Midterm (solutions)

This is a **closed book** exam. To get the full credit, write complete, detailed solutions. No credit will be given for an answer without a proof.

Problem 1 (10 points)**.** *a)* Let H be a group. What does it mean for H to be *non-commutative*?

b) Let G be a commutative group, and H a *non-commutative* group. Prove that there is no injective homomorphism

$$\varphi\colon H \to G.$$

Solution. *a)* Recall that a group $(H,*)$ is commutative if **for any** $x, y \in H$ we have

$$x * y = y * x. \tag{1}$$

The negation of this statement is that equation (1) does not hold 'all the time', i.e.,

$$\boxed{\textbf{there exist } x, y \in H \text{ such that } \quad x * y \neq y * x} \tag{2}$$

■

Note. Quantifiers are essential in mathematical proofs. Without a specified quantifier, one can not interpret a statement rigorously.

b) Since $(H,*)$ is not commutative, by (a) there exist elements $x, y \in H$ such that (2) hold:

$$x * y \neq y * x.$$

Let $\varphi\colon (H,*) \to (G,\circ)$ be any homomorphism. We are about to prove that φ is not injective. Indeed, by homomorphism property we have

$$\varphi(x*y) = \varphi(x)\circ\varphi(y) \quad \text{and} \quad \varphi(y*x) = \varphi(y)\circ\varphi(x).$$

On the other hand, since $(G,\circ)$ is commutative, we have

$$\varphi(x)\circ\varphi(y) = \varphi(y)\circ\varphi(x).$$

Consequently

$$\varphi(x*y) = \varphi(y*x), \quad \text{yet } x*y \neq y*x.$$

Therefore φ is not injective (since the preimage of $\varphi(y*x) \in G$ has at least to elements $x*y$ and $y*x$ in H). ■

Problem 2 (10 points)**.** Consider group[1] $G = \mathbb{Z} \times \mathbb{Z}_3$.

a) Find all elements $g \in G$ of finite order.

b) Find an *infinite* proper subgroup $H \subsetneq G$.

Solution. *a)* The neutral element with respect to addition in $\mathbb{Z}\times\mathbb{Z}_3$ is $(0,[0])$.

Let $g = (a,[b])$ be any element in $\mathbb{Z}\times\mathbb{Z}_3$, so that

$$a \in \mathbb{Z}, \quad [b] \in \mathbb{Z}_3.$$

Then

$$\underbrace{g + \cdots + g}_{k \text{ times}} = (ka,[kb]).$$

This element can not possibly equal to $(0,[0])$ unless $a = 0$. On the other hand, if $a = 0$ and $k = 3$, then clearly

$$(0,[b]) + (0,[b]) + (0,[b]) = (0,[3b]) = (0,[0]).$$

So the elements of finite order are

$$\boxed{(0,[0]), \quad (0,[1]), \quad (0,[2])}$$

■

[1] As usual, groups $\mathbb{Z}$ and $\mathbb{Z}_n$ are considered with respect to addition.

b) There are many infinite subgroups in $\mathbb{Z} \times \mathbb{Z}_3$. It is enough to take any element g other than elements in (a). Then g has infinite order, hence the cyclic group generated by g

$$\langle g \rangle \subset \mathbb{Z} \times \mathbb{Z}_3$$

will be infinite. For instance, for $g = (1, [0])$ we would get

$$\boxed{\langle (1,[0]) \rangle = \mathbb{Z} \times \{[0]\} \subset \mathbb{Z} \times \mathbb{Z}_3}$$

Another option would be fix $m > 1$ and consider

$$\boxed{m\mathbb{Z} \times \mathbb{Z}_3 = \{(ma,[b]) \mid a \in \mathbb{Z}, [b] \in \mathbb{Z}_3\} \subset \mathbb{Z} \times \mathbb{Z}_3}$$

■

Problem 3 (10 points)**.** Prove or disprove: for any of the following statements, figure out if it is true or false, by either proving it or providing a counterexample.

a) Group $\mathbb{Z}_{100}$ has a subgroup of order $d \in \mathbb{Z}$ for every divisor d of 100.

b) Set H consisting of matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

is a group with respect to matrix multiplication and is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Solution. a) $\boxed{\text{True.}}$ Indeed, if d is any divisor of an integer n, then we can consider cyclic subgroup of $\mathbb{Z}_n$ generated by $a = n/d$:

$$\langle n/d \rangle = \{[0], [n/d], [2n/d], [3n/d], \ldots, [(d-1)n/d]\}.$$

This subgroup has exactly d. Instead of listing all the elements, as we just did, one might invoke the result from class stating that for $[k] \in \mathbb{Z}_n$

$$\operatorname{ord}([k]) = \frac{n}{\gcd(n,k)},$$

so for $a = n/d$ we would have $\operatorname{ord}([a]) = d$. ■

b) $\boxed{\text{True}}$ We check that H is a subgroup of $GL_2(\mathbb{R})$ which would imply that H is a group itself. To this end we need to check that

1. For any $h_1, h_2 \in H$ we have $h_1 h_2 \in H$;
2. For any $h \in H$ we have $h^{-1} \in H$.

Since the first matrix is the identity matrix (let us call it e), the two properties obviously hold for it. Hence we need to check both properties for the remaining three matrices.

