M E T U Department of Mathematics

Math 116 Basic Algebraic Structures Spring 2019 Final Exam 1 June 2019 09:30		
F U L L N A M E	S T U D E N T I D	DURATION 120 MINUTES
7 QUESTIONS ON 4 PAGES	SHOW ALL YOUR WORK	TOTAL 80 POINTS

By signing below, I pledge that I will write this examination as my own work and without the assistance of others or the usage of unauthorized material or information. I understand that possession of any kind of electronic device during the exam is prohibited. I also understand that not obeying the rules of the examination will result in immediate cancellation and disciplinary procedures.

Signature ....

***(12 pts)* 1.** Let $G = \{x \in \mathbb{R} : -1 < x < 1\}$. Consider the binary operation $*$ on G given by

$$x * y = \frac{x+y}{1+xy}$$

for all $x, y \in G$. You are **given that** the binary operation $*$ is associative. Show that G is a group and is abelian, with respect to the binary operation $*$.

Since we are already given that $*$ is associative, we check the other properties. Note that $0 \in G$ and moreover, for every $x \in G$, we have that

$$0 * x = \frac{0+x}{1+0x} = \frac{x}{1} = x$$

and

$$x * 0 = \frac{x+0}{1+x0} = \frac{x}{1} = x$$

Thus, 0 is the identity element of the binary operation $*$. Now, let $x \in G$. Then, $-1 < x < 1$ and so $-1 < -x < 1$, which means that $-x \in G$. Moreover, we have that

$$x * (-x) = \frac{x + (-x)}{1 + x(-x)} = \frac{0}{1-x^2} = 0 = \frac{(-x)+x}{1+(-x)x} = (-x) * x$$

Therefore, $-x$ is the inverse of x with respect to $*$. Since $*$ is associative, has an identity in G and every element in G has an inverse with respect to $*$, we have that G is a group with respect to $*$. We now check that $(G, *)$ is abelian. Let $x, y \in G$. Then we have that

$$x * y = \frac{x+y}{1+xy} = \frac{y+x}{1+yx} = y * x$$

Therefore, $(G, *)$ is abelian.

(6 pts) **2.** By writing f as a product of transpositions, determine whether the following permutation in S_9 is even or odd.

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 1 & 5 & 8 & 3 & 4 & 2 & 9 & 6 \end{bmatrix}$$

We have that $f = (172)(35)(4896) = (12)(17)(35)(46)(49)(48)$ and hence f is even since it is a product of even number of transpositions.

(4+4+4+4+4 pts) **3.** Let G be a group and let e denote the identity element of G. Suppose that there exists a positive integer n such that $(xy)^n = x^n y^n$ for all $x, y \in G$. Consider the following subsets

$$H = \{x^n : x \in G\} \quad \text{and} \quad K = \{x \in G : x^n = e\}$$

You are given that H is a subgroup of G.

a) Show that K is a subgroup of G and is normal.

Note that $e^n = e$ and so $e \in K$, which means that $K \neq \emptyset$. Now, let $x, y \in K$. Then, by definition, $x^n = e$ and $y^n = e$, which means that $y^{-n} = (y^{-1})^n = e$. It then follows from the given assumption that $(xy^{-1})^n = x^n(y^{-1})^n = e$ and so $xy^{-1} \in K$. Therefore, K is a subgroup of G.

To prove that K is normal, let $g \in G$ and $k \in K$. Then, $e = k^n$ and

$$(gkg^{-1})^n = (gkg^{-1})(gkg^{-1})\dots(gkg^{-1}) = gk^n g^{-1} = gg^{-1} = e$$

and so $gkg^{-1} \in K$. This shows that K is normal in G.

b) Show that the map $\varphi : G/K \to H$ given by $\varphi(xK) = x^n$ is well-defined.

Let $x, y \in G$ be such that $xK = yK$. Then $xy^{-1} \in K$ and so $(xy^{-1})^n = e$. Then, by the given assumption, $e = (xy^{-1})^n = x^n(y^{-1})^n = x^n y^{-n} = x^n(y^n)^{-1}$ and so $x^n = y^n$, that is, $\varphi(xK) = \varphi(yK)$. Thus, φ is well-defined.

c) Show that φ is an epimorphism.

Let $xK, yK \in G/K$. Then we have that

$$\varphi(xK \cdot yK) = \varphi(xyK) = (xy)^n = x^n y^n = \varphi(xK)\varphi(yK)$$

Thus, φ is a homomorphism. Now, let $h \in H$. Then, by the definition of H, there exists $g \in G$ such that $h = g^n$. Then, $gK \in G/K$ and so $\varphi(gK) = g^n = h$. Therefore, φ is onto and so is an epimorphism.

d) Find the kernel of φ.

