THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2078 Honours Algebraic Structures 2023-24
Homework 4 Solutions
22nd 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. (a) Let $H = \langle 4 \rangle = \{4k : k \in \mathbb{Z}\} \leq \mathbb{Z}$, then for any $n \in \mathbb{Z}$, consider the left coset $n+H = \{n+4k : k \in \mathbb{Z}\}$, here we use the notation $n+H$ instead of the commonly written form nH to stress that we are considering addition as the group operation. Then $n + H = m + H$ if and only if $n - m = 4k$ for some $k \in \mathbb{Z}$. Thus the left coset nH only depends on the value of n mod 4. So there are 4 left cosets: $H, 1 + H, 2 + H, 3 + H$, they exactly correspond to the set of integers in $\mathbb{Z}$ whose remainder is $n = 0, 1, 2, 3$ respectively when divided by 4.

   (b) Again let $H = \langle 4 \rangle = \{0, 4, 8\} \leq \mathbb{Z}_{12}$ and consider $n + H$ for $n \in \mathbb{Z}_{12}$. Then the above discussion also holds in this case, meaning that the left cosets of H in $\mathbb{Z}_{12}$ are exactly the set of integers in $\mathbb{Z}_{12}$ whose remainders are $n = 0, 1, 2, 3$. So we have $H, 1 + H = \{1, 5, 9\}, 2 + H = \{2, 6, 10\}$ and $3 + H = \{3, 7, 11\}$.

   (c) Let s be a reflection, $H = \langle s \rangle = \{e, s\} \leq D_n$, for each reflection r^k where $k = 0, 1, ..., k-1$, we have the cosets $r^k H = \{r, r^k s\}$. For $r^j \neq r^k$, we have $r^j H \neq r^k H$. This is due to $r^j r^{-k} = r^{j-k} \in \{e, s\}$ precisely when $r^{j-k} = e$, so that $j = k$. Since $|H| = 2$ and $|D_n| = 2n$, by Lagrange's theorem, $[D_n : H] = 2n/2 = n$, so we have described all the left cosets.

2. A 4-cycle in S_4 will generate a cyclic subgroup of order 4. For example, we may take $\sigma = (1234)$, and $H = \langle \sigma \rangle = \{e, (1234), (13)(24), (1432)\}$. Note that $|H| = 4$ and $|S_4| = 24$, so there are 6 left cosets of H in S_4.

   Clearly e represents the trivial coset H.

   We may continue by taking an element outside H, say (12) and look at the coset represented by (12): $(12)H = \{(12), (234), (2413), (143)\}$.

   Again, we can continue by picking an element outside H and $(12)H$, say (23), and consider $(23)H = \{(23), (341), (2431), (214)\}$.

   Next, we take (13), we have $(13)H = \{(13), (12)(34), (24), (14)(23)\}$.

   Next we pick (14), we have $(14)H = \{(14), (123), (1342), (432)\}$.

   Note that (34) is not in any of the above cosets. So we may pick (34) and consider $(34)H = \{(34), (312), (1423), (132)\}$.

   Since we have written down 6 different cosets, they must be all the cosets of H in S_4.

3. By Lagrange's theorem, every proper subgroups of G has order dividing $|G| = pq$, so they have orders either 1 or p or q. If the subgroup has order 1, it is the trivial group, which is cyclic. Otherwise, the subgroup has order p or q, which are assumed to be prime. Recall that a group of prime order is always cyclic. This finishes the the proof.

4. See the solution to Tutorial 5 Q2c. Note that we always have $H \trianglelefteq G \iff$ left and right cosets of H in G coincide.

5. See Tutorial 5 Q3.

6. *First proof*: Consider the sequence of subgroups $H \cap K \leq H \leq G$, by tower law for index of subgroups (see Q5 above), we have $[G : H \cap K] = [G : H][H : H \cap K]$. We will first show that there is a well-defined injective function

$$f : \{\text{Left cosets of } H \cap K \text{ in } H\} \to \{\text{Left cosets of } K \text{ in } G\},$$

therefore $[H : H \cap K] \leq [G : K] = n$. The function f is defined by $f(aH \cap K) = aK$. This is well-defined because if $aH \cap K = bH \cap K$, then $ab^{-1} \in H \cap K \leq K$, in particular $aK = bK$. This function is injective because if $f(aH \cap K) = f(bH \cap K)$, then $ab^{-1} \in K$, but then $aH \cap K$ and $bH \cap K$ are cosets in H, so a, b are assumed to be elements of H, so that $ab^{-1} \in H \cap K$, therefore $aH \cap K = bH \cap K$.

