THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2078 Honours Algebraic Structures 2023-24
Tutorial 3 solutions
29th January 2024

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

1. Let $x, y \in gHg^{-1}$, then by definition there are $u, v \in H$ such that $x = gug^{-1}$ and $y = gvg^{-1}$, then $xy = gug^{-1}gv^{-1}g^{-1} = guv^{-1}g^{-1}$. Since $H \leq G$, $uv^{-1} \in H$ and thus $xy \in gHg^{-1}$.

   We claim that the function $f_1 : H \to gHg^{-1}$ defined by $x \mapsto gxg^{-1}$ is a bijection, thus $|H| = |gHg^{-1}|$. This is because the function $f_2 : gHg^{-1} \to H$ defined by $y \mapsto g^{-1}yg$ is the inverse function to f_1, since $f_1(f_2(y)) = gg^{-1}ygg^{-1} = y$ and $f_2(f_1(x)) = g^{-1}gxg^{-1}g = x$.

2. $H \cap K$ is a subgroup. Let $x, y \in H \cap K$, then $x, y \in H$ and $x, y \in K$, and since H, K are subgroups of G, we have xy^{-1} lies in H and K, so $xy^{-1} \in H \cap K$.

   $H \cup K$ is not necessarily a subgroup. For example, take $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, $H = \mathbb{Z}_2 \times \{0\}$ and $K = \{0\} \times \mathbb{Z}_2$, then $H \cup K = \{(0,0), (1,0), (0,1)\}$. This is not a subgroup of G since $(1,0), (0,1) \in H \cup K$ but $(1,0) + (0,1) \notin H \cup K$.

3. Let $(h_1, k_1), (h_2, k_2) \in H \times K$, since H, K are subgroups of G_1, G_2 respectively, we have $h_1h_2^{-1} \in H$ and $k_1k_2^{-1} \in K$, thus $(h_1, k_1) * (h_2, k_2^{-1}) = (h_1h_2^{-1}, k_1k_2^{-1}) \in H \times K$.

4. Let $g, h \in Z$, by definition $gh^{-1}x = g(x^{-1}h)^{-1} = g(hx^{-1})^{-1} = gx^{-1}h^{-1} = x^{-1}gh^{-1}$ for arbitrary $x \in G$. Since gh^{-1} commutes with arbitrary $x \in G$, $gh^{-1} \in Z$. So Z is a subgroup.

5. Let $g, h \in N_G(H)$, it suffices to prove that $gh^{-1}Hhg^{-1} = H$. First, we show that $h^{-1}Hh = H$. This follows from the fact that $h \in N_G(H)$, so that $hHh^{-1} = H$. Note that $h^{-1}(hHh^{-1})h$ by definition equals to $\{h^{-1}xh : x \in hHh^{-1}\} = \{h^{-1}(hyh^{-1})h : y \in H\} = \{y : y \in H\} = H$. So that composing $h^{-1}(-)h$ on both sides, we get $H = h^{-1}(hHh^{-1})h = h^{-1}Hh$. So $gh^{-1}Hhg^{-1} = gHg^{-1} = H$, as desired.

6. Consider $\mathbb{Z}_{>0} \subset \mathbb{Z}$, this subset is closed under multiplication, since if $m, n > 0$, then $mn > 0$. But $\mathbb{Z}_{>0}$ is not a subgroup of $\mathbb{Z}$, since the inverse of $1 \in \mathbb{Z}_{>0}$, which is -1, is not in $\mathbb{Z}_{>0}$.

7. If G is finite, then for any $x \in H \subset G$, let $n = |x|$. We have $x^n = e$, so that $x^{n-1} = x^{-1}$. Since H is closed under group operation, this shows that $x^{-1} \in H$. So that H is also closed under taking inverse.

8. False, in $\mathbb{Z}_2 \times \mathbb{Z}_2$, every proper subgroup is cyclic. But it is not a cyclic group since there is no element of order 4. The subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2$ are $\{(0,0)\}$, $\langle(1,0)\rangle$, $\langle(0,1)\rangle$, $\langle(1,1)\rangle$ and the group itself, which are all cyclic.

   Alternatively, every dihedral group D_n where n is a prime number also has proper subgroups that are cyclic.

9. Recall that every subgroups of $\mathbb{Z}_n$ is cyclic. So it suffices to consider all subgroups of the form $\langle k\rangle \leq \mathbb{Z}_n$. Furthermore, this subgroup is uniquely determined by $\gcd(k,n)$. So it suffices to look at all possible gcd's.

