M E T U
Department of Mathematics

<table>
<tr><td colspan="2"></td><td colspan="2">Basic Algebraic Structures
FINAL EXAM</td><td></td></tr>
<tr><td colspan="2">Code : Math 116
Acad. Year : 2018 Spring
Instructor : A.Beyaz, G.Ercan, M.Kuzucuoğlu, Ö.Küçüksakallı F.Özbudak.
Date : June 3, 2018
Time : 9:30
Duration : 120 minutes</td><td colspan="3">Last Name :
Name : Student No. :
Department : Section :
Signature :

4 QUESTIONS ON 4 PAGES
100 TOTAL POINTS</td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td></td></tr>
</table>

1. (25pts) Let R be a ring. Consider $Z(R) = \{x \in R \mid xr = rx \text{ for all } r \in R\}$.

(a) Prove that $Z(R)$ is a subring of R.

Solution: The additive identity $0 = 0_R$ is an element of $Z(R)$. This is because $0r = r0$ for all $r \in R$. Thus $Z(R)$ is nonempty.

Let x and y be elements of $Z(R)$. We have $xr = rx$ and $yr = ry$ for all $r \in R$. Our purpose is to show that $x - y \in Z(R)$ and $xy \in Z(R)$.

For all $r \in R$, we have

$$(x - y)r = xr - yr = rx - ry = r(x - y).$$

Here, the first and the last equality are obtained by the distributive laws. The equality in the middle holds because $x \in Z(R)$ and $y \in Z(R)$. We conclude that $x-y \in Z(R)$.

Secondly, we have

$$xyr = xry = rxy.$$

for all $r \in R$. Here, the first and the second equalities follow from $x \in Z(R)$ and $y \in Z(R)$, respectively. Thus we have $xy \in Z(R)$.

(b) Give an example of a ring R such that $Z(R)$ is not an ideal of R.

Solution: If R is a commutative ring then $R = Z(R)$ and therefore $Z(R)$ is trivially an ideal. We shall look for a counterexample of a ring R in which the ring multiplication is not commutative.

Indeed, any non-commutative ring with unity constitutes a counterexample. In such a case pick $x \in R - Z(R)$. On the other hand $1_R \in Z(R)$ but $1_R \cdot x \notin Z(R)$. Thus $Z(R)$ is not an ideal.

In particular, the ring of quaternions is a concrete example. Recall that $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$. Observe that $1_\mathbb{R} \in Z(\mathbb{H})$ but $i \notin Z(\mathbb{H})$. On the other hand $1_\mathbb{R} \cdot i = i \notin Z(\mathbb{H})$.

2. (25pts) Let $a \in \mathbb{Z}$. Define the map $\alpha : \mathbb{Z} \longrightarrow \mathbb{Z}_{15}$ by $\alpha(n) = [an]$ for each $n \in \mathbb{Z}$.

(a) Show that α is a ring homomorphism if and only if $a^2 \equiv a \pmod{15}$.

Solution: Suppose that $\alpha : \mathbb{Z} \longrightarrow \mathbb{Z}_{15}$ is a ring homomorphism. We have

$$[a] = \alpha(1) = \alpha(1 \cdot 1) = \alpha(1)\alpha(1) = [a][a] = [a^2].$$

It follows that $a \equiv a^2 \pmod{15}$.

Conversely suppose that $a^2 \equiv a \pmod{15}$. Let x and y be elements of $\mathbb{Z}$. We have

$$\alpha(xy) = [axy] = [a^2xy] = [ax][ay] = \alpha(x)\alpha(y).$$

Moreover,

$$\alpha(x + y) = [a(x + y)] = [ax + ay] = [ax] + [ay] = \alpha(x) + \alpha(y)$$

We conclude that α is a ring homomorphism.

(b) Now fix $a = 6$. For this choice, find $\mathrm{Im}(\alpha)$ and $\mathrm{Ker}(\alpha)$.

Solution: By definition, we have $\mathrm{Im}(\alpha) = \{\alpha(x) \mid x \in \mathbb{Z}\}$. For $a = 6$, the image is given by $\{[6x] \mid x \in \mathbb{Z}\}$. Clearly, $\mathrm{Im}(\alpha) \supseteq \{[0], [3], [6], [9], [12]\}$. Conversely, $\mathrm{Im}(\alpha) \subseteq \{[0], [3], [6], [9], [12]\}$ because $\gcd(6, 15) = 3$. We conclude that

$$\mathrm{Im}(\alpha) = \{[0], [3], [6], [9], [12]\}.$$

By definition, we have $\mathrm{Ker}(\alpha) = \{x \in \mathbb{Z} \mid \alpha(x) = [0]\}$. For $a = 6$, the kernel is given by $\{x \in \mathbb{Z} \mid [6x] = [0]\}$. Observe that $15|6x \Leftrightarrow 5|2x \Leftrightarrow 5|x$. We see that $x \in \mathrm{Ker}(\alpha)$ if and only if $5|x$. Therefore

$$\mathrm{Ker}(\alpha) = \langle 5 \rangle = \{5k \mid k \in \mathbb{Z}\}.$$

3. (25pts) Let $R = \mathbb{Z}_{12}$ and $I = \langle[3]\rangle$ be the principal ideal of R generated by $[3]$.

