Math 103A: Homework 6 solutions

1. Solution to Problem 1
We need to show that $\phi : S_A \to S_B$ is a bijection and it satisfies the homomorphism property.
ϕ is well defined. $f : A \to B$ is a bijection, so $f^{-1} : B \to A$ is a bijection. Also, given $\sigma \in S_A$, $\sigma : A \to A$ is a bijection by definition. Since composition of bijections is a bijection, $\phi(\sigma) = f \circ \sigma \circ f^{-1} : B \to A \to A \to B$ is a bijection. Hence $\phi(\sigma) \in S_B$.
ϕ is surjective. Given $\gamma \in S_B$, let $\sigma = f^{-1} \circ \gamma \circ f$. By similar arguments as above, we see that $\sigma \in S_A$. But $\phi(\sigma) = f \circ \sigma \circ f^{-1} = f \circ f^{-1} \circ \gamma \circ f \circ f^{-1} = \gamma$.
ϕ is injective. $\phi(\sigma) = \phi(\gamma) \implies f \circ \sigma \circ f^{-1} = f \circ \gamma \circ f^{-1} \implies f^{-1} \circ f \circ \sigma \circ f^{-1} \circ f = f^{-1} \circ f \circ \gamma \circ f^{-1} \circ f \implies \sigma = \gamma$.
ϕ satisfies the homomorphism property. $\phi(\sigma_1) \circ \phi(\sigma_2) = f \circ \sigma_1 \circ f^{-1} \circ f \circ \sigma_2 \circ f^{-1} = f \circ \sigma_1 \sigma_2 \circ f^{-1} = \phi(\sigma_1 \sigma_2)$.

2. Solution to Problem 2
(a) We know matrix multiplication is associative, and G_n contains the identity. So we need only show that G_n is closed under multiplication and it contains all the inverses. G_n contains two types of elements, R^i and $R^i X$ for $0 \le i \le n-1$. Note that $X^2 = I$, $R^n = I$ (as rotating a vector n times by $\frac{2\pi}{n}$ radians maps a vector to itself), and $RXR = X$ (by explicit computation, for example). The last identity gives $XR = R^{-1}X$. Given this, we have: $R^a R^b = R^{(a+b) \mod n}$, $R^a(R^b X) = R^{(a+b) \mod n} X$, $(R^a X)R^b = R^a(XR^b) = R^a(R^{-b}X) = R^{(a-b) \mod n} X$ and $(R^a X)(R^b X) = (R^a X)(XR^{-b}) = R^a R^{-b} = R^{(a-b) \mod n}$. This covers all the four cases, and G_n is closed under multiplication.
For inverses, we use the above computations to see that the inverse of R^i for $1 \le i \le n-1$ is R^{n-i} and the inverse of everything else is itself.
(b) We give an explicit bijection $f : D_4 \to G_4$, and verify that it satisfies the homomorphism property. First note that D_4 is generated by ρ_1 = (1 2 3 4) and μ_1 = (1 2)(3 4) as given on Pg. 80 in the book. The eight elements are in fact $\{\rho_0 = {\rho_1}^0 = id, \rho_1, \rho_2 = {\rho_1}^2, \rho_3 = {\rho_1}^3, \mu_1, \mu_2 = {\rho_1}^3\mu_1, \delta_1 = \rho_1\mu_1, \delta_2 = {\rho_1}^2\mu_1\}$. Also note that ${\rho_1}^4 = {\mu_1}^2 = id$, and $\rho_1\mu_1\rho_1$ = (1 2)(3 4) = μ_1. This implies $\mu_1\rho_1 = {\rho_1}^{-1}\mu_1$ and ${\mu_1}^a{\rho_1}^b = {\rho_1}^{(-1)^a b}{\mu_1}^a$.
Also, since $RXR = X$ and $R^4 = X^2 = I$, the above computations work analogously in G_4 as well and we get $X^a R^b = R^{(-1)^a b} X^a$.
Now we define $f : D_4 \to G_4$ as $f(\rho^a \mu^b) = R^a X^b$. It is clearly onto, and as $|G_4| = |D_4|$, f is a bijection. To see that it satisfies the homomorphism property:
$f((\rho^a\mu^b)(\rho^c\mu^d)) = f(\rho^a(\mu^b\rho^c)\mu^d) = f(\rho^a(\rho^{(-1)^b c}\mu^b)\mu^d) = f(\rho^{(a+(-1)^b c)}\mu^{(b+d)}) = R^{(a+(-1)^b c)}X^{(b+d)}$.
$f(\rho^a\mu^b)f(\rho^c\mu^d) = (R^a X^b)(R^c X^d) = R^a(X^b R^c)X^d = R^a R^{(-1)^b c} X^b X^d = R^{(a+(-1)^b c)}X^{(b+d)}$.
Hence, f is an isomorphism.

