M E T U Department of Mathematics

Math 116 Basic Algebraic Structures Spring 2019 Midterm II 10 April 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 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 ....

***(8+2+2 pts)* 1.** Consider the **well-defined** binary operation $*$ on the set $\mathbb{Z}_3 \times \mathbb{Z}_2$ given by

$$([a],[b]) * ([c],[d]) = ([a+c],[b+d]) \text{ for all } a,b,c,d \in \mathbb{Z}$$

a) Show that $\mathbb{Z}_3 \times \mathbb{Z}_2$ is an abelian group with respect to $*$.

Let $a,b,c,d,e,f \in \mathbb{Z}$ be integers. Then we have that

$$\Big(([a],[b]) * ([c],[d])\Big) * ([e],[f]) = ([a+c],[b+d]) * ([e],[f]) = ([(a+c)+e],[(b+d)+f]) = ([a+(c+e)],[b+(d+f)])$$

$$= ([a],[b]) * ([c+e],[d+f]) = ([a],[b]) * \Big(([c],[d]) * ([e],[f])\Big)$$

and hence $*$ is **associative**. Now, let $a,b \in \mathbb{Z}$. Then we have that

$$([a],[b]) * ([0],[0]) = ([a+0],[b+0]) = ([a],[b]) = ([0+a],[0+b]) = ([0],[0]) * ([a],[b])$$

and hence $*$ has an **identity element**, which is $([0],[0])$. For any $a,b \in \mathbb{Z}$, we have that

$$([a],[b]) + ([-a],[-b]) = ([a-a],[b-b]) = ([0],[0]) = ([-a+a],[-b+b]) = ([-a],[-b]) * ([a],[b])$$

and hence every element $([a],[b])$ has an **inverse element** with respect to $*$, namely, the element $([-a],[-b])$. Finally, for any $a,b,c,d \in \mathbb{Z}$, we have that

$$([a],[b]) * ([c],[d]) = ([a+c],[b+d]) = ([c+a],[d+b]) = ([c],[d]) * ([a],[b])$$

and hence $*$ is **commutative**. Therefore, $\mathbb{Z}_3 \times \mathbb{Z}_2$ is an abelian group with respect to $*$.

b) Find the order of the element $([1],[1])$ in the group $\mathbb{Z}_3 \times \mathbb{Z}_2$.

We have that $([1],[1])^1 = ([1],[1])$, $([1],[1])^2 = ([2],[0])$, $([1],[1])^3 = ([0],[1])$, $([1],[1])^4 = ([1],[0])$, $([1],[1])^5 = ([2],[1])$ and $([1],[1])^6 = ([0],[0])$. Thus the order of $([1],[1])$ is 6.

c) Is the group $\mathbb{Z}_3 \times \mathbb{Z}_2$ (with respect to $*$) a cyclic group?

By part b, we have that $\langle([1],[1])\rangle = \{([1],[1]),([2],[0]),([0],[1]),([1],[0]),([2],[1]),([0],[0])\} = \mathbb{Z}_3 \times \mathbb{Z}_2$ and hence $\mathbb{Z}_3 \times \mathbb{Z}_2$ is cyclic.

***(6 pts)* 2.** Let G, H be groups and $f : G \to H$ be a group **isomorphism** and $a \in G$ be an element. Prove that if $G = \langle a \rangle$, then $H = \langle f(a) \rangle$.

Assume that $G = \langle a \rangle$. We wish to show that $H = \langle f(a) \rangle$. It is clear that $\langle f(a) \rangle = \{f(a)^k : k \in \mathbb{Z}\} \subseteq H$ as a group is closed with respect to its group operation. To prove the converse inclusion, let $h \in H$. Since f is an isomorphism, f is surjective and consequently, there exists $g \in G$ such that $f(g) = h$. On the other hand, it follows from $G = \langle a \rangle$ that $g = a^\ell$ for some $\ell \in \mathbb{Z}$. Since f is a homomorphism, we have that $h = f(g) = f(a^\ell) = f(a)^\ell \in \langle f(a) \rangle$. Thus $H \subseteq \langle f(a) \rangle$ and hence $H = \langle f(a) \rangle$.

