THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2078 Honours Algebraic Structures 2023-24
Homework 2 Solutions
1st February 2024

- If you have any questions, please contact Eddie Lam via echlam@math.cuhk.edu.hk or in person during office hours.

Compulsory Part

1. Let $\omega = e^{\pi i/12} \in \mathbb{C}$, consider $\omega^k = e^{k\pi i/12}$. $\operatorname{ord}(\omega^k)$ is the smallest positive integer n such that $(\omega^k)^n = \omega^{kn} = 1$. Now $e^{kn\pi i/12} = 1$ implies that $kn/12$ is a multiple of 2, so that kn is a multiple of 24. The smallest positive integer n is achieved when this multiple is also smallest. In other words, $kn = \text{lcm}(24, k)$.

   For example, when $k = 8$, $\text{lcm}(24, 8) = 24$ and so $n = 3$. When $k = 13$, we have $n = 13 \times 24/13 = 24$. When $k = 22$, we have $n = 11 \times 24/22 = 12$. When $k = 2078 = 24 \times 86 + 14$ so $\text{lcm}(2078, 24) = 2078 \times 24/2$, therefore $n = 2078 \times 12/2078 = 12$.

2. (a) $A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ is an element of $SL(2, \mathbb{R})$ since its determinant is $(-1)^2 = 1$. It is clearly of order 2.

   (b) Consider the matrix $B = \begin{pmatrix} \cos(2\pi/3) & -\sin(2\pi/3) \\ \sin(2\pi/3) & \cos(2\pi/3) \end{pmatrix} = \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix}$. This matrix clearly has determinant 1 since $\sin^2 x + \cos^2 x = 1$ for any x. We claim that this matrix has order 3. This can be verified directly

   $$B^3 = \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix}^3 = \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix} \begin{pmatrix} -1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

   (Alternatively, one can show that the matrix is diagonlizable over $\mathbb{C}$ with eigenvalues $\omega_1 = e^{2\pi i/3}$ and $\omega_2 = e^{4\pi i/3}$. Therefore it is diagonalizable, i.e. there exists some invertible P such that $B = P \begin{pmatrix} \omega_1 & 0 \\ 0 & \omega_2 \end{pmatrix} P^{-1}$. So we have $B^3 = P \begin{pmatrix} \omega_1^3 & 0 \\ 0 & \omega_2^3 \end{pmatrix} P^{-1} = PP^{-1} = I$. Here we have used $\omega_1^3 = \omega_2^3 = 1$.)

   (c) $C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has determinant 1, so it is an element of $SL(2, \mathbb{R})$. It has infinite order, since for any $n \in \mathbb{Z}_{>0}$, we have

   $$C^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

   This can be shown by an induction argument, as

   $$C^{n+1} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}.$$

   So $C^n \neq I$ for any $n > 0$. It has infinite order.

3. Suppose that $a, b \in G$ so that $|ab|$ is finite, say $|ab| = n$, notice that $(ba)^{n+1} = \underbrace{(ba)(ba)...(ba)}_{n+1 \text{ times}} = b\underbrace{(ab)(ab)...(ab)}_{n \text{ times}}a = bea = ba$. Therefore by multiplying $(ba)^{-1}$ to both sides, we obtain $(ba)^n = e$. Now we claim that $(ba)^k$ cannot be the identity for $0 < k < n$. Otherwise by the same argument (swapping b and a), this would imply that $(ab)^k = e$ for $0 < k < n$, which contradicts with the definition of $n = |ab|$. So n is equal to the order of ba as well.

4. Let μ_1, μ_2 be disjoint cycles, let $|\mu_1| = n_1$ and $|\mu_2| = n_2$, then since disjoint cycles commute, we have $(\mu_1\mu_2)^{\text{lcm}(n_1,n_2)} = \mu_1^{\text{lcm}(n_1,n_2)} \cdot \mu_2^{\text{lcm}(n_1,n_2)}$. Now lcm$(n_1, n_2)$ is a multiple of both n_1, n_2, and so when μ_1 and μ_2 are raised to that power, we get e. Therefore, we have $(\mu_1\mu_2)^{\text{lcm}(n_1,n_2)} = e$.

