THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2078 Honours Algebraic Structures 2022-23
Tutorial 4 Solutions
5th February 2024

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

1. Denote $K = \bigcap_{S \subset H \leq G} H$, we will show that $\langle S \rangle = K$ by both inclusions $\subset$ and $\supset$.

   ($\subset$) Let $x = a_1^{m_1} \cdots a_n^{m_n} \in \langle S \rangle$ be an arbitrary element and let H be any subgroup of G containing S, then we have $a_1, ..., a_n \in S \subset H$, so by property of H being a subgroup, we have $x = a_1^{m_1} \cdots a_n^{m_n} \in H$ since x is obtained from multiplication and taking inverse on the a_i's. Thus $x \in H$ for every subgroup H containing S, i.e. $x \in \bigcap_{S \subset H \leq G} H$.

   ($\supset$) It suffices to prove that $\langle S \rangle$ is a subgroup containing S, then $\langle S \rangle \in \{H : S \subset H \leq G\}$ and thus $\langle S \rangle \supset \bigcap_{S \subset H \leq G} H$. Firstly, $\langle S \rangle$ contains S since for every $a \in S$, taking $n = 1$, $a_1 = a$ and $m_1 = 1$ yields $a \in \langle S \rangle$. Secondly, $\langle S \rangle$ is a subgroup, since for $x = a_1^{m_1} \cdots a_n^{m_n}$ and $y = b_1^{k_1} \cdots b_l^{k_l}$, we have $xy^{-1} = a_1^{m_1} \cdots a_n^{m_n} b_l^{-k_l} \cdots b_1^{-k_1}$, with $m_1, ..., m_n, -k_l, ..., -k_1 \in \mathbb{Z}$, so $xy^{-1} \in \langle S \rangle$.

   By "the smallest subgroup of G containing S", we are referring to the subgroup T of G with the properties that $S \subset T$, and whenever H is another subgroup containing S, then $T \leq H$.

   We will show that $T = K$, hence the remark that $\langle S \rangle$ is precisely the smallest subgroup of G containing S. First of all, since K contains the subset S, we have $T \leq K$ by definition of T. On the other hand, since T is a subgroup containing S, $T \in \{H : S \subset H \leq G\}$, and hence $T \geq \bigcap_{S \subset H \leq G} H = K$. Hence, we have $T = K$.

   Remark. Such construction for the smallest sub-structure containing a given set appears in many different contexts. The general phenomenon is, given an algebraic structure A (think of it as group, ring, field, algebras, etc), and any subset $S \subset A$, one can informally think of

   $\langle S \rangle :=$ The set of elements in A generated by taking algebraic operations on elements of S.

   When equipped with the algebraic operation, $\langle S \rangle$ forms a sub-structure (subgroup, subring, subfield, subalgebra, etc). Then one can prove that

   $$\langle S \rangle = \bigcap_{A' :\, S \subset A' \leq A} A' = \text{The smallest substructure of } A \text{ containing the subset } S.$$

   For a more familiar example, let V be a vector space, say over $\mathbb{R}$, and $S \subset V$ any subset. Then one can define

   $$\langle S \rangle = \text{Span}(S) := \left\{ \sum_{i=1}^{n} a_i v_i : \, v_i \in S, a_i \in \mathbb{R} \right\} \leq V.$$

   Then $\langle S \rangle$ is the vector subspace of V generated by subset S, which can be shown to be equal to $\bigcap_{S \subset W \leq V} W$ the intersection of all subspace containing S.

2. Recall that for any element $g \in G$, $\langle g \rangle$ is always cyclic, thus it suffices to find out what $|g|$ is. In our case, $\langle r^i \rangle \leq \langle r \rangle \cong \mathbb{Z}_n$ and thus $\langle r^i \rangle = \{e, r^i, r^{2i}, ..., r^{(k-1)i}\}$, where $k = n/\gcd(i, n)$. As for $s \in D_n$, $|s| = 2$ always holds, so $\langle s \rangle = \{e, s\}$.

3. We will show that $H_1 = S_4$. One way of showing this is that adjacent transpositions are sufficient to generate all transpositions. In our case, we may obtain $(13), (24)$ and (14) from the given from transpositions as follows: $(13) = (13)(12)(12) = (123)(12) = (12)(23)(12) \in H_1$; and $(24) = (24)(23)(23) = (234)(23) = (23)(34)(23) \in H_1$; and $(14) = (14)(12)(12) = (124)(12) = (12)(24)(12) \in H_1$. Once we have all transpositions, we can generate all k-cycles. In fact, the last statement works for all S_n, suppose $(x_1 x_2 \dots x_k) \in S_n$ is a k-cycle, then $(x_1 x_2 \dots x_n) = (x_1 x_k)(x_1 x_{k-1}) \dots (x_1 x_2)$ can be expressed as a product of transpositions. Since every element of S_4 is a product of disjoint cycles, this shows that $H_1 = S_4$.

