equiv 0(\text{modulo } 3)$, we have $|1| = 3$ under addition. So $char(R) = 3$, by Theorem 13.3.
(b.) Yes. Since it both has a unity and no non-zero zero divisors.
(c.) Yes, by Theorem 13.2, since $\mathbb{Z}_3[\sqrt{2}]$ is a finite integral domain.

(93.) $\mathbb{R}[x]$

(a.) Note that since $\mathbb{R}$ is an infinite set, if we adjoin x on to it, then we still have $\mathbb{R}[x]$ is of infinite order, by Theorem 13.3. Thus $char(\mathbb{R}[x]) = 0$.
(b.) Yes, since the unity of $\mathbb{R}[x]$ has the identity of 1 and no non-zero zero divisors since the equation: $(a_0 + a_1x + ...)(b_0 + b_1x + ...) = 0$ if and only if either all of $a_i = 0$ or $b_i = 0$ for all $i \in \mathbb{N}$. Thus by definition $\mathbb{R}[x]$ is an integral domain.
(c.) No, consider the element $4x^3 \in \mathbb{R}[x]$, the inverse of this element is $\frac{1}{4x^3}$, but this isn't an element of our ring, since $\frac{1}{x^3}$ is not a real number adjoined with x. Hence $4x^3$ is a non-zero element that isn't a unit. Thus $\mathbb{R}[x]$ isn't a field.

(94.)

(a.) If c is a nonzero element in an integral domain R, prove that the <u>only</u> solutions to $x^2 - cx = 0$ in $R[x]$ are x = 0 and x = c.

Proof. Let R be an integral domain and $c \in R$. Then consider $x^2 - cx = 0$ in $R[x]$. Then consider $x^2 - cx = x(x-c) = 0$. Since x is a variable over the elements of R, and R is an integral domain and has no non-zero divisors, we have either $x = 0$ or $x - c = 0$. Thus either $x = 0$ or $x = c$. □

(b.) Does the result of part (a.) remain true if we assume that R is an arbitrary ring instead of an integral domain? Justify your answer.

No, consider the equation $x^2 - 6x = 0$ in $\mathbb{Z}_8[x]$. Then we have $x(x-6) = 0$, but if x = 2, then we have $2 * (2-6) \equiv 2(-4) \equiv 2 * 4 \equiv 0$(modulo 8). Hence we have $x^2 - 6x = 0$, but $x \not\equiv 0$(modulo 8) and $x \not\equiv 6$(modulo 8). Hence our result from part(a.) doesn't follow for arbitrary rings.

(95.) Prove that $\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$ is a field under the operations of ordinary real number addition and multiplication. Use only results from Chapter 13 or before in your proof. (Suggestion: First, show that $\mathbb{Q}[\sqrt{3}]$ is a subring of $\mathbb{R}$)

Proof. Let $\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$. First, we will show that $\mathbb{Q}[\sqrt{3}]$ is a subring of $\mathbb{R}$ using Theorem 12.3.
(a - b $\in \mathbb{Q}[\sqrt{3}]$)
Let $a, b \in \mathbb{Q}[\sqrt{3}]$. Then for some $c, d, e, f \in \mathbb{Q}$, we have $a = c + d\sqrt{3}$ and $b = e + f\sqrt{3}$. Hence $a - b = c + d\sqrt{3} - (e + f\sqrt{3}) = c - e + d\sqrt{3} - f\sqrt{3} = c - e + (d - f)\sqrt{3}$, since $c - e, d - f \in \mathbb{Q}$, we have $a - b \in \mathbb{Q}[\sqrt{3}]$.
(ab $\in \mathbb{Q}[\sqrt{3}]$)
Let $a, b \in \mathbb{Q}[\sqrt{3}]$. Then for some $c, d, e, f \in \mathbb{Q}$ we have $a = c + d\sqrt{3}$ and $b = e + f\sqrt{3}$. Then consider the following:

$$\begin{aligned} ab &= (c + d\sqrt{3})(e + f\sqrt{3}) \\ &= ce + cf\sqrt{3} + ed\sqrt{3} + df(\sqrt{3})^2 \\ &= ce + df3 + cf\sqrt{3} + ed\sqrt{3} \\ &= (ce + 3df + (cf + ed)\sqrt{3}) \end{aligned}$$

