Extra Problems 1 Solutions

Midterm 1 is on **Friday, April 26 from 1pm to 1:50pm**. If your last name begins with A–R, you will take the exam in Cognitive Science Building 001. If your last name begins with S–Z, you will take the exam in Solis Hall 109.

The following includes textbook problems and problems from past Math 103B courses to give you additional practice for the exam. However, you should still review all past homework problems, lecture notes, discussion notes, and sections 18 through 21 of the textbook.

1. Let $R$ be a ring. The center of $R$ is the set $Z(R) = \{x \in R \mid ax = xa \text{ for all } a \in R\}$. Prove that $Z(R)$ is a subring of $R$.

   **Proof.** Let $R$ be a ring.
   
   - Let $x, y \in Z(R)$. For any $a \in R$, $ax = xa$ and $ay = ya$, which implies that $a(x + y) = ax + ay = xa + ya = (x + y)a$. Therefore, $x + y \in Z(R)$, so $Z(R)$ is closed under addition.
   - For any $a \in R$, $a0 = 0 = 0a$, so $0 \in Z(R)$.
   - Let $x \in Z(R)$. For any $a \in R$, $ax = xa$, which implies that $a(-x) = -(ax) = -(xa) = (-x)a$. Therefore, $-x \in Z(R)$.
   - Let $x, y \in Z(R)$. For any $a \in R$, $ax = xa$ and $ay = ya$, which implies that $a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a$. Therefore, $xy \in Z(R)$, so $Z(R)$ is closed under multiplication.

   Hence, $Z(R)$ is a subring of $R$. \qed

2. Let $R$ be a nonzero ring. Prove that if $a^2 = a$ for all $a \in R$, then the characteristic of $R$ is 2. **Hint:** Consider the element $a + a$ for $a \in R$.

   **Proof.** Let $R$ be a nonzero ring. Suppose that $a^2 = a$ for all $a \in R$. Note that the characteristic of $R$ cannot be 1, since this would imply that every element in $R$ is 0. If $a \in R$, then

   $$a + a = (a + a)^2 = (a + a)(a + a) = a^2 + a^2 + a^2 + a^2 = a + a + a + a.$$  

   Therefore, $a + a = a + a + a + a$, so $a + a = 0$. Since $n = 2$ is the smallest positive integer $n$ such that $n \cdot a = 0$ for all $a \in R$, the characteristic of $R$ is 2. \qed

3. Let $R$ and $R'$ be rings, and let $\phi: R \to R'$ be a ring homomorphism. Prove that if $S$ is a subring of $R$, then $\phi[S]$ is a subring of $R'$.

   **Proof.** Let $R$ and $R'$ be rings and $\phi: R \to R'$ be a ring homomorphism. Let $S$ be a subring of $R$.

   - Let $y_1, y_2 \in \phi[S]$. Then $y_1 = \phi(x_1)$ and $y_2 = \phi(x_2)$ for some $x_1, x_2 \in S$. Since $\phi$ is a homomorphism, $y_1 + y_2 = \phi(x_1) + \phi(x_2) = \phi(x_1 + x_2)$. Since $x_1 + x_2 \in S$ because $S$ is a subring and hence closed under addition, $y_1 + y_2 \in \phi[S]$. 

   - Let $r \in R$ and $y \in \phi[S]$. Then $y = \phi(x)$ for some $x \in S$. Since $\phi$ is a homomorphism, $yr = \phi(r\phi(x)) = \phi(rx)$. Since $rx \in S$, $yr \in \phi[S]$.
Therefore, $\phi[S]$ is closed under addition.

- Since $0 \in S$ and $\phi(0) = 0$, $0 \in \phi[S]$.
- Let $y \in \phi[S]$. Then $y = \phi(x)$ for some $x \in S$. Since $-x \in S$ and $\phi(-x) = -\phi(x) = -y$, $-y \in \phi[S]$.
- Let $y_1, y_2 \in \phi[S]$. Then $y_1 = \phi(x_1)$ and $y_2 = \phi(x_2)$ for some $x_1, x_2 \in S$. Since $\phi$ is a homomorphism, $y_1 y_2 = \phi(x_1) \phi(x_2) = \phi(x_1 x_2)$. Since $x_1 x_2 \in S$ because $S$ is a subring and hence closed under multiplication, $y_1 y_2 \in \phi[S]$. Therefore, $\phi[S]$ is closed under multiplication.