   As for H_2, we have $(132) = (123)^2 \in H_2$, as well as $(132)(234) = (134) \in H_2$, and also $(123)(324) = (124) \in H_2$. Thus we have H_2 containing all the 3-cycles (there are 8 of them). Note that $|S_4|$ has 24 elements, and $|H_2| \geq 9$ since H_2 has 8 non-trivial elements along with the identity. Thus by Lagrange's theorem, $|H_2| = 12$ or 24. We know that H_2 is not the whole group S_4 since both (123) and (234) are even elements, so any element that is a product of these elements will again be even. In particular, any odd element, for example (12) will not be an element of H_2. Thus $|H_2| = 12$ and $[S_4 : H_2] = 2$, the only index 2 subgroup of S_4 is the alternating group A_4, so $H_2 = A_4$.

4. (a) Symmetry: If $a \sim b$, then there is some g so that $b = gag^{-1}$, then for $g^{-1} \in G$, we have $a = g^{-1}ag = g^{-1}a(g^{-1})^{-1}$.
   Reflexivity: $a \sim a$ holds since $eae^{-1} = a$.
   Transitivity: if $a \sim b$ and $b \sim c$, then there are $g, h \in G$ so that $b = gag^{-1}$ and $c = hbh^{-1}$, then for $hg \in G$, we have $c = hbh^{-1} = (hg)a(hg)^{-1}$, so that $a \sim c$.

   (b) i. $a = (12)$ is a 2-cycle, by tutorial 2 Q1, we know that conjugates of any 2-cycle are precisely all the 2-cycles (there are 6 such cycles, namely $(12), (13), (14), (23), (24)$ and (34).

   ii. For $a = r^2 \in D_6$, for another rotation $r^k \in D_6$, since $r^k r^2 r^{-k} = r^{k+2-k} = r^2$, we do not get new elements in the conjugacy class. And for reflections sr^k, note that $sr^k r^2 r^{-k} s = sr^2 s = r^{-2} = r^4$. Thus, the conjugacy class $C_a = \{r^4, r^2\}$.

   iii. The same calculation in part (ii) yields that the only elements in C_a for $a = r^3$ are r^3 and $r^{-3} = r^3$. So in this case, $C_a = \{r^3\}$.

   iv. For any $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, we have $(a, b)+(1, 2)+(-(a, b)) = (a+1-a, b+2-b) = (1, 2)$, so $C_a = \{(1, 2)\}$.

   v. If G is an abelian group, then $gag^{-1} = agg^{-1} = a$ for any $g \in G$, so the conjugacy class C_a is always a singleton consisting of a.

   (c) Let $b, c \in C_a$ be elements of the same conjugacy class, then we may write $b = gag^{-1}$ and $c = hah^{-1}$ for some $g, h \in G$. Then

$$\begin{aligned} b^k = e &\iff (gag^{-1})^k = ga^k g^{-1} = e \\ &\iff a^k = e \\ &\iff (hah^{-1}) = ha^k h^{-1} = e \\ &\iff c^k = e. \end{aligned}$$

In particular, if b has some finite order n, that means n is the minimal positive integer so that $b^n = e$, so n is also the order of c. And if b has infinite order, then $b^k \neq e$ for any positive k, so the same holds for c as well.

(d) Let $g, h \in C_G(a)$, then by assumption we have $gag^{-1} = hah^{-1} = a$. So $(gh)a(gh)^{-1} = g(hah^{-1})g^{-1} = gag^{-1} = a$, and we have $gh \in C_G(a)$ as well. Also multiplying g^{-1} on the left and g on the right to the equation $gag^{-1} = a$ gives $a = g^{-1}ag$, so that $g^{-1} \in C_G(a)$. So $C_G(a)$ is a subgroup.

(e) We define a function $f : \{\text{Left cosets of } C_G(a) \text{ in } G\} \to C_a$ as follows, if $gC_G(a)$ is a left coset, we map it to the element $gag^{-1} \in C_a$. We will show that this map is a well-defined bijection.

First, if g and h represents the same left cosets, i.e. $g_1C_G(a) = g_2C_G(a)$, then $g_1^{-1}g_2 \in C_G(a)$. So $g_1^{-1}g_2a(g_1^{-1}g_2)^{-1} = g_1^{-1}g_2ag_2^{-1}g_1 = a$. If we multiply g_1 to the equation on the left and g_1^{-1} on the right, we obtain $g_2ag_2^{-1} = gag^{-1}$. Thus $f(g_1C_G(a)) = f(g_2C_G(a))$, and the function is well-defined (i.e. it is independent of the choice of representatives g_1, g_2.) Next, the function f is injective. Since if $f(gC_G(a)) = f(hC_G(a))$, then $gag^{-1} = hah^{-1}$, so that $h^{-1}gag^{-1}h = a$, i.e. $h^{-1}g \in C_G(a)$. This means that $gC_G(a) = hC_G(a)$. Finally for surjectively, this is clear from definition since every element of C_a is of the form gag^{-1} for some $g \in G$, so it is the image $f(gC_G(a))$.

The bijection establishes the equality of the cardinality of sets, so that $[G : C_G(a)] = |C_a|$.