M E T U   Department of Mathematics

Math 116 Basic Algebraic Structures Spring 2019 Midterm I 13 March 2019 17:40		
F U L L N A M E	S T U D E N T I D	DURATION 70 MINUTES
5 QUESTIONS ON 2 PAGES		TOTAL 40(+3) 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 ....

***(4+4+4 pts)* 1.** a) Using the Euclidean algorithm, find the greatest common divisor d of 178 and 87.

Applying Euclidean algorithm, we have

$$\begin{aligned} 178 &= 87 \cdot 2 + 4 \\ 87 &= 4 \cdot 21 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

and hence the greatest common divisor of 178 and 87 is 1, which is the last non-zero remainder in the process.

b) Find integers $x, y \in \mathbb{Z}$ such that $d = 178x + 87y$.

Using the equalities we obtained during the Euclidean algorithm, we have that

$$\begin{aligned} 1 &= 4 + 3 \cdot (-1) \\ 1 &= 4 + (87 + 4 \cdot (-21)) \cdot (-1) = 4 \cdot 22 + 87 \cdot (-1) \\ 1 &= 4 \cdot 22 + 87 \cdot (-1) = (178 + 87 \cdot (-2)) \cdot 22 + 87 \cdot (-1) \\ 1 &= 178 \cdot 22 + 87 \cdot (-45) \end{aligned}$$

c) Does $[87]$ have an inverse in $\mathbb{Z}_{178}$ with respect to multiplication? If so, find its inverse. If not, explain why there is no inverse.

By part b, we have that $1 = 178 \cdot 22 + 87 \cdot (-45)$ and hence $178 \mid 87 \cdot (-45) - 1$, which means that $87 \cdot (-45) \equiv 1\ (mod 178)$. Therefore, $[87][-45] = [87][133] = [133][87] = [1]$ in $\mathbb{Z}_{178}$ and hence, $[133]$ is the inverse of $[87]$ with respect to multiplication in $\mathbb{Z}_{178}$.

***(4+4 pts)* 2.** Let a, b, d, m be positive integers such that d is the greatest common divisor of a and b. Let k, ℓ be positive integers such that $a = dk$ and $b = d\ell$.

a) Show that k and ℓ are relatively prime, that is, the greatest common divisor of k and ℓ is 1.

Since d is the greatest common divisor of a and b, there exist integers x and y such that $d = ax + by$. It follows from $d = dkx + d\ell y$ that $1 = kx + \ell y$. This implies that $\gcd(x, y) | 1$ and so $\gcd(x, y) = 1$, that is, x and y are relatively prime.

OR

Set $e = \gcd(k, \ell)$. Since $e|k$ and $e|\ell$, by definition, we have that $k = ek'$ and $\ell = e\ell'$ for some integers k' and ℓ'. Then, $a = dek'$ and $b = de\ell'$ and hence, we have $de|a$ and $de|b$. It follows from the definition of the greatest common divisor that $de|d$ and so $e|1$. Thus $e = 1$.

b) Show that if $a|bm$, then $k|m$.

Assume that $a|bm$. Then, as $a = dk$ and $b = d\ell$, we have $dk|d\ell m$ and so $k|\ell m$. Since $k|\ell m$ and k and ℓ are relatively prime by part a, we have that $k|m$.

<u>***(4+4 pts)* 3.**</u> Consider the binary operation $*$ on $\mathbb{Z}$ given by

$$a * b = \begin{cases} a+b & \text{if } a \text{ is even} \\ ab & \text{if } a \text{ is odd} \end{cases}$$

a) Is the binary operation $*$ commutative?

By the definition of $*$, we have that $1 * 0 = 1 \cdot 0 = 0$ and $0 * 1 = 0 + 1 = 1$. Since $1 * 0 \neq 0 * 1$, the binary operation $*$ is not commutative.

b) Does the binary operation $*$ have an identity element?

We claim there exists no identity element of $*$. Assume towards a contradiction that $*$ has an identity element, say, $i \in \mathbb{Z}$ is an identity element of $*$. Then, by the definition of identity, we should have that $1 * i = 1$ and $0 * i = 0$. However, the first equality implies that $i = 1 \cdot i = 1 * i = 1$ and the second equality implies that $i = 0 + i = 0 * i = 0$, which is a contradiction. Therefore, $*$ does not have an identity element.

<u>***(4+4 pts)* 4.**</u> Consider the subset $\mathcal{M} = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} : a \in \mathbb{R} \right\}$ of $M_{2x2}(\mathbb{R})$.

a) Is the set $\mathcal{M}$ closed with respect to matrix multiplication? Does $\mathcal{M}$ have an identity with respect to matrix multiplication?

Let $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$ be elements of $\mathcal{M}$. Then we have that

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 \cdot 1 + a \cdot 0 & 1 \cdot b + a \cdot 1 \\ 0 \cdot 1 + 1 \cdot 0 & 0 \cdot b + 1 \cdot 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}$$

is in $\mathcal{M}$ as $a+b \in \mathbb{R}$. Therefore, $\mathcal{M}$ is closed with respect to matrix multiplication. Clearly $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in \mathcal{M}$ and moreover, we have that $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ for every $a \in \mathbb{R}$. Thus, $\mathcal{M}$ contains an identity with respect to matrix multiplication.

b) Show that every element of $\mathcal{M}$ has an inverse in $\mathcal{M}$ with respect to matrix multiplication.

Let $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \in \mathcal{M}$. Then $\begin{bmatrix} 1 & -a \\ 0 & 1 \end{bmatrix} \in \mathcal{M}$ and moreover,

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -a \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+(-a) \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Thus, every element of $\mathcal{M}$ has an inverse in $\mathcal{M}$ with respect to matrix multiplication.

<u>***(7 pts)* 5.**</u> Let $*$ be an associative binary operation on a non-empty set X. Let $\mathcal{H} = \mathcal{P}(X) - \{\emptyset\}$. Consider the binary operation $\square$ on the set $\mathcal{H}$ given by

$$A \square B = \{a * b \mid a \in A, b \in B\}$$

for all $A, B \in \mathcal{H}$. Show that $\square$ is associative.

We wish to show that $(A \square B) \square C = A \square (B \square C)$ for all $A, B, C \in \mathcal{H}$. Let $x \in (A \square B) \square C$. Then $x = y * c$ for some $y \in A \square B$ and $c \in C$. Since $y \in A \square B$, there exist $a \in A$ and $b \in B$ such that $y = a * b$. Thus $x = (a * b) * c$. By associativity of $*$, we have that $x = a * (b * c)$. But then, since $a \in A$ and $b * c \in B \square C$, we have that $x \in A \square (B \square C)$. Therefore, $(A \square B) \square C \subseteq A \square (B \square C)$. Now, let $x \in A \square (B \square C)$. Then $x = a * z$ for some $a \in A$ and $z \in B \square C$. Since $z \in B \square C$, there exist $b \in B$ and $c \in C$ such that $z = b * c$ and so, $x = a * (b * c)$. By associativity of $*$, we have that $x = (a * b) * c$. But then, since $a * b \in A \square B$ and $c \in C$, we have that $x \in (A \square B) \square C$. Therefore, $A \square (B \square C) \subseteq (A \square B) \square C$, which completes the proof that $(A \square B) \square C = A \square (B \square C)$.