Thus, $\phi[S]$ is a subring of $R'$.

4. Let $R$ be an integral domain such that characteristic of $R$ is a prime number $p$. Prove that $\phi: R \to R$ where $\phi(x) = x^p$ is a ring homomorphism.

\textit{Proof.} Let $R$ be an integral domain such that the characteristic of $R$ is a prime number $p$. Define $\phi: R \to R$ where $\phi(x) = x^p$ for all $x \in R$. Let $x, y \in R$. Then, using the binomial theorem since $R$ is an integral domain and hence commutative,

$$\phi(x + y) = (x + y)^p = \sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i = x^p + y^p = \phi(x) + \phi(y)$$

because $p$ is prime so for $i = 1, \ldots, p - 1$, any binomial coefficient $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ is divisible by $p$. Moreover, $\phi(xy) = (xy)^p = x^p y^p = \phi(x) \phi(y)$ because $R$ is commutative. Therefore, $\phi$ is a ring homomorphism.

5. (§20, #6) Compute the remainder of $2^{(2^{17})} + 1$ when divided by 19. \textit{Hint: You will need to compute the remainder of $2^{17}$ modulo 18.}

Note that $2^{17} = (2^4)^4 \equiv (-2)^4 \equiv 16 \equiv 2 \equiv 14 \mod 18$. Therefore, $2^{17} = 18q + 14$ for some $q \in \mathbb{Z}$.

Now, since 2 and 19 are relatively prime, by Fermat’s theorem, $2^{18} \equiv 1 \mod 19$. Therefore,

$$2^{2^{17}} + 1 = 2^{18q+14} + 1$$
$$= (2^{18})^q 2^{14} + 1$$
$$\equiv 1^q \cdot 2^{14} + 1$$
$$\equiv (2^4)^3 2^2 + 1$$
$$\equiv (-3)^3 \cdot 4 + 1$$
$$\equiv 11 \cdot 4 + 1$$
$$\equiv 7 \mod 19,$$
6. Prove or disprove each of the following statements.

(a) The set of all continuous real-valued functions on $\mathbb{R}$ with the usual addition and multiplication of functions is an integral domain.

False. Take

$$f(x) = \begin{cases} 0 & \text{if } x < 0 \\ x & \text{if } x \geq 0 \end{cases}, \quad g(x) = \begin{cases} x & \text{if } x < 0 \\ 0 & \text{if } x \geq 0 \end{cases}.$$ 

Then $f(x)$ and $g(x)$ are both continuous real-valued functions on $\mathbb{R}$. Since $f(x)$ and $g(x)$ are nonzero but their product is 0, this set contains zero divisors and thus is not an integral domain.

(b) There exists a field of characteristic 6.

False. By HW 2, any integral domain has characteristic 0 or a prime number. Since every field is an integral domain, any field must also have characteristic 0 or a prime number. Since 6 is not prime, no such field exists.

(c) If $R$ is a ring with unity and $S$ is a ring with unity, then $R \times S$ is a ring with unity.

True. Let $1_R$ be the unity of $R$ and $1_S$ be the unity of $S$. Then $(1_R, 1_S)$ is the unity of $R \times S$ because for any $(x, y) \in R \times S$, $(x, y)(1_R, 1_S) = (x1_R, y1_S) = (x, y)$ and $(1_R, 1_S)(x, y) = (1_Rx, 1_Sy) = (x, y)$.

(d) If $R$ is an integral domain and $S$ is an integral domain, then $R \times S$ is an integral domain.

False. $\mathbb{Z}$ is an integral domain but $\mathbb{Z} \times \mathbb{Z}$ is not because $(0, 1)$ is a zero divisor of $\mathbb{Z} \times \mathbb{Z}$: $(0, 1)(1, 0) = (0, 0)$.