From the above, we have $[G : H \cap K] = [G : H][H : H \cap K] \leq [G : H][G : K] = mn$. The tower law also implies that $m = [G : H]$ divides $[G : H \cap K]$, similarly we can apply the tower law to the sequence $H \cap K \leq K \leq G$, which would imply that $n = [G : K]$ divides $[G : H \cap K]$. Therefore, $\text{lcm}(m, n)$ divides $[G : H \cap K]$ and we have $\text{lcm}(m, n) \leq [G : H \cap K] \leq mn$. Now if $\gcd(m, n) = 1$, then $\text{lcm}(m, n) = mn/\gcd(m, n) = mn$. So both inequality signs must be equality, so $[G : H \cap K] = mn$.

Alternatively proof: Let $aH \in G/H$ and $bK \in G/K$, we can take their intersection $aH \cap bK$. Since any left $H \cap K$ coset in G is an intersection $c(H \cap K) = cH \cap cK$, we know that there are at most mn many left $H \cap K$ cosets in G. It suffices to show that there are at least $\text{lcm}(m, n)$ many cosets. This follows from m and n both divide $[G : H \cap K]$ by the tower law (see Q5, and above).

Remark: There is yet an easier proof using Lagrange's theorem if G is assumed to be finite. However, in the infinite case, we have to work with cosets because the groups G, H, K all have infinite orders.

Optional Part

1. The subgroup $H = \langle i \rangle$ is given by $\{1, i, -1, -i\}$. Its index is $|Q|/|H| = 2$, so the left cosets are simply H and $Q \setminus H$. The representatives of a coset is simply the elements in the coset, so they are exactly H and $Q \setminus H = \{j, -j, k, -k\}$.

2. (a) Recall that any reflection can be expressed as a product of $s = s_1$ and $r = r_1$. Consider the products $(sr_3)s = sr^3s = ssr^{-3} = r^{-3} = r_3$. This calculation shows that $H = \{r_0, r_3, s_1, s_1r_3\}$ is a subgroup: indeed it suffices to check that it is closed under multiplication and taking inverse. Each element is its own inverse. And for multiplications, the only "non-trivial" ones are $r_3s_1 = s_1r_3$ and along with $s_1r_3s_1 = r_3$, which are both in H. So we have obtained a subgroup of order 4. In fact, replacing s_1 with any other reflection works.

   (b) Consider $H = \langle r_2, s_1 \rangle$, then $H = \{r_0, r_2, r_4, s_1, s_1r_2, s_1r_4\}$. It is a subgroup of order 6. (See HW3 optional Q5b). It is also non-cyclic. Since the element r_0 has order 1, r_2, r_4 has order 3 and s_1, s_1r_2, s_1r_4 has order 2. If it was cyclic, then there would be some order 6 element.

3. Suppose G is a group with no nontrivial proper subgroup, and $|G| \geq 2$, we will first show that G has prime order. If it was not the case, say $|G|$ is composite, write $|G| = mn$ for some positive integers m, n that are not equal to 1. Then elements of G would have order dividing $|G|$. It is impossible to have $|g| = |G|$ for all $e \neq g \in G$. This is because if $|g| = |G| = mn$ for some g, then g^m would have order n. So there are some non-identity element $h \in G$ of order strictly smaller than $|G|$, so that $\langle h \rangle$ is a nontrivial proper subgroup of G. Now that we know $|G|$ is prime, it must then be cyclic, since a non-identity element $g \in G$ must has order equals to $|G|$, so it is a generator.

4. If every left coset of H is a right coset of H, then for any left coset gH, there are some $a \in G$ so that $gH = Ha$. The condition $g \in gH = Ha$ implies that there is some $h \in H$ so that $g = ha$. So $Ha = Hg$. Since g is arbitrary, we have shown that $gH = Hg$ for any $g \in G$, i.e. $H \trianglelefteq G$.

5. Let S be the set of elements in G of order n, note that for any $g \in G$, we have $gSg^{-1} = S$, since $|x| = n$ if and only if $|gxg^{-1}| = n$. It remains to prove that $\langle gSg^{-1} \rangle = g\langle S \rangle g^{-1}$, then we have for any $g \in G$,

$$\langle S \rangle = \langle gSg^{-1} \rangle = g\langle S \rangle g^{-1},$$

   i.e. $\langle S \rangle$ is normal.

   The equality $\langle gSg^{-1} \rangle = g\langle S \rangle g^{-1}$ holds in general for any subset S, not just the one described above. This follows directly from $(ga_1g^{-1})^{k_1} \cdots (ga_mg^{-1})^{k_m} = g(a_1^{k_1} \cdots a_m^{k_m})g^{-1}$, where the LHS is a general element in $\langle gSg^{-1} \rangle$ and RHS is a general element in $g\langle S \rangle g^{-1}$.