Ring Theory Midterm

Ata Berk Saraç

April 2025

Question 1. For the ring $R = \mathbb{Z}_{60}$, determine:

a) The set of zero-divisor elements.

b) The set of nilpotent elements.

c) The set of unit elements.

d) The set of idempotent elements.

Solution. The set of zero-divisor elements $Z(R)$ consists exactly of the elements $z \in R$ such that $\gcd(z, 60) \neq 1$.

The set of nilpotent elements $N(R)$ consists exactly of the elements $n \in R$ such that $\gcd(n, 60) = 2 \cdot 3 \cdot 5 = 30$.

The set of unit elements $U(R)$ consists exactly of the elements $u \in R$ such that $\gcd(u, 60) = 1$.

The set of idempotent elements $I(R)$ consists exactly of the elements $e \in R$ such that $e^2 - e = e(e-1) \equiv 0 \pmod{60}$.

The rest is just computation.

$$Z(R) = \{0, 2, 3, 4, 5, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28, 30, 32, 33, 34,\\ 35, 36, 38, 39, 40, 42, 44, 45, 46, 48, 50, 51, 52, 54, 55, 56, 57, 58\},$$

$$N(R) = \{0, 30\},$$

$$U(R) = \{1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59\},$$

$$I(R) = \{0, 1, 16, 21, 25, 36, 40, 45\}.$$

Question 2. Prove that a non-trivial finite ring without non-zero zero divisors is a ring with identity.

Solution. Before we start our proof, we sketch a proof for a claim that we will use. The claim is that if S is a finite semigroup under multiplication, then $a^i = a^{i+p}$ for some minimal i and p for every $a \in S$. So, consider an infinite sequence $a, a^2, a^3, \ldots$, since S is closed and finite, our result follows by the pigeonhole principle.

Now, let R be a non-trivial finite ring without non-zero zero divisors.

We are trying to find an element 1 in R such that $x1 = 1x = x$ for all $x \in R$.

For non-zero $a \in R$ and all $b, c \in R$, if $ab = ac$, we have $ab - ac = a(b - c) = 0$ implies that $b = c$, a similar approach follows for $ba = ca$. Thus, right/left cancellation property holds in R.

Fix a non-zero element e of R, and assume that $e^i = e^{i+n}$ for some minimal i and n (since we treat R as a finite semigroup under multiplication). If $x \mapsto xe$ is a mapping called f, then f is injective since whenever $xe = ye$, we have $x = y$ for all $x, y \in R$, by cancellation. Since R is finite, f is bijective. Note that additivity property holds for f since $f(x) + f(y) = xe + ye = (x + y)e = f(x + y)$ for all $x, y \in R$. It follows that $f(e^i) = e^{i+1}$ and $f(e^{i+n}) = e^{i+n+1}$ so that $f(e^{i+n}) - f(e^i) = f(e^{i+n} - e^i) = (e^{i+n} - e^i)e = 0e = f(0)$, hence $e^{i+n+1} = e^{i+1}$ so that $e^{n+1} - e = 0$ by cancellation.

It implies that $0x = (e^{n+1} - e)x = e(e^n x - x) = 0$, implying that $e^n x = x$, by a similar algebraic computation $x0 = x(e^{n+1} - e) = (xe^n - x)e = 0$ implying that $xe^n = x$ so that e^n is the identity we are looking for, for all $x \in R$. We have completed our proof.

Question 3. Define a regular ring, and prove that $R = M_2(\mathbb{R})$ is a regular ring.

Solution. A ***regular ring*** is a ring S where for each $a \in S$, there exists $x \in S$ such that $a = axa$.

For invertible $A \in R$, the result follows by a simple computation: $A = AXA$ if and only if $X = A^{-1}$.

For any non-invertible matrix $A \in R$ of rank $r = 0, 1, 2$, there exist invertible $U, V \in R$ such that $A = U \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} V$. We examine the case $r = 1$ only (since $r = 0$ is trivial and $r = 2$ implies that A is invertible): if $A = \begin{pmatrix} x & y \\ ax & ay \end{pmatrix}$, for all nonzero $x, y \in \mathbb{R}$ and some $a \in \mathbb{R}$, then $A = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ -x & y \end{pmatrix}$. We have found that for

$$X = \begin{pmatrix} 1/2x & -1/2x \\ 1/2y & 1/2y \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -a & 1 \end{pmatrix},$$

we have the required result. We are done.

Question 4. Show that $S = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} \mid a \in \mathbb{R} \right\}$ is a subring of $M_2(\mathbb{R})$ and find the unity element of S.

Solution. Since $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in S$, S is nonempty.

For all $a, b \in \mathbb{R}$, $a - b \in \mathbb{R}$ and so $\begin{pmatrix} a & a \\ a & a \end{pmatrix} - \begin{pmatrix} b & b \\ b & b \end{pmatrix} = \begin{pmatrix} a-b & a-b \\ a-b & a-b \end{pmatrix} \in S$.

For all $a, b \in \mathbb{R}$, $2ab \in \mathbb{R}$ and so $\begin{pmatrix} a & a \\ a & a \end{pmatrix} \begin{pmatrix} b & b \\ b & b \end{pmatrix} = \begin{pmatrix} 2ab & 2ab \\ 2ab & 2ab \end{pmatrix}$.

