# THE CHINESE UNIVERSITY OF HONG KONG <br> Department of Mathematics <br> MATH 3030 Abstract Algebra 2023-24 <br> Homework 7 <br> Due Date: 9th November 2023 

## Compulsory Part

1. Let $G$ be a finite group, and suppose that there exist representatives $g_{1}, \ldots, g_{r}$ of the $r$ distinct conjugacy classes in $G$ such that $g_{i} g_{j}=g_{j} g_{i}$ for all $i, j$. Show that $G$ is abelian.

Proof. Consider $G$ acting on itself by conjugations. Fix a particular $g_{i}$, then for any $x \in G$, we know that it is belongs to some conjugacy class, i.e. $g x g^{-1}=g_{j}$ for some $g$. By assumption $g_{j}$ commutes with $g_{i}$ and so $g x g^{-1} \in Z_{G}\left(g_{i}\right)$ the stabilizer of $g_{i}$. In other words, $x \in g^{-1} Z_{G}\left(g_{i}\right) g$. This implies that $x \in \bigcup_{g \in G} g^{-1} Z_{G}\left(g_{i}\right) g$. So we necessarily have $G=\bigcup_{g \in G} g^{-1} Z_{G}\left(g_{i}\right) g$.
Recall from tutorial 6 question 4 b that this only happens when $Z_{G}\left(g_{i}\right)=G$ because for a proper subgroup $H \lesseqgtr G$ there are at most $[G: H]$ distinct subgroups of the form $g \mathrm{Hg}^{-1}$ and so the union contains at most $[G: H](|H|-1)+1<|G|$ many elements.
Therefore $g_{i}$ commutes with all of $G$ for any $i$, so the conjugacy class is just a singleton $\left\{g_{i}\right\}$. Since this holds for all representative of each individual conjugacy class, this implies that $G$ is abelian.
2. Let $G$ be a finite group and let primes $p$ and $q \neq p$ divide $|G|$. Prove that if $G$ has precisely one proper Sylow $p$-subgroup, then it must be a normal subgroup, and hence $G$ is not simple.
Proof. By the second Sylow theorem, any Sylow p-subgroups are conjugate to each other. If $P$ is the unique proper Sylow p-subgroup of $G$, then $\mathrm{gPg}^{-1}$ is again a Sylow p-subgroup, which must be itself. So for arbitrary $g \in G$ we have $g P g^{-1}=P$, hence it is a proper normal subgroup.
3. Let $G$ be a finite group and let $p$ be a prime dividing $|G|$. Let $P$ be a Sylow $p$-subgroup of $G$.
(a) Show that $P$ is the only Sylow $p$-subgroup of $N_{G}\left(N_{G}(P)\right)$.
(b) Using part (a) and applying Sylow Theorems, show that $N_{G}\left(N_{G}(P)\right)=N_{G}(P)$.

Proof.
(a) Recall that $N_{G}(P)$ is the normalizer of $P$, i.e. consisting of all $g$ so that $g P g^{-1}=P$. By definition $P$ is normal in $N_{G}(P)$ and so it is the unique Sylow p-subgroup of $N_{G}(P)$. Now let $h \in N_{G}\left(N_{G}(P)\right)$, then $h N_{G}(P) h^{-1}=N_{G}(P)$. Restricting this on $P$, by order consideration $h P h^{-1}$ must be some Sylow p-subgroup inside $N_{G}(P)$ so $h P h^{-1}=P$ by uniqueness. This implies that $P$ is also normal in $N_{G}\left(N_{G}(P)\right)$, so it is also the unique Sylow p-subgroup.
(b) Recall that $N_{G}(P)=\left\{g \in G: g P g^{-1}=P\right\}$, since any $h \in N_{G}\left(N_{G}(P)\right)$ satisfies this condition by part (a), we have $N_{G}\left(N_{G}(P)\right)=N_{G}(P)$.
4. Show that there are no simple groups of order $p^{r} m$, where $p$ is a prime, $r$ is a positive integer, and $1<m<p$.
Proof. Suppose $G$ is a group of order $p^{r} m$ with $1<m<p$, consider Sylow p-subgroups of $G$, by third Sylow theorem, $n_{p}=p^{i} k \equiv 1 \bmod p$ for $0 \leq i \leq r$ and $1|k| m$. This implies that $i$ must be zero and $k=1$. So $n_{p}=1$ and there is a unique Sylow p-subgroup of $G$, which is proper and normal. So $G$ cannot be simple.
5. Let $G$ be a group of order 6 . Suppose $G$ is not abelian.
(a) Show that $G$ has three subgroups of order 2 .
(b) Show that there is a homomorphism $\phi: G \rightarrow S_{3}$ with $|\operatorname{ker}(\phi)| \leq 2$. [Hint: Consider the action of $G$ on the set of left cosets of a subgroup of order 2 in $G$ (as in HW6, Optional Q.5).]
(c) Show that $G \simeq S_{3}$.