7. Find the quotient field of $D = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Justify your answer.

**Proof.** Let $F = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Since $0 = 0 + 0\sqrt{2}$, $0 \in F$. If $x, y \in F$, then $x = a + b\sqrt{2}, y = c + d\sqrt{2}$ for some $a, b, c, d \in \mathbb{Q}$. Then $x + y = (a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in F$ and $xy = (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in F$ because $a + c, b + d, ac + 2bd, ad + bc \in \mathbb{Q}$. Moreover, $-x = -(a + b\sqrt{2}) = -a + (-b)\sqrt{2} \in F$ because $-a, -b \in \mathbb{Q}$. Therefore, $F$ is a subring of $\mathbb{R}$ and hence a ring. Commutativity of multiplication is inherited from $\mathbb{R}$, and $F$ contains $1 = 1 + 0\sqrt{2}$, which is not 0. If $x = a + b\sqrt{2} \in F$ is nonzero, then $a, b \in \mathbb{Q}$ where $a \neq 0$ or $b \neq 0$. Then

$$\frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}} a - b\sqrt{2} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}. $$
Note that $a^2 - 2b^2 \neq 0$. If not, $a^2 = 2b^2$. If $a \neq 0$, then $1 = 2 \left( \frac{b}{a} \right)^2$, so $\frac{1}{2} = \left( \frac{b}{a} \right)^2$, which is a contradiction because $\sqrt{\frac{1}{2}}$ is irrational (since otherwise, $\sqrt{2}$ would also be rational). If $b \neq 0$, then $2 = \left( \frac{a}{b} \right)^2$. If $a = \frac{p}{q}, b = \frac{r}{s}$ for some integers $p, q, r, s$ where $r, s$ are nonzero, then $2 = \left( \frac{ps}{qr} \right)^2$, which is a contradiction because $\sqrt{2}$ is irrational. Therefore, $a, a^2 - 2b^2 + b = \sqrt{2} \in F$, so $F$ is a field.

Since $\mathbb{Z} \subseteq \mathbb{Q}$, $D \subseteq F$. If $x \in F$, then $x = a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$. Then $a = \frac{p}{q}$ and $b = \frac{r}{s}$ for some $p, q, r, s \in \mathbb{Z}$ where $q, s$ are nonzero. Then

$$x = a + b\sqrt{2} = \frac{p}{q} + \frac{r}{s}\sqrt{2} = \frac{ps + qr\sqrt{2}}{qs}.$$ 

Notice that $ps + qr, qs \in \mathbb{Z}$ and $qs \neq 0$ because $q$ and $s$ are nonzero, so $x$ is a quotient of elements in $D$. This shows that $F$ is the quotient field of $D$. $\square$

8. Let $L$ be a field of characteristic 0. Prove that $L$ contains a subfield isomorphic to $\mathbb{Q}$.

**Hint:** Define an injective ring homomorphism from $\mathbb{Z}$ into $L$.

**Proof.** Let $L$ be a field of characteristic 0. Since $L$ contains unity 1, we can define the map $\phi: \mathbb{Z} \to L$ by $\phi(n) = n \cdot 1$. For $m, n \in \mathbb{Z}$,

$$\phi(m + n) = (m + n) \cdot 1 = (m \cdot 1) + (n \cdot 1) = \phi(m) + \phi(n)$$

and

$$\phi(mn) = (mn) \cdot 1 = (m \cdot 1)(n \cdot 1) = \phi(m)\phi(n),$$

so $\phi$ is a ring homomorphism. If $\phi(m) = \phi(n)$ for $m, n \in \mathbb{Z}$, then $m \cdot 1 = n \cdot 1$. Without loss of generality, say $m \geq n$. Since $(m \cdot 1) - (n \cdot 1) = 0$, $(m - n) \cdot 1 = 0$. If $m \neq n$, then $m - n$ is a positive integer and hence $L$ has positive characteristic, which is a contradiction. Therefore, $m = n$, so $\phi$ is injective. This means that $L$ contains a subring isomorphic to $\mathbb{Z}$ and therefore must also contain a subfield isomorphic to $\mathbb{Q}$, the quotient field of $\mathbb{Z}$. $\square$