(a) List all elements of $I = \langle[3]\rangle$. (Hint: $|I| = 4$)

Solution: $I = \langle[3]\rangle = \{[3], [6], [9], [0]\}$.

(b) List all elements of R/I. (Hint: $|R/I| = 3$)

Solution: $R/I = \{[0] + I, [1] + I, [2] + I\}$.

(c) Find the addition and the multiplication tables of the quotient ring R/I.

Solution: The addition table of the quotient ring R/I is as follows:

$+$	$[0]+I$	$[1]+I$	$[2]+I$
$[0]+I$	$[0]+I$	$[1]+I$	$[2]+I$
$[1]+I$	$[1]+I$	$[2]+I$	$[0]+I$
$[2]+I$	$[2]+I$	$[0]+I$	$[1]+I$

The multiplication table of the quotient ring R/I is as follows:

$*$	$[0]+I$	$[1]+I$	$[2]+I$
$[0]+I$	$[0]+I$	$[0]+I$	$[0]+I$
$[1]+I$	$[0]+I$	$[1]+I$	$[2]+I$
$[2]+I$	$[0]+I$	$[2]+I$	$[1]+I$

(d) Is R/I an integral domain?

Solution: Yes! The ring $R = Z_{12}$ is commutative. It follows that R/I is commutative, too. Note that $[1]+I$ is the multiplicative identity of R/I. Finally, each possible pairs of nonzero elements have nonzero products. We verify this by checking each case as follows:

$$([1] + I)([1] + I) = ([1] + I) \neq ([0] + I),$$
$$([1] + I)([2] + I) = ([2] + I) \neq ([0] + I),$$
$$([2] + I)([1] + I) = ([2] + I) \neq ([0] + I),$$
$$([2] + I)([2] + I) = ([1] + I) \neq ([0] + I).$$

(e) Is R/I a field?

Solution: Yes! The quotient ring R/I has three elements and it is an integral domain. It follows that R/I is a field because any finite integral domain is a field.

4. (25pts) Let $f(x) = x^4 + 4x^3 + 8x^2 + 9x + 2$ and $g(x) = x^3 + 4x^2 + 7x + 6$ be elements of the ring $\mathbb{R}[x]$.

(a) Show that the greatest common divisor of $f(x)$ and $g(x)$ is $d(x) = x + 2$.

Solution: We apply the Euclidean algorithm:

$$\begin{aligned} f(x) &= g(x) \cdot x + (x^2 + 3x + 2) \\ g(x) &= (x^2 + 3x + 2) \cdot (x + 1) + (2x + 4) \\ x^2 + 3x + 2 &= (2x + 4) \cdot \left(\frac{x}{2} + \frac{1}{2}\right) + 0 \end{aligned}$$

Recall that the greatest common divisor is monic by definition. We conclude that the greatest common divisor of $f(x)$ and $g(x)$ is $d(x) = x + 2$.

(b) Find polynomials $s(x)$ and $t(x)$ in $\mathbb{R}[x]$ such that $d(x) = f(x)s(x) + g(x)t(x)$.

Solution: We apply the Euclidean algorithm in reverse:

$$\begin{aligned} 2x + 4 &= g(x) - (x^2 + 3x + 2)(x + 1) \\ &= g(x) - (f(x) - xg(x))(x + 1) \\ &= f(x) \cdot (-(x + 1)) + g(x) \cdot (x^2 + x + 1). \end{aligned}$$

We can pick $s(x) = -(x + 1)/2$ and $t(x) = (x^2 + x + 1)/2$ which are elements of $\mathbb{R}[x]$.

(c) Write $g(x)$ as a product of irreducible polynomials over $\mathbb{R}$.

Solution: Observe that $g(x) = (x+2)(x^2+2x+3)$. It is obvious that the term $x+2$ is irreducible. The quadratic term $x^2 + 2x + 3$ is irreducible if and only if it has no real zeroes. Completing it to a square, we find that $x^2+2x+3 = (x+1)^2+2$. It is obvious that this expression is strictly positive. Thus the polynomial x^2+2x+3 is irreducible over $\mathbb{R}$, too. The (unique) factorization of $g(x)$ into irreducibles is $(x+2)(x^2+2x+3)$.