Proof.
(a) If $G$ is of order 6 and nonabelian, then by third Sylow theorem $n_{3} \equiv 1 \bmod 3$ and $n_{3} \mid 6$ imply that $n_{3}=1$. While $n_{2} \equiv 1 \bmod 2$ and $n_{2} \mid 6$ imply that $n_{2}$ can be 1 or 3 . If $n_{2}$ was also 1 , then the Sylow subgroups are isomorphic to $\mathbb{Z}_{2}$ and $\mathbb{Z}_{3}$, and $G \cong \mathbb{Z}_{2} \times \mathbb{Z}_{3}$, which is abelian. This gives a contradiction. So $n_{2}=3$ and there are three subgroups of order 2.
(b) Suppose $P$ is one of the Sylow 2-subgroups, then $G$ acts on the left coset space $G / P$ by left multiplication. As $|G / P|=3$, this group action induces a homomorphism $\phi: G \rightarrow S_{3}$. Since the action is transitive, the image of $\phi$ consists of (123). So $|\phi(G)| \geq 3$, or $\operatorname{ker}(\phi) \leq 2$.
(c) Consider the non-identity element $x$ of $P$, we would like to prove that $x$ acting on left $P$-cosets nontrivially, i.e $\phi(x) \neq \mathrm{id} \in S_{3}$. Assume for the sake of contradiction that $\phi(x)=\mathrm{id}$, then for an arbitrary $y \in G, y$ lies in some coset $y P$ and we have $x \cdot y P=y P$ since we have assumed that $x$ acts trivially. This implies that $y^{-1} x y \in P$. So we have $y^{-1} P y=P$. But since $y$ is arbitrary, this would imply that $P$ is a normal subgroup, contradicting the fact that $P$ is not the unique Sylow 2-subgroup.
Now $x$ acts nontrivially on $G / P=\left\{P, g_{1} P, g_{2} P\right\}$, and $x$ fixes $P$ because $x \in P$. So it swaps the two other cosets. In other words, $\phi(x)$ is a 2-cycle in $S_{3}$. Since $\phi(G)$ contains a 2-cycle and a 3-cycle, it is the whole group. And $\phi: G \rightarrow S_{3}$ is an isomorphism.
6. (a) Let $G$ be a finite group, and $H, K<G$. Show that

$$
|H K|=\frac{|H| \cdot|K|}{|H \cap K|} .
$$

(Note that $H K$ may not be a subgroup of $G$, so the above is just an equality between orders of sets.)
(b) Suppose that $G$ is a finite group of order 48.
i. Applying Sylow Theorems, show that the number $n_{2}$ of Sylow 2-subgroups in $G$ is either 1 or 3 .
ii. Suppose that $n_{2}=3$ and let $H, K$ be two distinct Syloew 2-subgroups in $G$. Show that $|H \cap K|=8$ by applying part (a). From this and considering the normalizer $N_{G}(H \cap K)$, deduce that $H \cap K$ is normal in $G$, thereby showing that $G$ cannot be simple.