3. Solution to II.8 Q2
   $\tau^2\sigma = \begin{pmatrix} 1&2&3&4&5&6 \\ 2&4&1&5&6&3 \end{pmatrix}$

4. Solution to II.8 Q8
   Since σ is a cycle of length 6, $\sigma^6 = id$. So, $\sigma^{100} = (\sigma^6)^{16}\sigma^4 = \sigma^4 = \begin{pmatrix} 1&2&3&4&5&6 \\ 6&5&2&1&3&4 \end{pmatrix}$

5. Solution to II.8 Q12
   The orbit of 1 under τ is $\{1,2,3,4\}$ (since $1 \to 2 \to 4 \to 3 \to 1$).

6. Solution to II.8 Q21
   (a) We know that matrix multiplication is associative and the identity matrix is among the 6 matrices. So we only need to show that the set is closed under multiplication and has all the inverses.
   Let $A_1, A_2, \cdots A_6$ be the given matrices. Note that $A_1\cdot$ [1 2 3] $^\intercal$ = [1 2 3]$^\intercal$, $A_2\cdot$ [1 2 3] $^\intercal$ = [2 3 1]$^\intercal$, $A_3\cdot$ [1 2 3] $^\intercal$ = [3 1 2]$^\intercal$ etc, and we get 6 different permutations of the vector [1 2 3]$^\intercal$ when multiplied by the six matrices. So, when we multiply A_i and A_j, A_i permutes the three columns of A_j and the resulting matrix has exactly one 1 in each column and each row. So the set is closed under multiplication.
   For inverses, note that for any A_i, it's transpose ${A_i}^\intercal$ is clearly in the set, as the property of having exactly one 1 in each column and row is preserved. But $A_i \cdot {A_i}^\intercal = I$. So it contains all the inverses, and hence is a group.
   (b) By the first half of part *(a)*, we see that the group is isomorphic to S_3.

7. Solution to II.8 Q47
   Let σ be a non-identity permutation in $S_{n\geq 3}$. We need to prove that there exists γ in S_n such that $\sigma\gamma \neq \gamma\sigma$. Since σ is not the identity, there exists $1 \leq i \leq n$ such that $\sigma(i) = j$ and $i \neq j$. Let γ be the permutation $(i\ k)$ where $k \neq i \neq j$ (here we need $n \geq 3$ to get the three distinct elements). Then $(\sigma\gamma)(i) = \sigma(k) \neq j$ (as $\sigma(i) = j$ and permutation is a bijection). But $(\gamma\sigma)(i) = \gamma(j) = j$. So $(\sigma\gamma)(i) \neq (\gamma\sigma)(i)$, and that implies $\sigma\gamma \neq \gamma\sigma$.

8. Solution to II.8 Q49
   Let $A = \{a_1, a_2, \cdots, a_n\}$. Let $\sigma \in S_A$ be the permutation $(a_1, a_2, \cdots, a_n)$ (written in cyclic notation). Then $<\sigma>$, the subgroup generated by σ, clearly has size $|A|$, and is transitive. In fact, given $a_i, a_j \in A$ with $i < j$, $\sigma^{j-i}(a_i) = a_j$, and its inverse would take a_j to a_i.

9. Solution to II.9 Q2
   The orbits of the permutation are $\{1,5,7,8\}$, $\{2,3,6\}$ and $\{4\}$.

10. Solution to II.9 Q9
    $(1,2)(4,7,8)(2,1)(7,2,8,1,5) = (1,5,8)(2,4,7)$. Here, the four cycles in the left hand side are four different permutations, but two cycles on the right hand side is just one permutation written in the cyclic notation.

11. Solution to II.9 Q13
    (a) The order of the cycle $(1, 4, 5, 7)$ is 4.
    (b) Part *(a)* suggests that the order of a cycle of length n is n.
    (c) The order of $(4, 5)(2, 3, 7)$ is 6, and the order of $(1, 5)(3, 5, 7, 8)$ is 4.
    (d) The orders of the permutations in Exercise 10,11 and 12 are 6,6 and 8 respectively.
    (e) The order of a permutation is the least common multiple of the lengths of its disjoint cycles.

12. Solution to II.9 34
    Let $\sigma = (a_1, a_2, \cdots, a_n)$ where n is odd. Then $\sigma^2 = (a_1, a_2, \cdots, a_n)(a_1, a_2, \cdots, a_n) = (a_1, a_3, \cdots, a_n, a_2, a_4, \cdots a_{n-1}$, which is a cycle of length n.