(4+4 pts) **3.** You are **given** that the set $G = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a, b \in \mathbb{R} \text{ and } a > 0, b > 0 \right\}$ is a group with respect to matrix multiplication. Consider the following subset of G.

$$H = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a, b \in \mathbb{R} \text{ and } a > 0, b > 0 \text{ and } ab = 1 \right\}$$

a) Show that H is a subgroup of G.

It is clear that $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in H$ and hence $H \neq \emptyset$. Let $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \in H$. Then, $ab = 1$ and $cd = 1$. It follows that

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \cdot \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}^{-1} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \cdot \begin{bmatrix} \frac{1}{c} & 0 \\ 0 & \frac{1}{d} \end{bmatrix} = \begin{bmatrix} \frac{a}{c} & 0 \\ 0 & \frac{b}{d} \end{bmatrix} \in H$$

since $\frac{a}{c}\frac{b}{d} = \frac{ab}{cd} = \frac{1}{1} = 1$. Therefore, H is a subgroup of G.

b) Show that the map $\varphi : G \to \mathbb{R} - \{0\}$ given by $\varphi\left(\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\right) = ab$ is a homomorphism where $\mathbb{R} - \{0\}$ is considered as a group with respect to multiplication.

Let $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \in G$. Then we have that

$$\varphi\left(\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \cdot \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}\right) = \varphi\left(\begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix}\right) = (ac)(bd) = (ab)(cd) = \varphi\left(\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\right)\varphi\left(\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}\right)$$

Thus, φ is a homomorphism.

(4+4 pts) **4.** Let G be a cyclic group of order 18 and $a \in G$ be an element such that $G = \langle a \rangle$.

a) Find all generators of G.

By a theorem that we proved in class, if $G = \langle a \rangle$, then $G = \langle a^1 \rangle = \langle a^m \rangle$ if and only if $(m, |G|) = 1$. Thus, the generators of G are exactly those elements of the form a^m where $1 \leq m < 18$ and $(m, 18) = 1$. It follows that the generators of G are $a^1, a^5, a^7, a^{11}, a^{13}$ and a^{17}.

b) List all distinct subgroups of G.

We proved in class that the subgroups of G are exactly those subgroups of the form $\langle a^d \rangle$ where d is a positive divisor of 18. Thus, G has six subgroups which are $\langle a^1 \rangle, \langle a^2 \rangle, \langle a^3 \rangle, \langle a^6 \rangle, \langle a^9 \rangle$ and $\langle a^{18} \rangle$.

(2+4 pts) **5.** Consider the group $\mathbb{Z}_{14}^* = \{[a] \in \mathbb{Z}_{14} : (a, 14) = 1\} = \{[1], [3], [5], [9], [11], [13]\}$ with respect to multiplication.

a) Determine whether or not $\mathbb{Z}_{14}^*$ is cyclic.

We have that $[3]^1 = [3]$, $[3]^2 = [9]$, $[3]^3 = [27] = [13]$, $[3]^4 = [81] = [11]$, $[3]^5 = [243] = [5]$ and $[3]^6 = [1]$. Thus, the order of $[3]$ is 6 and $\langle [3] \rangle = \{[3]^k : k \in \mathbb{Z}\} = \mathbb{Z}_{14}^*$. Thus $\mathbb{Z}_{14}^*$ is cyclic.

b) Determine whether or not $\mathbb{Z}_{14}^*$ isomorphic to S_3.

S_3 is not abelian and $\mathbb{Z}_{14}^*$ is abelian. Therefore, these cannot be isomorphic.

OR

S_3 is not cyclic and $\mathbb{Z}_{14}^*$ is cyclic (by part a.) Therefore, these cannot be isomorphic.