## Proof.

(a) Suppose $H \times K$ acts on $H K$ by $(h, k) \cdot g=h g k^{-1}$. One can check that

$$
\left(h_{1}, k_{1}\right)\left(h_{2}, k_{2}\right) \cdot g=h_{1} h_{2} g k_{2}^{-1} k_{1}^{-1}=\left(h_{1} h_{2}\right) g\left(k_{1} k_{2}\right)^{-1}=\left(h_{1} h_{2}, k_{1} k_{2}\right) \cdot g
$$

And $(e, e) \cdot g=g$. Furthermore given $g, g^{\prime} \in H K$, we can write $g=h k$ and $g^{\prime}=h^{\prime} k^{\prime}$ and hence $g^{\prime}=\left(h^{\prime} h^{-1}, k^{\prime-1} k\right) \cdot g$. So this defines a transitive action. Note that any stabilizer $(h, k)$ of $e \in H K$ satisfies $(h, k) \cdot e=h k^{-1}=e$. In other words, $(H \times K)_{e}=\{(h, k) \in H \times K: h=k\} \cong H \cap K$. By orbit-stabilizer theorem,

$$
|H K|=\frac{|H \times K|}{\left|(H \times K)_{e}\right|}=\frac{|H| \cdot|K|}{|H \cap K|}
$$

(b) i. For a group $G$ of order $48=2^{4} \cdot 3$, third Sylow theorem implies that $n_{2} \equiv 1$ $\bmod 2$ and $n_{2} \mid 48$. Since $n_{2}$ cannot be even, this forces $n_{2}=1$ or 3 .
ii. If $n_{2}=3$, for two distinct Sylow 2-subgroups $H, K$, we have that $H \cap K$ is also a 2-group, with order possibly given by $8,4,2$ or 1 . By considering part (a), $48 \geq|H K|=16^{2} / 2^{k}$ where $k=3,2,1$ or 0 . As $256 / 4=64>48$, the only possible value of $|H \cap K|$ is 8 ,. Now because $H \cap K$ has index 2 in $H$ and $K$, it is a normal subgroup of both $H$ and $K$. By definition $N_{G}(H \cap K)$ is the largest subgroup so that $H \cap K$ is normal in, so our observation implies that $H, K \leq N_{G}(H \cap K)$. Then $H K \subset N_{G}(H \cap K)$. Since $|H K|=32$, we immediately have $N_{G}(H \cap K)=G$. And so $H \cap K$ is in fact a proper normal subgroup in $G$. So that $G$ is not simple.

## Optional Part

1. Let $G$ be a finite group of odd order. Suppose that $g \in G$ and $g^{-1}$ lie in the same conjugacy class. Show that $g=e$.
Proof. Note that if $h g h^{-1}=g^{-1}$, then $h g^{-1} h^{-1}=\left(h g h^{-1}\right)^{-1}=g$. We can let $\langle h\rangle$ acts on the set $X=\left\{g, g^{-1}\right\}$, which has cardinality 1 or 2 depending on whether $g=e$ or not. But $\langle h\rangle$ has odd order and the action is transitive, this forces $|X|=\frac{\operatorname{ord}(h)}{d}$ where $d$ is the order of stabilizer of $g$, which is odd again. This implies that $|X|$ must be an odd number, hence it is equal to 1 and $g=e$.
2. Show that every group of order 30 contains a subgroup of order 15 .

Proof. Let $G$ be a group of order 30 , then $n_{3} \equiv 1 \bmod 3$ so there can be 1 or 10 Sylow 3 -subgroups. Likewise $n_{5} \equiv 1 \bmod 5$, so there can be 1 or 6 Sylow 5 -subgroups. It is impossible to have both $n_{3}=10$ and $n_{5}=6$ because the Sylow p-subgroups are cyclic
and have trivial intersection. So having 10 Sylow 3-subgroups would give $10 \cdot 2=20$ elements of order 3, and having 6 Sylow 5-subgroups would give $4 \cdot 6=24$ elements of order 5, clearly exceeding the total number of elements in $G$.
As a result, either the Sylow 3-subgroup or the Sylow 5-subgroup is unique, and hence is normal. Say we have a normal Sylow 3-subgroup $P$, then if $Q$ is any Sylow 5-subgroup, $P Q$ is a subgroup of order $|P Q|=15$, since they are cyclic and have trivial intersection. Same argument for the case when the Sylow 5-subgroup is unique.
3. Prove that no group of order 160 is simple.