Thus, S is a subring of R.

For all $a, b \in \mathbb{R}$, we have $\begin{pmatrix} a & a \\ a & a \end{pmatrix} \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} = \begin{pmatrix} a & a \\ a & a \end{pmatrix}$ for all $\begin{pmatrix} a & a \\ a & a \end{pmatrix}$ and so $\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} \in S$ is the identity element of S.

Question 5. Give an example of a subring of $R = \mathbb{Z}_5 \times \mathbb{Z}_5$ that is not an ideal of R, and write all the ideals of R.

Solution. Since 5 is prime, the only ideals of $\mathbb{Z}_5$ are the trivial ones. Thus, $\{0\} \times \{0\}$, $\{0\} \times \mathbb{Z}_5$, $\mathbb{Z}_5 \times \{0\}$, $\mathbb{Z}_5 \times \mathbb{Z}_5$.

Here is an example of a subring of R that is not an ideal: $2\mathbb{Z}_5 \times \mathbb{Z}_5$.

Question 6. Consider the set of all rational numbers $\mathbb{Q}$, where the binary operations are defined as:

$$a \oplus b = a + b - 1, \qquad a \odot b = ab - (a + b) + 2.$$

a) Show that $R = (\mathbb{Q}, \oplus, \odot)$ is a ring.

b) Is R commutative?

c) Is there an identity element in R?

d) Is R an integral domain?

Solution. a) Clearly, R inherits its additive closure and commutativity from $\mathbb{Q}$, $1 \in \mathbb{Q}$ is the additive identity of R, and $-a+1 \in \mathbb{Q}$ is the additive inverse of $a \in R$, lastly, for all $a, b, c \in R$,

$$(a \oplus b) \oplus c = (a+b-1) \oplus c = a+b-1+c-1 = a+(b+c-1)-1 = a+(b \oplus c)-1 = a \oplus (b \oplus c).$$

R inherits its multiplicative closure from $\mathbb{Q}$, R is associative under multiplication

$$\begin{aligned}
(a \odot b) \odot c &= (ab - (a + b) + 2) \odot c \\
&= (ab - (a + b) + 2)c - ((ab - (a + b) + 2) + c) + 2 \\
&= abc - ac - bc + 2c - ab + a + b - 2 - c + 2 \\
&= abc - ab - ac + 2a - a - bc + b + c - 2 + 2 \\
&= a(bc - (b + c) + 2) - (a + (bc - (b + c) + 2)) + 2 \\
&= a \odot (bc - (b + c) + 2) \\
&= a \odot (b \odot c)
\end{aligned}$$

for all $a, b \in \mathbb{Q}$

b) R inherits its multiplicative commutativity from the additive and multiplicative commutativity of $\mathbb{Q}$.

c) $a \odot b = ab - (a+b) + 2 = a$, then $ab - 2a = a(b-2) = b - 2$ for all $a \in \mathbb{Q}$, which means that $b = 2$ is the identity of R.

d) $a \odot b = ab - (a+b) + 2 = 0$, then $a = \frac{2-b}{1-b}$, thus such natural number pairs $a, b \neq 1 = 0_R$ are zero-divisors of R.

Question 7. Let R be a ring such that for all $x \in R$, $x^2 + x$ is in $Z(R)$, the center of R. Prove that R is commutative.

Solution. We assume that for any $x \in R$, $x^2 + x$ is in the center $Z(R)$ of the ring R. This means that for any $x, a \in R$, we have $(x^2 + x)a = a(x^2 + x)$. Expanding, we obtain that

$$x^2 a + xa = ax^2 + ax$$

This implies that

$$x^2 a - ax^2 = ax - xa \quad (*)$$

This equality holds for all $x, a \in R$.

Consider the element $(a+b)^2 + (a+b)$ for any elements $a, b \in R$. By assumption, this element is in the center of R.

$$(a+b)^2 + (a+b) = a^2 + ab + ba + b^2 + a + b$$

So, for all $c \in R$, we have:

$$(a^2 + ab + ba + b^2 + a + b)c = c(a^2 + ab + ba + b^2 + a + b)$$

Using the fact that $a^2 + a \in Z(R)$ and $b^2 + b \in Z(R)$, we have $a^2c + ac = ca^2 + ca$ and $b^2c + bc = cb^2 + cb$. Expanding the previous equality:

$$a^2c + ac + bc + b^2c + abc + bac = ca^2 + ca + cb + cb^2 + cab + cba$$

Subtracting the terms $a^2c + ac + bc + b^2c$ from the left-hand side and their equivalents $ca^2 + ca + cb + cb^2$ from the right-hand side, we have:

$$abc + bac = cab + cba$$

for all $a, b, c \in R$.

Let $c = a$ in the identity above, then

$$aba + baa = aab + aba$$

$$aba + ba^2 = a^2b + aba$$

Cancelling aba on both sides, we obtain:

$$ba^2 = a^2b$$

for all $a, b \in R$. The commutativity of R follows since $(*)$ becomes $ax - xa = 0$.