If we denote the last three matrices in the order above by h_1, h_2, h_3, we can easily check that

$$h_1^2 = h_2^2 = h_3^2 = e,$$

$$h_1 h_2 = h_2 h_1 = h_3,\ h_1 h_3 = h_3 h_1 = h_2,\ h_3 h_2 = h_2 h_3 = h_1.$$

This proves that H is a subgroup of $GL_2(\mathbb{R})$ and a group itself.

To prove that H is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, we define a bijection

$$\varphi \colon H \to \mathbb{Z}_2 \times \mathbb{Z}_2$$

sending

$$e \mapsto (0,0), \quad h_1 \mapsto (0,1), \quad h_2 \mapsto (1,0), \quad h_3 \mapsto (1,1).$$

Multiplication law for h_i which we deduced above shows that the bijective map φ is also a homomorphism. ■

Problem 4 (10 points)**.** Consider a group $G = \mathbb{Z} \times \mathbb{Z}$ and let H to be a subset

$$H = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x \text{ and } y \text{ are even}\} \subset H$$

a) Prove that H is a subgroup.

b) How many left cosets gH are there?

Solution. *a*) As in 3(b), we need to check that H is closed under the groups operation in G and under taking an inverse.

But this is trivial, since given any $(x_1, y_1), (x_2, y_2) \in H$ we will have

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2) \in H$$

since both numbers $(x_1 + x_2)$ and $(y_1 + y_2)$ are even, provided x_1, x_2, y_1, y_2 are even.

Similarly the inverse of (x_1, y_1) is $(-x_1, -y_1)$, which is also in H. ■

b) Group $G = \mathbb{Z} \times \mathbb{Z}$ can be split into disjoint union of four cosets with respect to H (left and right cosets coincide in this problem, since G is commutative):

$$\begin{aligned}(0,0) + H =& \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x \text{ and } y \text{ are even}\}\\(1,0) + H =& \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x \text{ is odd and } y \text{ is even}\}\\(0,1) + H =& \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x \text{ is even and } y \text{ is odd}\}\\(1,1) + H =& \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x \text{ and } y \text{ are odd}\}\end{aligned}$$

Hence there are $\boxed{\text{4 cosets}}$.

■

Problem 5 (10 points)**.** Let p be a prime number.

a) How many multiples of p are there in the set $\{1, 2, \dots, p^k\}$?

b) Find the size of the group $(\mathbb{Z}_{p^k}^\times, \times)$.

Solution. *a*) Every p^{th} number is divisible by p:

$$p, 2p, 3p, 4p, \dots.$$

Therefore among the numbers $\{1, 2, \dots, p^k\}$ there are exactly

$$\boxed{p^k/p = p^{k-1}}$$

multiples of p ■.

b) The group $(\mathbb{Z}_n^\times, \times)$ consists of units in $\mathbb{Z}_n$, i.e., congruence classes $[u]$ such that, there exists a congruence class $[v]$:

$$uv = 1 \mod n.$$

In class we have proved that congruence class $[u]$ is a unit if and only if $\gcd(n, u) = 1$. For $n = p^k$, as in our problem, this is equivalent to the claim that u is **not** divisible by p. The number os such equivalence classes is

$$(\text{number of all congruence classes}) - (\text{answer in (a)}) = \boxed{p^k - p^{k-1}}.$$

■

Problem 6 (10 points)**.** *a*) Find three non-isomorphic groups of order 8.

(Make sure to prove that the groups are indeed non-isomorphic.)

b) Find a subgroup of order 2 in each of these groups.

Solution. *a*) We consider groups

$$\boxed{\mathbb{Z}_8,\ \mathbb{Z}_4 \times \mathbb{Z}_2,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2}$$

and want to prove that they are not isomorphic to each other.

1. $\mathbb{Z}_8$ is not isomorphic to either of the two remaining groups, since $\mathbb{Z}_8$ is the only group having an element of order 8 ($[1]_8 \in \mathbb{Z}_8$), and isomorphisms must preserve orders of elements.
2. $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ since $\mathbb{Z}_2 \times \mathbb{Z}_4$ has an element of order 4 ($([1]_4, [0]_2) \in \mathbb{Z}_4 \times \mathbb{Z}_2$) while all non-identity elements of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ are of order 2.

b) To find a subgroup of order 2 in each of the above groups, we provide an element of order 2, so that the cyclic group generated by this element will have size 2:

$$[4]_8 \in \mathbb{Z}_8$$
$$([2]_4,\ [0]_2) \in \mathbb{Z}_4 \times \mathbb{Z}_2$$
$$([1]_2,\ [0]_2,\ [0]_2) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

■