Proof. Let $G$ be a group of order $160=2^{5} \cdot 5$, then $n_{2} \equiv 1 \bmod 2$ so there can be 1 or 5 Sylow 2-subgroups. If there are a unique Sylow 2-subgroup, then it is proper normal and $G$ cannot be simple.

Now suppose $n_{2}=5$. Recall that $G$ acts on the set of Sylow 2 -subgroups $T$ by conjugation. Since there are 5 such subgroups, we get a permutation homomorphism $G \rightarrow S_{5}$. Now $G$ has order 160 while $S_{5}$ has order 120. The kernel of such map must be nontrivial and we obtain a proper normal subgroup of $G$.
4. How many elements of order 7 are there in a simple group of order 168 ?

Proof. Let $G$ be a simple group of order 168. Then $n_{7} \mid 168$ and $n_{7} \equiv 1(\bmod 7)$. Then $n_{7} \mid 24$, and so $n_{7}=1$ or 8 . Since $G$ is simple, $n_{7} \neq 1$. Then $n_{7}=8$. Let $P_{1}, \ldots, P_{8}$ be the 8 subgroups of order 7 in $G$. Then $\left|P_{i} \cap P_{j}\right|=1$ for each $i \neq j$. Each element of order 7 lies in precisely one of $P_{1}, \ldots, P_{8}$, and each of $P_{1}, \ldots, P_{8}$ contains 6 elements of order 7 . Then there are $48=8 \cdot 6$ elements of order 7 in $G$.
5. Let $p, q$ be prime numbers. Show that a group of order $p^{2} q$ is solvable.

Proof. Let $p, q$ be prime numbers. Let $G$ be a group of order $p^{2} q$.
When $p=q$, it follows from Sylow I that $G$ contains a subnormal series $\{e\}=H_{0}<$ $H_{1}<H_{2}<H_{3}=G$, where each $\left|H_{i}\right|=p^{i}$. Then each $H_{i+1} / H_{i}$ is cyclic of order $p$. Then $G$ is solvable.

When $p>q, n_{p} \mid q$ and $n_{p} \equiv 1(\bmod p)$. Then $n_{p}=1$. Let $P$ be the unique Sylow $p$-subgroup of $G$. Then $P \triangleleft G$. Since $|P|=p^{2}$ and $|G / P|=q$, both $P$ and $G / P$ are abelian. Then $G$ is solvable.
When $p<q, n_{q} \mid p^{2}$ and $n_{q} \equiv 1(\bmod q)$. Then $n_{q}=1$ or $n_{q}=p^{2}$. In the former case, there is a unique Sylow $q$-subgroup $Q$ of $G$. Then $Q \triangleleft G,|Q|=q$ and $|G / Q|=p^{2}$. Again, $Q, G / Q$ are both abelian, so $G$ is solvable.
In the later case, $q \mid p^{2}-1$, so $q \mid p-1$ or $q \mid p+1$. But $p<q$, so it must be that $q \mid p+1$ and that $q=p+1$. Then $p=2, q=3$, and $n_{3}=4$. As in the last question, there are 8 elements of order 3. Any group of order 4 must consist of the remaining 4 elements in $G$. Then there exists a unique Sylow 2 subgroup $P$ of order 4. Then $P$ and $G / P$ are both abelian, so $G$ is solvable.
6. Let $p<q<r$ be prime numbers. Show that a group of order $p q r$ is not simple.

Proof. Let $p<q<r$ be prime numbers. Let $G$ be a group of order $p q r$ that is simple. Then $n_{p}\left|q r, n_{q}\right| p r, n_{r} \mid p q ; n_{p} \equiv 1(\bmod p), n_{q} \equiv 1(\bmod q), n_{r} \equiv 1(\bmod r)$, and $n_{p}, n_{q}, n_{r} \neq 1$.

Then $n_{r}=p q$. Then there are $p q(r-1)=p q r-p q$ many elements of order $r$. Note that $n_{q}=r$ or $p r$. This gives at least $(q-1) r$ many elements of order $q$. Now $q-1 \geq p, r>q$, so $(q-1) r+p q(r-1)>p q+p q(r-1)=p q r=|G|$. This exceeds the number of elements of $G$. Contradiction arises.

Therefore, a group of order $p q r$ is not simple.

