

MAT 444: Test 1 Solutions

1. (a) *Define group homomorphism and group isomorphism.*

If G and H are groups, and *group homomorphism* from G to H is a function $f : G \rightarrow H$ such that for all $a, b \in G$,

$$f(a * b) = f(a) * f(b).$$

A *group isomorphism* is a bijective group homomorphism.

- (b) *Define the order of an element of a group.*

If g is an element of a group G , the order of g is $|\langle g \rangle|$.

Alternatively, it would be acceptable to define the order of g as the smallest positive integer n such that $g^n = e$, and as infinite if no such positive integer exists.

- (c) *State Cayley's Theorem.*

Every group is isomorphic to a group of permutations.

2. *For $\mathbb{Z}_{36}$, give the orders of the subgroups of the given group and how many different subgroups there are for each order. (E.g., if D_5 was listed, the answer would be “there is 1 subgroup of order 1, 5 subgroups of order 2, 1 subgroup of order 5, and 1 subgroup of order 10.) No justification needs to be given.*

There is one subgroup of each of the following orders: 1, 2, 3, 4, 6, 9, 12, 18, 36

3. (a) *What is the order of 270 in $\mathbb{Z}_{10000}$.*

The order of 270 is $|\mathbb{Z}_{10000}| / \gcd(270, 10000) = 10000/10 = 1000$.

- (b) *If $\sigma = (1, 2, 3, 4)(5, 6, 7, 8, 9, 10)(11, 12, 13)$, compute σ^2 , and express it in disjoint cycle notation.*

You have to track what happens when it goes two steps forward in its cycle:
 $(1, 3)(2, 4)(5, 7, 9)(6, 8, 10)(11, 13, 12)$

4. *Determine, up to isomorphism, all abelian groups of order $625 = 5^4$. No justification needed.*

$\mathbb{Z}_{625}$, $\mathbb{Z}_5 \times \mathbb{Z}_{125}$, $\mathbb{Z}_{25} \times \mathbb{Z}_{25}$, $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_{25}$, and $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$

5. *What is the largest order of an element in $\mathbb{Z}_{12} \times \mathbb{Z}_{20} \times \mathbb{Z}_{75}$, and give an example of an element of that order.*

In a direct product, the order of an element is the least common multiple of the orders of its components. So the largest order is achieved by $(1, 1, 1)$ which has order $\text{lcm}(12, 20, 75) = 300$.

6. (a) *State Lagrange's theorem.*

If H is a subgroup of G , then $|G| = |H| \cdot [G : H]$.

(b) *Prove Lagrange's theorem.*

Define $\sim$ on G by $a \sim b \iff a^{-1}b \in H$. We show $\sim$ is an equivalence relation.

(R) For all $a \in G$, $a^{-1}a = e \in H$, so $a \sim a$.

(S) If $a \sim b$, then $a^{-1}b \in H$, but then $b^{-1}a = (a^{-1}b)^{-1} \in H$, so $b \sim a$.

(T) If $a \sim b$ and $b \sim c$, then $a^{-1}b \in H$ and $b^{-1}c \in H$, so $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$.

So, $\sim$ is an equivalence relation. Thus G is partitioned by the equivalence classes.

The equivalence class of a is

$$\begin{aligned} \{b \in G \mid a \sim b\} &= \{b \in G \mid a^{-1}b \in H\} \\ &= \{b \in G \mid a^{-1}b = h \text{ for some } h \in H\} \\ &= \{b \in G \mid b = ah \text{ for some } h \in H\} \\ &= \{ah \mid h \in H\} \\ &= aH \end{aligned}$$

So, G is partitioned by the left cosets of H . Now for each left coset aH , let $f : H \rightarrow aH$ be given by $f(h) = ah$. For all $x \in aH$, $x = ah$ for some $h \in H$, and so $f(h) = ah = x$ proving f is onto. If $f(x) = f(y)$, then $ax = ay$, but this implies $x = y$ by left cancellation. Thus f is also 1-1, so it is bijective and $|H| = |aH|$. Therefore, $|G| = |H| \cdot [G : H]$ where $[G : H]$ is the number of left cosets of H in G .

7. Suppose $f : G \rightarrow H$ is a group isomorphism and $g \in G$. Prove $|g| = |f(g)|$.

Note, for all $n \in \mathbb{Z}^+$,

$$f(g^n) = f(g \cdot g \cdot g \cdots g) = f(g) \cdot f(g) \cdot f(g) \cdots f(g) = f(g)^n$$

Now, if $g^n = e$, then $f(g)^n = f(g^n) = f(e) = e$. Conversely, if $f(g)^n = e$, then $f(g^n) = f(g)^n = e = f(e)$, so $g^n = e$ since f is injective. So, $\boxed{g^n = e \iff f(g)^n = e}$. This implies $|g| = |f(g)|$.

For more justification on the last statement, the boxed statement shows some positive power of g is the identity iff some positive power of $f(g)$ is the identity, so one has infinite order iff the other has infinite order. Otherwise, they both have finite order, and the smallest positive power giving the identity must then be the same for both.

8. Let G be a group and $g \in G$. Let $H = \{n \in \mathbb{Z} \mid g^n = e\}$. Prove that H is a subgroup of $\mathbb{Z}$.

First we note $g^0 = e$ (by the definition of g^0), so $0 \in H$.

Next, if $n, m \in H$, then $g^n = e$ and $g^m = e$. So,

$$g^{n+m} = g^n g^m = e \cdot e = e$$

Thus, $n + m \in H$.

Finally, if $n \in H$, then $e = g^n$. Taking the inverse of both sides we get $e = e^{-1} = (g^n)^{-1} = g^{-n}$. Thus, $-n \in H$.

Therefore, H is a subgroup of $\mathbb{Z}$.

9. Find, with justification, the order of $(1, 0) + \langle(2, 4)\rangle$ in $\mathbb{Z}_6 \times \mathbb{Z}_8 / \langle(2, 4)\rangle$.

First, we list the elements of the cyclic subgroup:

$$\langle(2, 4)\rangle = \{(0, 0), (2, 4), (4, 0), (0, 4), (2, 0), (4, 6)\}$$

Now we list multiples of $(1, 0) + \langle(2, 4)\rangle$ until we hit one where the representative is in the subgroup:

$$1 \cdot ((1, 0) + \langle(2, 4)\rangle) = (1, 0) + \langle(2, 4)\rangle$$

$$2 \cdot ((1, 0) + \langle(2, 4)\rangle) = (2, 0) + \langle(2, 4)\rangle$$

Since $(1, 0) \notin \langle(2, 4)\rangle$ but $(2, 0) \in \langle(2, 4)\rangle$, the order is 2.