MA2202 AY23/24 Sem 2 Final

Solution by Thang Pang Ern
Audited by Ong See Hai

Question 1

Let G be a group, and let $x \in G$ be an element of finite order $n < \infty$. Show that for any $r, s \in \mathbb{Z}_{>0}$ such that $n = rs$, the element $x^r \in G$ is of finite order equal to s.

Solution. Suppose there exists $k \in \mathbb{Z}_{>0}$ such that $x^k = e$. Then, the smallest such k is n. Since $n = rs$, then $(x^r)^s = x^{rs} = x^n = e$, so the order of x^r divides s. Suppose there exists some other $t \in \mathbb{Z}_{>0}$ such that $(x^r)^t = e$, so $x^{rt} = e$. By the definition of the order of an element, $n \mid rt$, so $rs \mid rt$.

Since $r > 0$, then $s \mid t$. Thus, any exponent t for which $(x^r)^t = e$ must be a multiple of s, and so the smallest such t is precisely s. □

Question 2

Let G be a group, and let H and K be subgroups of G. Show that the union $H \cup K$ is a subgroup of G if and only if either $H \subseteq K$ or $K \subseteq H$.

Solution. For the reverse direction, if $H \subseteq K$, $H \cup K = K$. Since K is a subgroup of G, then $H \cup K$ is also a subgroup of G. Similarly, if $K \subseteq H$, then $H \cup K = H$, and we repeat the earlier process, which shows that $H \cup K$ is also a subgroup of G.

For the forward direction, we prove using contraposition. That is, we wish to show

$$\text{if neither } H \subseteq K \text{ nor } K \subseteq H \quad \text{then} \quad H \cup K \text{ is not a subgroup of } G.$$

With this, choose $h \in H \setminus K$ and $k \in K \setminus H$. Note that for any $h, k \in H \cup K$, we have $hk \in H \cup K$. Either $hk \in H$ or $hk \in K$. If $hk \in H$, then $h^{-1}hk \in H$, so $k \in H$, which is a contradiction as $k \in K \setminus H$. Similarly, if $hk \in K$, then $hkk^{-1} \in K$, so $h \in K$. Again, this is a contradiction as $h \in H \setminus K$. We conclude that $H \cup K$ is not a subgroup of G. □

Question 3

(a) Determine the order of the centralizer of $(1\,2)(3\,4)$ in the symmetric group S_6, and justify your answer.

(b) Show that there does not exist any element of order 18 in the symmetric group S_9.

Solution.

(a) Recall that if an element in S_n has m_ℓ cycles of length ℓ, then its centralizer has size

$$\prod_{\ell} \left(\ell^{m_\ell} \cdot m_\ell!\right).$$

Here $x = (1\,2)\,(3\,4)$ has two 2–cycles and two fixed points (i.e. two 1–cycles), so

$$\left|C_{S_6(x)}\right| = \left(2^2 \cdot 2!\right) \times \left(1^2 \cdot 2!\right) = 16.$$

Equivalently, one can see that any $g \in C_{S_6}(x)$ may either

- rotate each of the two 2–cycles independently in 2 ways each,
- permute the mentioned two 2-cycles in 2! ways,
- permute the two fixed points in 2! ways,

so the order is $2^2 \cdot 2! \cdot 2! = 16$.

(b) Say $\sigma \in S_9$ has order $18 = 2 \cdot 3^2$. Then, $\operatorname{lcm}(\ell_1, \ldots, \ell_k) = 2 \cdot 3^2$, where ℓ_i denotes the length of each cycle.

So, there exists ℓ_i which is divisible by $3^2 = 9$. The only cycle of length divisible by 9 in S_9 is a single 9–cycle, but that alone has order 9, not 18, and it already uses up all 9 points so no disjoint 2–cycle can appear. Hence, no permutation in S_9 can have order 18. □

Question 4

Let G be a group and $N \trianglelefteq G$ be a normal subgroup. Suppose Γ is a group and $q : G \to \Gamma$ is a homomorphism with $\ker(q) \supseteq N$ satisfying the following universal property:

For any group H and any homomorphism $f : G \to H$ with $\ker(f) \supseteq N$, there exists a unique homomorphism $f' : \Gamma \to H$ such that $f = f' \circ q$.

Show that $\Gamma \cong G/N$.

