THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2070A Algebraic Structures 2019-20
Tutorial 2
Date: 16th September 2019

Problems:

1. Find the order of $(1+i)/\sqrt{2}$ and $1+i$ respectively as elements in the multiplicative group $\mathbb{C}^\times$ of the complex number.

Solution. Note that $\left[(1+i)/\sqrt{2}\right]^2 = i$, so the order of $(1+i)/\sqrt{2}$ is 8. Or by employing the polar form, one gets $(1+i)/\sqrt{2} = cis\frac{\pi}{4}$, so the order of $(1+i)/\sqrt{2}$ is 8.

The modulus of $1+i$ is $\sqrt{2}$ which suggests that the order of $1+i$ is ∞.

◀

2. Let G be a group and $e \neq a \in G$ where e is the identity of G. Suppose $|a| = n$.

   (a) If $a^h = e$, then show that $n|h$.

   (b) Show that for any positive integer m, $|a^m| = n/(m,n)$ where (m,n) is the gcd of m and n. [Hint: You may find the following facts useful: $(\frac{a}{(a,b)}, \frac{b}{(a,b)}) = 1$ and if $a|bc$ and $(a,b) = 1$, then $a|c$.]

Solution. (a) By Division Algorithm, $h = qn + r$ for some $q \in \mathbb{Z}$ and $0 \leq r < n$. Then $a^r = a^h(a^n)^{-q} = e$.

Claim: r must be 0.
Proof: Assume not, i.e. $r \geq 1$ (and $r < n$). Then $a^r = e$ where $1 \leq r < n$, contradicting to $n = |a|$ which is, by definition, the smallest positive integer ℓ for which $a^\ell = e$.

Hence $h = qn$, so $n|h$.

(b) $|a^m| = \dfrac{n}{(n,m)}$. To justify it, we need to show the following two assertions.

1° $(a^m)^{\frac{n}{(n,m)}} = e$.

This follows from

$$(a^m)^{\frac{n}{(n,m)}} = a^{\frac{mn}{(n,m)}} = (a^n)^{\frac{m}{(n,m)}} \overset{a^n=e}{=\!=\!=} e^{\frac{m}{(n,m)}} \overset{\frac{m}{(n,m)}\in\mathbb{Z}}{=\!=\!=} e$$

2° If $k \in \mathbb{N}$ such that $(a^m)^k = e$, then $k \geq \frac{n}{(n,m)}$.

From $(a^m)^k = e$, Part (a) implies $n \big| mk$, so by the second part of hint $\dfrac{n}{(n,m)} \Big| k$ because $(\frac{n}{(n,m)}, \frac{m}{(n,m)}) = 1$.
Hence $\frac{n}{(n,m)}$ is the smallest positive integer ℓ such that $(a^m)^\ell = e$, i.e. $|a^m| = \dfrac{n}{(n,m)}$.

◀

3. True or false: If σ is a cycle, then σ^2 must be a cycle.

Solution. False. Consider $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix} \in S_5$. Then $\sigma^2 = \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix}$.

◀

4. Show that S_n is a nonabelian group for $n \geq 3$.

Solution.

$$\begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 \end{pmatrix} \neq \begin{pmatrix} 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$$

◀

5. Draw the group table for $D_4 = \{e, r, r^2, r^3, s, rs, r^2s, r^3s\}$. [Hint: Use Question 6 of Optional part in HW2.]

Solution.

$\cdot$	e	r	r^2	r^3	s	rs	r^2s	r^3s
e	e	r	r^2	r^3	s	rs	r^2s	r^3s
r	r	r^2	r^3	e	rs	r^2s	r^3s	s
r^2	r^2	r^3	e	r	r^2s	r^3s	s	rs
r^3	r^3	e	r	r^2	r^3s	s	rs	r^2s
s	s	r^3s	r^2s	rs	e	r^3	r^2	r
rs	rs	s	r^3s	r^2s	r	e	r^3	r^2
r^2s	r^2s	rs	s	r^3s	r^2	r	e	r^3
r^3s	r^3s	r^2s	rs	s	r^3	r^2	r	e

◀

6. Show that if $n \geq 3$, then the only element of $\sigma \in S_n$ satisfying $\sigma\tau = \tau\sigma$ for all $\tau \in S_n$ is the identity element.

Solution. Assume that there exists such a non-identity element $\sigma \in S_n$. So we can find two positive integers i and j such that $i \neq j$ and $\sigma(i) = j$. Now $n \geq 3$. We can have another integer k different from i and j. Consider $\gamma = \begin{pmatrix} i & k \end{pmatrix} \in S_n$. Then one has

$$\gamma\sigma(i) = j \neq \sigma(k) = \sigma\gamma(i)$$

as σ is bijective and $\sigma(i) = j$. A contradiction occurs as $\sigma\gamma \neq \gamma\sigma$.

◀

Optional Part

1. Let g and h be two elements of a group G. g and h are conjugate if $g = \alpha h \alpha^{-1}$ for some $\alpha \in G$. Let σ and τ be two elements in S_n. Show that σ and τ are conjugate if and only if they are of the same cycle pattern.

Solution. Only if part: Suppose σ and τ are conjugate. Then $\sigma = \alpha\tau\alpha^{-1}$ for some $\alpha \in S_n$. Note that any permutation in S_n can be written as a product of disjoint cycles. To argue that they are of the same cycle pattern, we need the following two facts:

$$\alpha \begin{pmatrix} a_1 & \cdots & a_k \end{pmatrix} \alpha^{-1} = \begin{pmatrix} \alpha(a_1) & \cdots & \alpha(a_k) \end{pmatrix},$$

and if $\begin{pmatrix} a_1 & \cdots & a_k \end{pmatrix}$ and $\begin{pmatrix} b_1 & \cdots & b_h \end{pmatrix}$ are disjoint, then $\begin{pmatrix} \alpha(a_1) & \cdots & \alpha(a_k) \end{pmatrix}$ and $\begin{pmatrix} \alpha(b_1) & \cdots & \alpha(b_h) \end{pmatrix}$ are also disjoint as α is bijective.

If part: Suppose σ and τ are of the same cycle pattern. WLOG, we can only consider $\sigma = \begin{pmatrix} a_1 & \cdots & a_k \end{pmatrix}$ and $\tau = \begin{pmatrix} b_1 & \cdots & b_k \end{pmatrix}$. We want to pick a correspondence α between $\begin{pmatrix} a_1 & \cdots & a_k \end{pmatrix}$ and $\begin{pmatrix} b_1 & \cdots & b_k \end{pmatrix}$. For any α satisfying $\alpha(b_i) = a_i$ for $i = 1, 2, \ldots, k$, we have $\begin{pmatrix} a_1 & \cdots & a_k \end{pmatrix} = \alpha \begin{pmatrix} b_1 & \cdots & b_k \end{pmatrix} \alpha^{-1}$.

◀