Since $(ce + 3df), (cf + ed) \in \mathbb{Q}$, we have $ab \in \mathbb{Q}[\sqrt{3}]$.
Thus by Theorem 12.3, we have $\mathbb{Q}[\sqrt{3}]$ is a subring of $\mathbb{R}$, hence a ring itself.
Note that since $\mathbb{Q}[\sqrt{3}]$ is a subring of $\mathbb{R}$, they share the same unity element 1. Next to show is that every nonzero element is a unit. Note that this is equivalent to saying that every nonzero element has a multiplicative inverse. Hence we will show this. So let $a \in \mathbb{Q}[\sqrt{3}] \setminus \{0\}$. Then for some $c, d \in \mathbb{Q}[\sqrt{3}]$, we have $a = c + d\sqrt{3}$. Then note that the inverse of a is $\frac{1}{c+d\sqrt{3}}$, we can put this in standard form by multiplying by the conjugate; that is, $\dfrac{1}{c + d\sqrt{3}} * \dfrac{c - d\sqrt{3}}{c - d\sqrt{3}} = \dfrac{c - d\sqrt{3}}{c^2 - 3d^2} = \dfrac{c}{c^2 - 3d^2} - \dfrac{b}{c^2 - 3d^2}\sqrt{3}$. So we have $a^{-1} \in \mathbb{Q}[\sqrt{3}]$. Thus every element of $\mathbb{Q}[\sqrt{3}]$ has a multiplicative inverse, hence every non-zero element of $\mathbb{Q}[\sqrt{3}]$ is a unit. Thus $\mathbb{Q}[\sqrt{3}]$ is a field. □

(96.) The nonzero elements of $\mathbb{Z}_3[i]$ form an Abelian group of order 8 under multiplication. Is it isomorphic to $\mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$? Justify your answer.

First, note that $\mathbb{Z}_3[i] \setminus \{0\} = < 1 + i >$. Since $(1+i)^1 = 1+i, (1+i)^2 = 2i, (1+i)^3 = 1+2i, (1+i)^4 = 2, (1+i)^5 = 2+2i, (1+i)^6 = i, (1+i)^7 = 2+i$, and $(1+i)^8 = 1$. Hence $(1+i)$ is a generator for $\mathbb{Z}_3[i]$, so $\mathbb{Z}_3[i]$ is cyclic. Note that neither $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ are cyclic, by Corollary 1 to Theorem 8.2. Since $\mathbb{Z}_8 =< 1 >$ hence is cyclic, we have the only option is that $\mathbb{Z}_3[i] \approx \mathbb{Z}_8$.

(97.) Find a nonzero element in a ring that is neither a zero-divisor nor a unit. Clearly specify the ring and the element, and show that your example works.

Note from Example 1 from Chapter 13 of the workbook, we have the ring $\mathbb{Z}[x]$ is an integral domain hence has no zero divisors. Moreover we have the only units of the ring are 1 and -1. We know that these are the only two possible units since the problem $(a_0 + a_1x + ...)(b_0 + b_1x + ...) = 1$, has no solution in the integers, when $b_i, a_i \in \mathbb{Z}$ for all $i \in \mathbb{N}$. Hence the element $x \in \mathbb{Z}[x]$ is a not a zero-divisor and is not a unit.

(98.) List all zero-divisors of $\mathbb{Z}_{20}$. What do all the zero-divisors of $\mathbb{Z}_{20}$ have in common? What do all the units of $\mathbb{Z}_{20}$ have in common?

The zero-divisors of $\mathbb{Z}_{20}$ is the set $\{0, 2, 4, 5, 6, 8, 10, 12, 14, 15, 16, 18\}$. By previous exercise we have the units of $\mathbb{Z}_{20}$ are $U(20)$. There two sets of zero-divisors and units of $\mathbb{Z}_{20}$ are disjoint, and form the entire group; that is, they partition $\mathbb{Z}_{20}$.

(99.) Find the characteristic of $\mathbb{Z}_4 \oplus 4\mathbb{Z}$, and explain why your answer is correct.

First, note that the ring $\mathbb{Z}_4 \oplus 4\mathbb{Z}$ has no unity element, since $1 \notin 4\mathbb{Z}$. So we will use the definition of the characteristic to find it for this ring, that is the smallest positive integer such that $nx = 0$ for all $x \in \mathbb{Z}_4 \oplus 4\mathbb{Z}$. So note that the 0 in $\mathbb{Z}_4 \oplus 4\mathbb{Z}$ is $(0, 0)$, we have the characteristic of $\mathbb{Z}_4$ is 4, but since $4\mathbb{Z}$ is infinite it has 0 characteristic. Hence $\mathbb{Z}_4 \oplus 4\mathbb{Z}$ has characteristic 0.