MATH 375.17

Class 17: PracTest Selected Answers

1. **a)** Suppose that $g \in G$, a group and that $g^{12} = e$. What can you say about $|g|$? **Solution:** $|g| \Big| 12 \Rightarrow |g| = 1, 2, 3, 4, 6$, or 12.

b) Suppose that $x \in \mathbf{Z}_{35}$. What can you say about $|x|$? **Solution:** By Sam's Theorem $|x| \Big| 35 \Rightarrow |x| = 1, 5, 7$ or 35.

c) Suppose that $\phi : G \to \mathbf{Z}_{35}$ is a group homomorphism of the groups in parts (a) and (b). What are the possible choices for $\phi(g)$ in $\mathbf{Z}_{35}$? Explain. **Solution:** Since ϕ is a homomorphism, $|\phi(g)| \Big| |g|$. But from the previous two parts, the only possibility is $|\phi(g)| = 1$, so $\phi(g) = 0$.

2. **a)** Show that $|S_4| = |D_{12}|$. Prove that S_4 is **not** isomorphic to D_{12}. **Solution:** D_{12} has an element of order 12 (namely r_{30}). But the maximum order of an element in S_4 is 4 (as you can check). Since the order of an element is preserved under isomorphism, there can't be any isomorphism between these two groups *even though both groups have the same number of elements,* $4! = 24 = 12 \times 2$.

b) Prove that neither is isomorphic to $\mathbf{Z}_{24}$. **Solution:** $\mathbf{Z}_{24}$ is cyclic, the other two are not.

3. Let $G = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$. Note that G is a group under addtion. Show that $\mathbf{Z} \cong G$. Do this by finding a mapping $\phi : Z \to G$ which you verify is an isomorphism. **Solution:** Both are infinite cyclic groups. Use the mapping $\phi(n) = 3n$ or $\gamma(n) = -3n$. These are the only two possible isomorphisms, which are easily checked.

4. Find three elements that generate $\mathbf{Z}_{10}$ and two that don't. **Solution:** Generators are $1, 3, 7, 9$ (elements relatively prime to 10). All others are not generators.

5. **a)** Let H be a subgroup of an **abelian** group G. Let $K = \{a \in G | a^2 \in H\}$. (In other words, a is in K if its square is in H.) Is K a subgroup of G? **Solution:** Use the two step method. Closure: Let $a, b \in K$. Show that $ab \in K$, that is, show $(ab)^2 \in H$. But $a, b \in K$ means that a^2 and b^2 are in H. So because G is abelian,

$$(ab)^2 = (ab)(ab) = a^2 b^2 \in H$$

because H is closed and both a^2 and b^2 are in H. Inverses: Let $a \in K$. Show $a^{-1} \in K$, that is, show $(a^{-1})^2 \in H$. But $a \in K$, so $a^2 \in H$. Since H is a subgroup, $(a^2)^{-1} = (a^{-1})^2 \in H$.

6. Find $|400|$ in $\mathbf{Z}_{532}$. **Solution:** $|400| = \frac{532}{\gcd(532,400)} = \frac{532}{4} = 133$.

7. Suppose that $a^6 = a^{10}$ in a group. What is the **maximum** possible order of a? **Solution:** We have $|a| \Big| 6$ and $|a| \Big| 10$, so $|a| \Big| \gcd(6, 10) = 2$. So the maximum possible order is 2.

8. Express $\alpha = (1, 3, 4, 5, 2)(1, 2, 3, 4, 6, 5)(3, 2, 4, 1, 5)$ as a product of disjoint cycles, and as a product of transpositions. What is its order? Is it odd or even? Find its inverse. **Solution:** $\alpha = (134)(26) = (14)(13)(26)$. $|\alpha| = \text{lcm}(3, 2) = 6$, It is odd. $\alpha^{-1} = (62)(431)$.

9. **a)** Determine whether the function $f : \mathbf{R}^2 \to \mathbf{R}^2$ by $f(x, y) = (x + y, x + 2y)$ is one-to-one.**Solution:** Assume $f(a, b) = f(x, y)$. Show $(a, b) = (x, y)$. But

$$f(a,b) = f(x,y) \iff (a+b, a+2b) = (x+y, x+2y) \iff \begin{cases} a+b = x+y \\ a+2b = x+2y \end{cases}$$

$$\iff \begin{cases} a+b = x+y \\ b = y \end{cases} \iff \begin{cases} a = x \\ b = y \end{cases}$$

$$\iff (a,b) = (x,y)$$

b) Is it onto? **Solution:** Let $(c,d) \in \mathbf{R}^2$ (codomain). Find $(x,y) \in \mathbf{R}^2$ so that $f(x,y) = (c,d)$. But

$$f(x,y) = (c,d) \iff (x+y, x+2y) = (c,d) \iff \begin{cases} x+y=c \\ x+2y=d \end{cases} \iff \begin{cases} x+y=c \\ y=d-c \end{cases} \iff \begin{cases} x=2c-d \\ y=d-c \end{cases}$$

So let $(x,y) = (2c-d, d-c)$.

c) Is it a group homomorphism? **Solution:** Let $(a,b), (c,d) \in \mathbf{R}^2$.

$$\begin{aligned} f((a,b)+(c,d)) = f((a+c, b+d)) &= ((a+c)+(b+d), (a+c)+2(b+d)) \\ &= ((a+b)+(c+d), (a+2b)+(c+2d)) \\ &= (a+b, a+2b)+(c+d, c+2d) \\ &= f(a,b)+f(c,d). \end{aligned}$$

So it is a group homomorphism.