   For $\mathbb{Z}_8$, the possible gcd's are $1,2,4,8$, generated by $8/1, 8/2, 8/4, 8/8$ respectively. So the subgroups are: $\langle 0\rangle, \langle 4\rangle, \langle 2\rangle, \langle 1\rangle$.

   For $\mathbb{Z}_{11}$, the gcd's are $1, 11$, generated by $11, 1$ respectively. So the subgroups are $\langle 0\rangle, \langle 1\rangle$.

   For $\mathbb{Z}_{12}$, the gcd's are $1,2,3,4,6,12$, generated by $12/1, 12/2, 12/3, 12/4, 12/6, 12/12$ respectively, so the possible subgroups are $\langle 0\rangle, \langle 6\rangle, \langle 4\rangle, \langle 3\rangle, \langle 2\rangle, \langle 1\rangle$.

10. If G is finite, then clearly G has finitely many subgroups, since a subgroup is in particular a subset of G, and therefore the set of subgroups of G can be regarded as subset of the power set of G, so its cardinality is bounded above by $2^{|G|}$.

    Now suppose that G is infinite. If there exists some $g \in G$ such that $\langle g\rangle$ is infinite, then $\langle g\rangle \cong \mathbb{Z}$, then $\langle ng\rangle \leq \langle g\rangle \leq G$ for each $n \in \mathbb{Z}_{>0}$, so there are infinitely many subgroups of G.

    Otherwise, if $\langle g\rangle$ is always finite for any $g \in G$, we shall prove that $\{\langle g\rangle : g \in G\}$ is an infinite set, and thus G has infinitely many subgroups. If it was the case that $\{\langle g\rangle : g \in G\}$ is finite, then $G = \bigcup_{g\in G}\langle g\rangle$ as sets, can be expressed as a finite union of finite sets, thus is finite. This is a contradiction.

    In both situations, G has infinitely many subgroups.

11. Assume that G is some group such that it is a union of two proper subgroups, say $G = H \cup K$. Note that $H \not\subset K$ and $K \not\subset H$, otherwise $G = H$ or $G = K$ and the subgroups would not be proper. Now pick $h \in H \setminus K$ and $k \in K \setminus H$ and consider $hk \in G$. We have $hk \in H$ or $hk \in K$. If $hk \in H$, then $h^{-1} \cdot hk = k \in H$, contradiction. Otherwise if $hk \in K$, then $hk \cdot k^{-1} = h \in K$, also a contradiction. So it is impossible for G to be the union of two proper subgroups.

12. (a) Let $x, y \in G$, by assumption $x^2 = y^2 = e$, so that $x = x^{-1}$ and $y = y^{-1}$. Now consider the element xy, we have $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$. So x, y commutes with each other for arbitrary $x, y \in G$, i.e. G is abelian.

    (b) To show that $H \cup gH$ is a subgroup, it suffices to prove that it is closed under group operation and inversion. $H \cup gH$ is closed under inversion simply because every non-identity element has inverse equals to itself, so $H \cup gH$ contains all inverses of its elements. As for closedness under operation, we consider the following cases:

       i. $x, y \in H$, then $xy \in H$ since H is a subgroup.
       ii. $x \in H, y = gk \in gH$, then $xy = xgk = g(xk) \in gH$ since $xk \in H$.
       iii. $x = gh \in gH, y \in H$, then $xy = g(hy) \in gH$ since $hy \in H$.
       iv. $x = gh, y = gk \in gH$, then $xy = ghgk = g^2hk = hk \in H$.

       So in any case, the product of two elements in $H \cup gH$ lies in itself.

    (c) Recall that the function $f : G \to G$ defined by $f(x) = gx$ defines a bijection. So $f|_H : H \to gH$ also restricts to a bijection. Therefore $|H| = |gH|$. Now we will show that $H \cap gH = \emptyset$, so that $|H \cup gH| = |H| + |gH| = 2|H|$ as desired. To see why, suppose $x \in H \cap gH$, then $x \in H$ and $x = gh$ for some $x \in H$. This implies $g = xh^{-1} \in H$, which contradicts with the assumption that $g \notin H$.

(d) Take $H_0 = \{e\}$, we will construct a sequence of subgroups $H_0 \leq H_1 \leq ... \leq H_k = G$, such that $|H_{i+1}| = 2|H_i|$. The construction is by induction, suppose H_i has been constructed for some $i \geq 0$, if $H_i = G$, then we are done. Otherwise, pick some $g \in G \setminus H_i$, then define $H_{i+1} = H_i \cup gH_i$, which is a subgroup by part (b), and the order satisfies $|H_{i+1}| = 2|H_i|$ by part (c). Since G is a finite group, this process must terminate at some finite step k, this gives $H_k = G$, so that G has order equals to $2^k|H_0| = 2^k$.