   Conversely, if $(\mu_1\mu_2)^k = \mu_1^k\mu_2^k = e$ for some k, then we must have $\mu_1^k = \mu_2^k = e$. This is because μ_1^k and μ_2^k are always comprised of disjoint cycles, so they are inverse to each other if and only if they are both trivial. This implies that $n_1|k$ and $n_2|k$, so lcm$(n_1, n_2)|k$. Thus lcm(n_1, n_2) is the minimal power of $\mu_1\mu_2$ that multiplies to e, i.e. it is the order of $\mu_1\mu_2$.

   For the general case, suppose that we have shown that for any r many disjoint cycles $\mu_1, ..., \mu_r$, we have $|\mu_1\mu_2...\mu_r| = \text{lcm}(k_1, ..., k_r)$ for $k_i = |\mu_i|$. Given $r + 1$ many disjoint cycles now, consider the first r cycles, we have $d := |\mu_1...\mu_r| = \text{lcm}(k_1, ..., k_r)$ by the induction hypothesis. Write $\sigma = \mu_1...\mu_r$, we have $(\sigma\mu_{r+1})^{\text{lcm}(d,k_{r+1})} = e$ as before, since d is the order of σ and k_{r+1} is the order of μ_{r+1}.

   Conversely, if $(\sigma\mu_{r+1})^l = e$, then again by the fact that σ and μ_{r+1} are comprised of disjoint cycles, this implies that $\sigma^l = \mu_{r+1}^l = e$. So that $d|l$ and $k_{r+1}|l$ and so lcm$(d, k_{r+1})|l$. Hence, lcm(d, k_{r+1}) is the smallest positive power of $\mu_1...\mu_{r+1}$ that multiplies to the identity, and we are done since lcm$(d, k_{r+1}) = \text{lcm}(k_1, ..., k_{r+1})$.

5. Let r be the rotation of the plane by $2\pi/6$, and s be any reflection in D_6. Then we have $D_6 = \{e, r, r^2, r^3, r^4, r^5, s, sr, sr^2, sr^3, sr^4, sr^5\}$. Any sr^i is a reflection and so has order equals to 2. Meanwhile a rotation has order 2 precisely when it is rotation by π, i.e. the rotation r^3. So there are 7 elements of order 2.

6. Note that $e^{-1} = e$. If it was the case that g has no order 2 element, then $g \neq g^{-1}$ for all $g \neq e$. And so G can be partitioned into subsets $\{e\}, \{g_1, g_1^{-1}\}, \{g_2, g_2^{-1}\}, ...$. But this would imply that G has odd order, this is a contradiction. So there must be some order 2 element.

Optional Part

1. We have $ab = eab = a^6b = a^3(a^3b) = a^3ba^3 = ba^6 = bae = ba$.

2. (a) The group operation given by matrix multiplication on $O(2, \mathbb{R})$ is associative since it inherits from that of $GL(2, \mathbb{R})$. The identity element is the identity matrix I, which is in $O(2, \mathbb{R})$ since $II^T = II = I$. It remains to show that $O(2, \mathbb{R})$ is closed under group operation and inversion, if $A, B \in O(2, \mathbb{R})$, then $(AB)^T(AB) = B^T(A^TA)B = B^TB = I$ and $(AB)(AB)^T = A(BB^T)A^T = AA^T = I$ so $AB \in O(2, \mathbb{R})$. And $AA^T = I$ implies that $I = I^{-1} = (AA^T)^{-1} = (A^T)^{-1}A^{-1}$, but $(A^{-1})^T = (A^T)^{-1}$ so this shows that $A^{-1} \in O(2, \mathbb{R})$.

(b) Take the matrix A described in compulsory Q2a, $A = -I$ is symmetric, so $AA^T = A^2 = I$, so that $A \in O(2, \mathbb{R})$ and has order 2.

