MATH 375.12

Class 12: Selected Answers

1. **a)** **Reading**: Chapter 5. Later in the week, look ahead to Chapter 6.

b) See the Web page `www.hws.edu/PEO/faculty/mitchell/math375/index.html` for previous answers and lecture notes.

c) Gallian page 107ff: #1, 3, 5, 9, 11, 13, 21 Assigned earlier: Gallian: page 80–81 #17, 21, 25, 31, 43, 51

2. **a)** Let G be a group. Let a be a fixed element of G. Prove that $\phi : G \to G$ by $\phi(g) = ag$ is one-to-one.

b) Prove that ϕ is onto.

c) What is the mapping ϕ^{-1}?

3. Write each of the following permutations as a product of disjoint cycles. What is the order of each. Find the inverse of each. Write each as a product of transpositions. Determine which are odd and which are even.

a) $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = (123)(45)$, so $|\alpha| = \text{lcm}(3,2) = 6$. $\alpha^{-1} = (54)(321)$. Finally, $\alpha = (13)(12)(45)$, so it is odd.

b) $\beta = (1358)$, so $|\beta| = 4$. $\beta^{-1} = (8531)$. Finally, $\beta = (18)(15)(13)$, so it is odd.

c) $\gamma = (15367)$, so $|\gamma| = 5$. $\gamma^{-1} = (76351)$. Finally, $\gamma = (17)(16)(13)(15)$, so it is even.

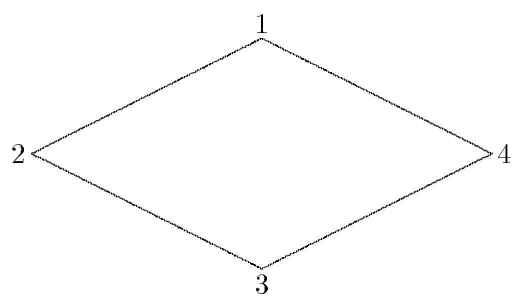
d) $\omega = (13)(324)(12) = (14)(23)$, so $|\omega| = \text{lcm}(2,2) = 2$. $\omega^{-1} = (32)(41)$. Finally, $\omega = (14)(23)$, so it is even.

4. Let $\alpha = (1,2,3)(4,5)$ and let $\beta = (1,2,5)$.

a) $\alpha\beta = (13)(245)$ and $\beta\alpha = (154)(23)$.

b) $|\alpha\beta| = \text{lcm}(2,3) = 6$. $|\beta\alpha| = \text{lcm}(3,2) = 6$.

5. Label the vertices of a rhombus 1, 2, 3, and 4. Write each motion of the rhombus as an element of S_4.



Solution: $r_0 = (1)$, $r_{180} = (13)(24)$, $v = (24)$, and $h = (13)$.

6. Use the table for A_4 on page 101 to:

a) $C(A_4) = \{\alpha_1 = (1)\}$.

b) $C((123)) = \{(1), (123), (132)\}$.

c) Extra Credit: Let G be any group and $x \in G$. The **centralizer** of x is $C(x) = \{a \in G \mid ax = xa\}$. Prove that $C(x)$ is a subgroup of G. **Solution:** Closure: Let $a, b \in C(x)$. Show $ab \in C(x)$. But

$$abx = a(bx) = a(xb) = (ax)b = (xa)b = xab.$$

Inverses: Let $a \in C(x)$. Then

$$ex = xe \Rightarrow (a^{-1}a)x = x(a^{-1}a) \Rightarrow (a^{-1}(ax) = x(a^{-1}a)$$
$$\Rightarrow (a^{-1}(xa) = x(a^{-1}a) \Rightarrow (a^{-1}x)a = (xa^{-1}a \Rightarrow a^{-1}x = xa^{-1}.$$

7. **a)** Let $\alpha = (a_1 a_2 \ldots a_k)$ be a k-cycle. Prove that α is odd if and only if k is even. **Solution:** We saw in class that $\alpha = (a_1 a_k) \ldots (a_1 a_3)(a_2 a_1)$ is a product of $k-1$ transpositions. Therefore, α is odd if and only if $k-1$ is odd if and only if k is even.

b) Prove that α is odd if and only if $|\alpha|$ is even. **Solution:** As seen in class, the order of a k-cycle is just its length. So $|\alpha|$ is even if and only if k is even and from the previous part k is even if and only if α is odd.