Solution. Define $\pi : G \to G/N$ be the canonical quotient map which is surjective. So, $\ker \pi = N \subseteq \ker q$. By the universal property of q, for any group H and any homomorphism $f : G \to H$, there exists a unique homomorphism $f' : \Gamma \to H$ such that $f = f' \circ q$. In particular, we can choose

$$H = G/N \quad q : G \to \Gamma \quad \pi = f \quad u = f',$$

so we construct

$$u : G/N \to \Gamma \quad \text{such that} \quad \pi = u \circ q.$$

As such, we have the following diagram:

$$\begin{tikzcd}
& G \arrow[dl, "\pi"'] \arrow[dr, "q"] & \\
G/N \arrow[rr, bend left, "v"] & & \Gamma \arrow[ll, "u"]
\end{tikzcd}$$

On the other hand, since $\ker q \supseteq N = \ker \pi$, the universal property of π yields a unique

$$v : G/N \longrightarrow \Gamma \quad \text{with} \quad q = v \circ \pi.$$

It now suffices to check that u and v are inverses. First,

$$(u \circ v) \circ \pi = u \circ (v \circ \pi) = u \circ q = \pi,$$

so by uniqueness of the factorisation through π, we get $u \circ v = \mathrm{id}_{G/N}$. Similarly,

$$(v \circ u) \circ q = v \circ (u \circ q) = v \circ \pi = q,$$

and the uniqueness of the factorisation through q forces $v \circ u = \mathrm{id}_\Gamma$. Hence u is an isomorphism, which implies that $\Gamma \cong G/N$. $\square$

Question 5

Prove or disprove: For any infinite set X, there exists a non-trivial proper normal subgroup N in the group $\mathrm{Perm}(X)$ of permutations on X.

Solution. The statement is true. To approach this question, one can take some infinite set as an example, say $X = \mathbb{R}$, and try to construct a corresponding non-trivial proper normal subgroup N. Thereafter, generalise the claim. In particular, the set

$$N = \{\sigma \in \mathrm{Perm}(X) : \text{the set } \{\sigma(x) \neq x\} \text{ is finite}\} \quad \text{is} \quad \text{an example.}$$

We prove that N satisfies the mentioned claims. Since $\sigma, \tau \in \mathrm{Perm}(X)$ each permute finitely many points, then so does $\sigma\tau$ and σ^{-1} (in fact $\sigma = \sigma^{-1}$), so $N \leq \mathrm{Perm}(X)$. $N \trianglelefteq \mathrm{Perm}(X)$ is clear as well.

Lastly, to establish properness, when X is infinite, there exist permutations of X whose support is infinite. In particular, we can choose an infinite cycle, so any such permutation $\sigma \in \mathrm{Perm}(X) \setminus N$. Note that throughout our discussion, N can be taken to not be the trivial group $\{e\}$ since we can choose any transposition $\sigma = (xy)$ which permutes precisely two points (and two is finite). $\square$

Question 6

Let G be a group, and let $N \trianglelefteq G$ be a proper normal subgroup of G. Suppose the only subgroups H of G satisfying $N \subseteq H \subseteq G$ are $H = N$ and $H = G$. Show that the index $[G:N]$ is finite and equal to a prime number.

Solution. Recall the lattice isomorphism theorem, which states that if G is a group and $\pi : G \to G/N$ denotes the canonical projection, then

$$H \to \pi(H) \quad \text{and} \quad X \to \pi^{-1}(X)$$

set up inverse bijections

$$\{H \leq G : N \subseteq H \subseteq G\} \leftrightarrow \{X \leq G/N\}.$$

Using this, we see that the only subgroups of G/N are $\left\{e_{G/N}\right\}$ and G/N. Next, take any non-trivial coset $gN \neq N$. Its cyclic subgroup $\langle gN \rangle$ is non-trivial, so $\langle gN \rangle = G/N$. As such, G/N is a cyclic group.

Suppose on the contrary that $\langle gN \rangle$ is infinite. Then, for each $k \geq 2$, $\left\langle (gN)^k \right\rangle$ would be a proper non-trivial subgroup of G/N, which is a contradiction, so $\langle gN \rangle$ is finite. Consequently, $[G:N]$ is finite, say of order m. In other words, $[G:N] = m$, which is finite.

Lastly, we prove that $|G/N|$ is prime. Recall that any finite cyclic group $\mathbb{Z}/m\mathbb{Z}$ has a unique subgroup of order d for every $d \mid m$. By way of contradiction, if m were composite, then we can write $m = ab$ with $1 < a < m$. So, $\langle (gN)^a \rangle$ is a proper non-trivial subgroup of order b, which again is a contradiction as there are no proper subgroups of G/N. Hence, m has no proper divisors other than 1 and itself, which implies m is prime. $\square$

Question 7

(a) Describe, up to isomorphism, all groups G with the following property: there exists $n \in \mathbb{Z}_{>0}$ and an injective homomorphism $G \hookrightarrow S_n$.