10. From a previous homework: Let $a \in G$, where G is a group. Define $f: G \to G$ by $f(g) = aga^{-1}$. Show that f is a one-to-one, onto, group homomorphism. **Solution:** Injective: Note that by cancellation.

$$\phi(g) = \phi(h) \iff aga^{-1} = aha^{-1} \iff g = h.$$

Surjective: Let $b \in G$. We must find $g \in G$ so that $\phi(g) = b$. But

$$\phi(g) = b \iff aga^{-1} = b \iff g = a^{-1}ba.$$

Note that $g = a^{-1}ba \in G$ since G is a group and it closed and has inverses. Homomorphism: Let $g, h \in G$. Then

$$\phi(g)\phi(h) = (aga^{-1})(aha^{-1}) = ag(a^{-1}a)ha^{-1} = a(gh)a^{-1} = \phi(gh).$$

11. **a)** If possible, find a one-to-one function from $\mathbf{Z}^+$ to $\mathbf{Z}^+$ that is not onto. **Solution:** There are many: How about $f(n) = (n+1)$. Notice that there is no $n \in \mathbf{Z}^+$ such that $f(n) = 1$ because $f(n) = n+1 = 1 \iff n = 0 \notin \mathbf{Z}^+$. So f is not onto, but it is injective because $f(n) = f(m) \iff n+1 = m+1 \iff m = n$.

b) If possible, find an onto function from $\mathbf{Z}^+$ to $\mathbf{Z}^+$ that is not one-to-one. **Solution:** There are many: How about:

$$f(n) = \begin{cases} 1, & \text{if } n = 1 \\ n-1, & \text{if } n > 1 \end{cases}.$$

Then $f(1) = f(2) = 1$, so f is not injective, but it is surjective because if $m \in \mathbf{Z}^+$, then $f(n) = m \Rightarrow n-1 = m \Rightarrow n = m+1 \in \mathbf{Z}^+$.

12. Let $G = \langle a \rangle$ be a cyclic group of order n. Suppose that there is an element $g \in G$ of order 2. Prove that n is even. **Solution:** Since $g \in \langle a \rangle$, then $g = a^k$, where $0 \le k < n$. Since $|g| = 2$, then $g \ne e$ so $k \ne 0$. But then, $g^2 = e \Rightarrow (a^k)^2 = a^{2k} = e$, where $2 \le 2k < 2n$. But $n \mid 2k$, and so we must have $n = 2k$. That is, n is even.

13. **a)** What is the largest possible order of an element in S_9. **Solution:** The largest possible order is 20 (use disjoint 4 and 5-cycles).

b) True or false: If α and β are in S_4 and $|\alpha| = 2$ and $|\beta| = 3$, then $|\alpha\beta| = 6$. **Solution:** False: Let $\alpha = (12)$ and $\beta = (123)$. Then $(12)(123) = (23)$ So $|\alpha| = 2$ and $|\beta| = 3$, but $|\alpha\beta| = 2$.

14. Let $\beta \in S_7$. Suppose that $\beta^4 = (2143567)$. Find β. **Solution:** If you are being careful, note that $|\beta^4| \Big| |\beta|$ since $\beta^4 \in \langle \beta \rangle$. So $7 \Big| |\beta|$. But you can check that the only elements of S_7 whose orders are divisible by 7 are 7-cycles. So $|\beta| = 7$. Thus, $(\beta^4)^2 = \beta^8 = \beta^1 = \beta = (2457136)$.

15. Assume that $\phi : V_4 \to \mathbf{Z}_4$ is a group homomorphism. Prove that ϕ is not an isomorphism. **Solution:** Recall that V_4 is the Klein Four-Group with Cayley Table

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Notice that the square of every element is e, so there is no element of order 4. But $\mathbf{Z}_4$ is cyclic of order 4. So the groups cannot be isomorphic.

16. Is there an isomorphism $\phi : U(14) \to \mathbf{Z}_6$. Explain. **Solution:** Yes. Verify that

$$U(14) = \{1, 3, 5, 9, 11, 13\} =< 3 > .$$

That is, $U(14)$ is a cyclic group of order 6 so it isomorphic to $\mathbf{Z}_6$.

17. Here's one I was going to put on the test. Assume that $\phi : G_1 \to G_2$ is a homomorphism such that the **only** element that ϕ maps onto $e_2 \in G_2$ is the identity is $e_1 \in G_1$. Prove that ϕ is injective. **Solution:** Assume that $\phi(a) = \phi(b)$. Then notice that

$$\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(b)\phi(b^{-1}) = \phi(bb^{-1}) = \phi(e_1) = e_2.$$

By assumption, since only e_1 is mapped to e_2, then $ab^{-1} = e_1 \Rightarrow a = b$. So ϕ is injective.

18. The following 8 permuations in S_4 are known as the **Octic group**, $O = \{e, a, a^2, a^3, b, g, d, t\}$, where $e = (1)$, $a = (1\,2\,3\,4)$, $b = (1\,4)(2\,3)$, $g = (1\,2)(3\,4)$, $d = (1\,3)$, and $t = (2\,4)$, and $t = gd = dg$.

a) Construct a group table for O.

b) Find the cyclic subgroups of O. **Solution:**

$$
\begin{aligned}
< e > &= \{e\} \\
< a^2 > &= \{e, a^2\} \\
< a > &= \{e, a, a^2, a^3\} =< a^3 > \\
< b > &= \{e, b\} \\
< c > &= \{e, c\} \\
< d > &= \{e, d\} \\
< g > &= \{e, g\} \\
< t > &= \{e, t\}
\end{aligned}
$$