THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2078 Honours Algebraic Structures 2022-23
Tutorial 4 Problems
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. Let S be a subset of a group G, recall that $\langle S\rangle$ is defined to be the set of all possible finite products elements in S, i.e. $\langle S\rangle := \{a_1^{m_1}...a_n^{m_n} : n \in \mathbb{N}, a_i \in S, m_i \in \mathbb{Z}\}$. Prove that $\langle S\rangle = \bigcap_{S\subset H\leq G} H$, and also explain why the latter can be understood as "the smallest subgroup of G containing S".

2. Describe the subgroups $\langle r^i\rangle, \langle s\rangle$ in D_n.

3. Describe the subgroups $H_1 = \langle(12),(23),(34)\rangle$ and $H_2 = \langle(123),(234)\rangle$ in S_4

4. (a) Let G be a finite group, define a relation $\sim$ on G by declaring $a \sim b$ if there exists some $g \in G$ such that $b = gag^{-1}$. Prove that $\sim$ is an equivalence relation. The equivalence class C_a of an element $a \in G$ is called the conjugacy class of a.

   (b) Find out what C_a is for the following elements in their respective groups.

      i. $a = (12) \in S_4$.

      ii. $a = r^2 \in D_6$.

      iii. $a = r^3 \in D_6$.

      iv. $a = (1,2) \in \mathbb{Z}\times\mathbb{Z}$.

      v. What can you say about C_a for any $a \in G$ in the case where G is abelian?

   (c) Show that elements in the same conjugacy class has the same order.

   (d) Let $C_G(a) := \{g \in G : gag^{-1} = a\}$, prove that $C_G(a)$ is a subgroup. It is called the centralizer of a.

   (e) Prove that $|C_a| = [G : C_G(a)]$, thus $|C_a|$ divides $|G|$. (Hint: find a bijection between C_a and the set of left cosets of $C_G(a)$.)

The following questions and materials are extra contents and will not be examined.

5. Let S be a set, define the $A(S) = \{a_1^{m_1}...a_n^{m_n} : n \in \mathbb{N}, a_i \in S, m_i \in \mathbb{Z}\} \cup \{e\}$, here we think of $A(S)$ as the set of "words" and e as the "empty word". We may define an equivalence relation $\sim$ on $A(S)$ as follows. If a^k and a^{-k} appear in a word next to each other, we may reduce the word by cancelling the two terms. More generally, if a^m and a^n appear next to each other in a word, we identify it with the word where $a^m a^n$ is replaced by a^{m+n}. If the resulting word is empty, we identify it with e. For example, under the equivalence relation, $abcc^{-1}ba \sim abba \sim ab^2a$, and $aa^{-1} \sim e$.

   Consider $F(S) := A(S)/\sim$ the set of equivalence classes in $A(S)$. We may define an operation $*$ on $F(S)$ by concatenation of words, i.e. we put two words next to each other and consider its class. For example, $abc * c^{-1}ba := abcc^{-1}ba \sim ab^2a$.

   Prove that $F(S)$ is a group under the operation $*$. This is called the *free group with generator S*.

6. Previously, we have defined $\langle S \rangle$ internally for a subset S in a group G. Now, we will define a group from generators that are subject to some relations, similar to the process above. Note that in the case for the free group $F(S)$, we impose no relations (under $\sim$) for the elements in S, except the reduction rule that are required to turn $F(S)$ a group.

   More generally, let S be a set, and let R be a set of words in S, we define an equivalence relation $\sim_R$ on $A(S)$ by the relation described in Q5, with the additional relation that the words in R are related to the empty word e (i.e. it can be deleted). For example, suppose $S = \{a, b\}$ and $R = \{aba^{-1}\}$, then we have $b^2a^2ba \sim_R b^2a(aba^{-1})a^2 \sim_R b^2aa^2 \sim_R b^2a^3$.

   We define the set $\langle S \,|\, R \rangle = A(S)/\sim_R$ to be the set of equivalent classes, and define the group operation by concatenation similar to that of Q5. This group is called the group generated by S subject to relation R.

   This definition took a lot of work and may seem complicated. So, it is instructive to look at some examples from familiar groups. Convince yourselves that the following identifications make sense.

   (a) $F(S) = \langle S \,|\, \emptyset \rangle$.

   (b) $\mathbb{Z} = F(\{a\}) = \langle a \,|\, \emptyset \rangle$

   (c) $\mathbb{Z}_n = \langle a \,|\, a^n \rangle$

   (d) $\mathbb{Z} \times \mathbb{Z} = \langle a, b |\, aba^{-1}b^{-1} \rangle$

   (e) $D_n = \langle r, s \,|\, r^n, s^2, rsrs \rangle = \langle s_1, s_2 \,|\, s_1^2, s_2^2, (s_1s_2)^n \rangle$

   (f) $S_n = \langle s_1, s_2, ..., s_{n-1} \,|\, s_i^2, (s_is_{i+1})^3, (s_is_j)^2 \text{ for } i \neq j \rangle$

7. Can you figure out why every group can be obtained from the construction of Q6?