c) OK, here's the hard part on the homework: Now let β be any element of S_n. Prove that if β is odd, then $|\beta|$ is even. Hint: First use Theorem 5.1. Then show at least one of the cycles must be even in length. Then use Ruffini's Theorem. **Solution:** We can write β as a product of n disjoint cycles, say $\beta = \alpha_1 \alpha_2 \cdots \alpha_n$. Let k_i be the length of α_i. First use a proof by contradiction to show that some k_i is even in length. Assume not. Then by part (a), all the k_i are odd, so all the α_i are even. So $\beta \in A_n$ and therefore β is even. This contradicts that we are given that β is odd. So some k_i must be even. But then by Ruffini's Theorem,

$$|b| = \operatorname{lcm}(k_1 k_2 \cdots k_n)$$

must be even since $k_i \mid \operatorname{lcm}(k_1 k_2 \cdots k_n)$ and k_i is even.

Optional Mastery and Review Exercises

8. Let G be a group and let H be a subgroup of G. Let a be some *fixed* element of G. Define the set aHa^{-1} to be $\{aha^{-1} \mid h \in H\}$. Show that aHa^{-1} is a subgroup of G. **Solution:** Closure: Let $ah_1a^{-1}, ah_2a^{-1} \in aHa^{-1}$. Then $h_1, h_2 \in H$. So

$$(ah_1a^{-1})(ah_2a^{-1}) = a(h_1h_2)a^{-1} \in aHa^{-1}.$$

because H is a subgroup so $h_h h - 2 \in H$. Inverses: Let $aha^{-1} \in aHa^{-1}$. Must show $(aha^{-1})^{-1} \in aHa^{-1}$. But $h^{-1} \in H$. So

$$(aha^{-1})^{-1} = ah^{-1}a^{-1} \in aHa^{-1}.$$

9. Suppose G is a group of order 16. If G has 5 elements for which $x^4 = e$, can G be cyclic? Explain. **Solution:** If G were cyclic of order 16, the elements whose order were were 4, 2 and 1 would satisfy this condition. Now if $< y >= G$, then these elements would be y^4, y^{12}, y^8, and e. So it is impossible.

10. Let P be the set of polynomials in x. Define $\phi : P \to P$ by $\phi(f) = f'$, where f' denotes the derivative of f. Why is ϕ not one-to-one? However, ϕ is onto. Can you prove this? **Solution:** Note that $\phi(x) = \phi(x+1) = 1$. So ϕ is not injective. It is onto. Let $f \in P$. Let $F = \int f\,dx$. Then F is a polynomial and $F' = f$ by the Fundamental Theorem of Calculus.

11. Let $\phi : X \to Y$ be a mapping. For $a, b \in X$, define $a \sim b$ to mean that $\phi(a) = \phi(b)$. Is $\sim$ an equivalence relation on X? **:** **Solution:** Reflexive: For any $a \in X$, we have $\phi(a) = \phi(a)$, so $a \sim a$. Symmetric: Given $a \sim b$. Show $\sim a$. But

$$a \sim b \iff \phi(a) = \phi(b) \iff \phi(b) = \phi(a) \iff b \sim a.$$

Transitive: Given $a \sim b$ and $b \sim c$. Show $a \sim c$. But $a \sim b \Rightarrow \phi(a) = \phi(b)$ and $b \sim c \Rightarrow \phi(b) = \phi(c)$. Therefore, $\phi(a) = \phi(c)$, so $\alpha \sim c$. Note that we have used the reflexive, symmetric, and transitive properties of equality in succesive steps.

12. Let G be a group of order p, where p is a prime.

a) Suppose that $x \in G$ and $|x| = p$. Prove that G is cyclic. **Solution:** Consider the set $\{e = x^0, x, x^2, \ldots, x^{p-1}\}$. If these p elements are distinct, then $< x >= G$ because G has order p and by closure $< x > \subset G$. Assume they are not distinct. Then $x^j = x^k$ where $k \neq j$. WMA $0 \leq j < k \leq p-1$. Then $x^j = x^k \Rightarrow e = x^{k-j} \Rightarrow |x| < k - j \leq k \leq p-1$. This contradicts the fact that $|x| = p$. So the elements were distinct.

b) Prove even more: That G has exactly $p-1$ elements of order p. **Solution:** Just apply Sam's Theorem. If $1 \leq k \leq p-1$, then $|x^k| = \frac{p}{\gcd(p,k)} = p$ since p is prime. So every non-identity element of G generates the group.