MAT401 – Problem Set 1: SOLUTIONS

EXERCISE 12-2

Observe that:

$0 \times 6 \equiv 0 \equiv 0 \pmod{10}$
$2 \times 6 \equiv 12 \equiv 2 \pmod{10}$
$4 \times 6 \equiv 24 \equiv 4 \pmod{10}$
$6 \times 6 \equiv 36 \equiv 6 \pmod{10}$
$8 \times 6 \equiv 48 \equiv 8 \pmod{10}$

Therefore the unity is 6. ¤

EXERCISE 12-13

All subrings of Z can be expressed in the form nZ for some non-negative $n \in Z$. From the textbook (pg 239, example 10) we know that nZ is a subring of Z. Suppose R is a subring of Z. If R contains only 0, then it is the same as 0Z. So suppose R contains at least one non-zero elements. Let g = gcd(R) be the greatest integer dividing all non-zero elements of R. We know $g \in R$, since the greatest common divisor of any set of numbers can be constructed by summing multiples of the elements of R. Since g generates gZ, we can conclude that gZ is a subring of R. Now suppose $\exists r \in R$ such that $r \notin gZ$. This means that $\forall x \in Z$, $x \times g \neq r \Rightarrow g \nmid r$, which contradicts the definition of g as the greatest common divisor. Thus R is a subring of gZ, and R = gZ.
¤

EXERCISE 12-19

Denote the centre of a ring R as $Z(R) = \{x \in R \mid ax = xa, \forall a \in R\}$. Since $\forall a \in R$, $a0 = 0a$, $0 \in Z(R)$ and thus Z(R) is non-empty. Let $u, v \in Z(R)$ be arbitrary. Then $\forall a \in R$, $au = ua$ and $av = va$. So $(u - v)a = ua - va = au - av = a(u - v)$, and thus $u - v \in Z(R)$.
Also, $(uv)a = u(va) = u(av) = (ua)v = (au)v = a(uv)$, so $uv \in Z(R)$.
Therefore, by the subring test, Z(R) is a subring of R. ¤

EXERCISE 12-22

Denote the unity in R as I_R. To show that U(R) is a group under the multiplication operator in R, we will show that it satisfies the four properties of a group.
<u>Identity:</u> $I_R \times I_R = I_R$, so $I_R \in U(R)$. Since $\forall r \in U(R)$, $r \times I_R = r$,
I_R is the identity in U(R).
<u>Inverse</u>: Suppose $a \in U(R)$. Then $\exists a^{-1} \in R$ such that
$a \times a^{-1} = a^{-1} \times a = I_R$.
So $a^{-1} \in U(R)$, and thus every element has an inverse.
<u>Closure</u>: Suppose $a, b \in U(R)$. Then were know $\exists a^{-1}, b^{-1} \in U(R)$ such that
$a \times a^{-1} = I_R$ and $b \times b^{-1} = I_R$.
Since R is closed under multiplication, we know that

$a \times b$, $b^{-1} \times a^{-1} \in R$. So $(a \times b) \times (b^{-1} \times a^{-1}) = a \times (b \times b^{-1}) \times a^{-1} = a \times a^{-1} = I_R$.
Thus $a \times b$ has an inverse in R, and is therefore in U(R). Therefore U(R) is closed under multiplication.

<u>Associativity</u>: Since R is a ring, we know that

$\forall a, b, c \in R, (a\times b)\times c = a \times (b \times c)$

Thus $\forall a, b, c \in U(R), (a \times b) \times c = a \times (b \times c)$.

Therefore, U(R) is a group under the multiplication of R. ¤

<u>Exercise 13-4</u>

List all zero divisors of Z_{20}:

Observe that:

$2 \times 10 = 20 \equiv 0 (\mathrm{mod}\ 20)$

$4 \times 5 = 20 \equiv 0 (\mathrm{mod}\ 20)$

$5 \times 8 = 40 \equiv 0 (\mathrm{mod}\ 20)$

$6 \times 10 = 60 \equiv 0 (\mathrm{mod}\ 20)$

$8 \times 5 = 40 \equiv 0 (\mathrm{mod}\ 20)$

$10 \times 8 = 80 \equiv 0 (\mathrm{mod}\ 20)$

$12 \times 10 = 120 \equiv 0 (\mathrm{mod}\ 20)$

$14 \times 10 = 140 \equiv 0 (\mathrm{mod}\ 20)$

$15 \times 4 = 60 \equiv 0 (\mathrm{mod}\ 20)$

$16 \times 5 = 80 \equiv 0 (\mathrm{mod}\ 20)$

$18 \times 10 = 180 \equiv 0 (\mathrm{mod}\ 20)$

$S_1 = \{2,4,5,6,8,10,12,14,15,16,18\}$ is the set of zero divisors of Z_{20}.

$S_2 = \{1,3,7,9,11,13,17,19\}$ is the set of units of Z_{20}.

Note: One can easily observe that $|S_2| = 8 = \phi(20)$ [Euler Phi function]

- All numbers which are not zero are either zero divisors or units of Z_{20}.

<u>Exercise 13-13</u>

Show that $\exists b \in R$ such that $(1 - a) \times b = 1$, where $a^n = 0$.

Let $b = 1+a+a^2+...+a^{n-2}+a^{n-1}$.

Since R is closed under both + and $\times$, $b \in R$.

Computing $a \times b$ we get

$a \times b = b - (a \times 1) - (a \times a) - ... - (a \times a^{n-1}) = b - (a + a^2 + ... + a^n) = 1 - a^n = 1 - 0 = 1$
(taking for granted associative and commutative properties of +). Thus b is the multiplicative inverse of $1 - a$. ¤