(c) We have seen that matrix B described in compulsory Q2b is a matrix of order 3, from the calculation, notice that B^2 is in fact B^T. So that $B^3 = B^2 B = B^T B = I$, thus $B \in O(2, \mathbb{R})$.

3. (a) (1325) is a 4-cycle, so it has order 4.

   (b) By compulsory Q4 above, this element has order $\text{lcm}(4, 2) = 4$.

   (c) The order is $\text{lcm}(4, 3) = 12$.

   (d) $(32)(46)(37)(35) = (46)(32)(573) = (46)(3572)$ is a product of disjoint cycles of lengths 2 and 4, so it has order $\text{lcm}(4, 2) = 4$.

4. (a) i. $\sigma = (1264)(2513) = (14)(16)(12)(23)(21)(25)$ (in general a k-cycle can be written as product of transition as follows: $(i_1 i_2 \cdots i_k) = (i_1 i_k)(i_1 i_{k-1}) \cdots (i_1 i_2)$). As for τ, it is easier to write it as product of disjoint cycles first, by chasing through elements (e.g. 1 is mapped to 4, 4 is mapped to 5, 5 maps back to 1, so there is a cycle (145) in τ.) Here $\tau = (145)(376)$. Then we may break it into transposition like previously, $\tau = (15)(14)(36)(37)$.

   ii. From the above, note that $(12)(23)(12) = (13)$, so we have $\sigma = (14)(16)(13)(25) = (1364)(25)$.
   $\tau = (145)(376)$ is computed in part (i).

   (b) σ and τ are both $(3, 3)$-cycles, so they both have order equals to $\text{lcm}(3, 3) = 3$. As for $\sigma\tau = (164)(253)(145)(376) = (256)(374)$ is also a $(3, 3)$-cycles, so it also has order 3.

5. (a) By compulsory Q4, an element of S_5 has order 3 precisely when it is a 3-cycle (also see Q3 of tutorial 2). Then by Q1c of tutorial 2, there are $P_3^5/3 = 20$ many 3-cycles.

   (b) An element of order 4 in S_6 can either be a 4-cycle of a disjoint product of 4-cycle and 2-cycle (i.e. a $(4, 2)$-cycle). There are $P_4^6/4 = 90$ many 4-cycles, and note that 4-cycle is in bijection with $(4, 2)$-cycle, as fixing a 4-cycle leaves no choice for the remaining two numbers. So there are in total 180 elements of order 4.

   (c) Again there are $P_3^7/3 = 70$ many 3-cycles in S_7, which are precisely the elements of order 3. It is also possible to have $(3, 3)$-cycles in S_7, there are $\frac{1}{2} \times P_3^7/3 \times P_3^4/3 = 280$ many $(3, 3)$-cycles, since fixing a 3-cycle leaves $P_3^4/3$ choices to pick another 3-cycle out of the remaining 4 numbers, then the $\frac{1}{2}$ is to take out the double-counting from the symmetry of the first and the second 3-cycles (for example, $(123)(456)$ and $(456)(123)$ are the same permutation, but would be double-counted). Therefore there are 350 many order 3 elements in S_7.

6. (a) We will proceed to prove the statement by induction on k. The case when $k = 1$ is tautological. Now suppose the statement has been proven for some k. Then

$$(srs)^k = (srs)^k(srs) = sr^k ssrs = sr^k rs = sr^{k+1}s.$$

   Therefore the statement holds for all $k \in \mathbb{Z}_{>0}$.

(b) One simple argument is to note that sr is again a reflection, and thus has order 2. So $srsr = e$, multiplying r^{-1} to the right on both sides yields $srs = r^{-1}$. In particular, this holds for all reflection s and rotation r.

Thus, it suffices to prove that sr is indeed a reflection. This follows from the intuitive fact that composition of two rotations is again a rotation. (If one wants to prove this rigorously, one may try to represent a rotation by a linear transformation, or as multiplication by a unit complex number by identifying $\mathbb{C} \cong \mathbb{R}^2$.) If sr was a rotation, then $sr = r'$ and so $s = r'r^{-1}$, would imply that s is a rotation.