Let $gK \in ker(\varphi)$, that is, $\varphi(gK) = e$. Then, by definition, $g^n = e$ and so $g \in K$. This means that $gK = K$, which is the identity of G/K. Thus, the kernel of φ is $\{K\}$.

e) Is φ an isomorphism? Explain your answer.

The kernel of φ is the trivial subgroup by part d and hence φ is one-to-one. By part c, φ is an epimorphism. Thus, being a one-to-one epimorphism, φ is an isomorphism.

***(6+6 pts)* 4.** Consider the polynomials $f(x) = 2x^3 + x$ and $g(x) = x^2 + x + 1$ in $\mathbb{Z}_3[x]$.

a) Find the greatest common divisor $d(x)$ of $f(x)$ and $g(x)$ in $\mathbb{Z}_3[x]$. Show your work.

Applying Euclidean algorithm for polynomials, we can get that

$$\begin{aligned} f(x) &= g(x)(2x+1) + (x+2) \\ g(x) &= (x+2)(x+2) + 0 \end{aligned}$$

Since $x+2$ is monic, the greatest common divisor of $f(x)$ and $g(x)$ is $d(x) = x + 2$.

b) Find polynomials $p(x), q(x) \in \mathbb{Z}_3[x]$ such that $d(x) = f(x)p(x) + g(x)q(x)$. Show your work.

Using the computations in part a, one gets that

$$\begin{aligned} d(x) = (x+2) &= f(x) - g(x)(2x+1) \\ &= f(x) \cdot 1 + g(x)(-2x-1) \\ &= f(x) \cdot 1 + g(x)(x+2) \end{aligned}$$

***(6 pts)* 5.** Let $p > 1$ be an integer with the property that for all $a, b \in \mathbb{Z}$, if $p|ab$, then $p|a$ or $p|b$. Show that p is prime.

Assume towards a contradiction that p is not prime. Then, by definition, there exists $1 < a, b < p$ such that $p = ab$. But then, $p \mid p = ab$, however, $p \nmid a$ and $p \nmid b$ since $1 < a, b < p$. This contradicts the given assumption.

(6+6 pts) **6.** Consider the set of polynomials $I = \{f(x) \in \mathbb{Z}[x] : f(0) \text{ is even}\}$.

a) Show that I is an ideal of $\mathbb{Z}[x]$.

Clearly, that the zero polynomial is in I and hence $I \neq \emptyset$. Now, let $f(x), g(x) \in I$. Then, by definition, $f(0)$ and $g(0)$ are even. It follows that $f(0) - g(0)$ is even and so the polynomial $f(x) - g(x)$ is in I.

Now, let $f(x) \in I$ and $g(x) \in \mathbb{Z}[x]$. Then, $f(0)$ is even and so $f(0)g(0) = g(0)f(0)$ is even. It follows that the polynomials $f(x)g(x)$ and $g(x)f(x)$ are in I. This completes the proof that I is an ideal of $\mathbb{Z}[x]$.

b) Show that for every $f(x) \in I$, there exists $g(x), h(x) \in \mathbb{Z}[x]$ such that $f(x) = x \cdot g(x) + 2 \cdot h(x)$.

Let $f(x) = a_0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n \in I$. Then, by definition, $f(0) = a_0$ is even, that is, $a_0 = 2k$ for some $k \in \mathbb{Z}$. Set $h(x) = k$ and $g(x) = a_1 + a_2x^1 + \cdots + a_nx^{n-1}$. It then follows that

$$f(x) = a_0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n = a_0 + x(a_1 + a_2x^1 + \cdots + a_nx^{n-1}) = 2 \cdot h(x) + x \cdot g(x)$$

(3+3+3+3 pts) **7.** Let $R = \{x, y, z, t\}$. You are given the fact that R is a commutative ring with respect to the addition $+$ and the multiplication $*$ whose tables are given below.

$+$	x	y	z	t
x	x	y	z	t
y	y	x	t	z
z	z	t	x	y
t	t	z	y	x

$*$	x	y	z	t
x	x	x	x	x
y	x	y	z	t
z	x	z	t	y
t	x	t	y	z

For parts a,b and c of this question, you do **not** need to justify your answer.

a) What is the zero element of R, that is, the additive identity of R? **x**

b) If it exists, what is the unity of R, that is, the multiplicative identity of R? **y**

c) If they exist, list the zero divisors of R. **There are no zero divisors**.

d) Is R a field? Explain your answer.

Solution 1. Since there are no zero divisors, R is an integral domain. However, we know that finite integral domains are fields and hence R is a field

OR

Solution 2. It suffices to show that every non-zero element has a multiplicative inverse. It follows from the multiplication table that $y * y = y$ and $z * t = t * z = y$. That is, y is the multiplicative inverse of itself, and t and z are multiplicative inverses of each other. So every non-zero element has a multiplicative inverse. This means that R is a field.