(b) Describe, up to isomorphism, all groups G with the following property: there exists $n \in \mathbb{Z}_{>0}$ and a surjective homomorphism $S_n \twoheadrightarrow G$.

Solution.

(a) By Cayley's theorem, every group G is isomorphic to some subgroup of a symmetric group S_n. Since every subgroup of S_n is finite, then G is precisely the set of all finite groups, up to isomorphism.

(b) Recall that a surjection exhibits, i.e. $G \cong S_n/N$ for some $N \trianglelefteq S_n$. We consider a few cases.

For $n \geq 5$, the only normal subgroups are $\{e\}, A_n, S_n$ so the only non-trivial proper quotient is $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$. Aside from the trivial quotient $S_n/S_n \cong \{e\}$ and the identity map $S_n/\{e\} \cong S_n$, there are no others.

If $n = 4$, besides $\{e\}, A_4, S_4$, we recall that the Klein four-group V is $\trianglelefteq S_4$, and that $S_4/V \cong S_3$.

If $n = 3$, the only non-trivial proper normal subgroup is A_3, so $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$. If $n = 2$ or $n = 1$, there are no non-trivial proper quotients.

To conclude, all such groups G, up to isomorphism, are $\{e\}$, $\mathbb{Z}/2\mathbb{Z}$ or S_k for $k \geq 3$. $\square$

Question 8

Describe all elements of the automorphism group $\mathrm{Aut}(\mathbb{Z})$ of the group $\mathbb{Z}$.

Solution. Let $\varphi : \mathbb{Z} \to \mathbb{Z}$ be a group homomorphism. Then, $\varphi(n) = n\varphi(1)$ for all $n \in \mathbb{Z}$. Note that φ is bijective if and only if $\varphi(1)$ is a generator of $\mathbb{Z}$. Recall that the only generators of the infinite cyclic group $\mathbb{Z}$ are ± 1, so $\varphi(1) = \pm 1$. Consider the maps

$$\varphi_+ : \mathbb{Z} \to \mathbb{Z} \text{ where } n \mapsto n \quad \text{and} \quad \varphi_- : \mathbb{Z} \to \mathbb{Z} \text{ where } n \mapsto -n.$$

Under composition, these maps satisfy the following:

$$\varphi_+ \circ \varphi_+ = \varphi_+ \quad \varphi_+ \circ \varphi_- = \varphi_- \quad \varphi_- \circ \varphi_- = \varphi_+$$

As such, we conclude that $\mathrm{Aut}(\mathbb{Z}) = \{\pm 1\}$. $\square$

Question 9

Let G be a finite group. Suppose $N \trianglelefteq G$ is a normal subgroup such that $|N|$ and $[G:N]$ are relatively prime. Show that N is the unique subgroup of G of order $|N|$.

Solution. Let $K \leq G$ be such that $|K| = |N|$. We will prove that $K = N$. Since $N \trianglelefteq G$, then $NK \leq G$, so $|NK| \mid |G|$ by Lagrange's theorem. Recall that

$$|NK| = \frac{|N|\,|K|}{|N \cap K|} = \frac{|N|^2}{|N \cap K|} \quad \text{and} \quad |G| = |N| \cdot [G:N].$$

So,

$$\frac{|N|^2}{|N \cap K|} \mid |G| \quad \text{which implies} \quad \frac{|N|^2}{|N \cap K|} \mid |N| \cdot [G:N].$$

As such,

$$\frac{|N|}{|N \cap K|} \mid [G:N].$$

Since $\gcd(|N|, [G:N]) = 1$, then $\frac{|N|}{|N \cap K|} = 1$, so $|N| = |N \cap K|$. Hence, $N \cap K = K$, which implies $K \subseteq N$. Since $|K| = |N|$ and $K \subseteq N$, then $K \supseteq N$. It follows that $K = N$. $\square$

Question 10

Let G be a finite group. Let p be a prime and let $P \subseteq G$ be a p-Sylow subgroup. Suppose P is abelian. Show that for any $x, y \in P$, if there exists $g \in G$ such that $gxg^{-1} = y$, then there exists $n \in N_G(P)$ such that $nxn^{-1} = y$.

In other words, two elements of P which are conjugate in G are already conjugate in the normalizer $N_G(P)$ of P.

Solution. Let $x, y \in P$, and suppose there exists $g \in G$ such that $gxg^{-1} = y$. Since $y \in P$ and P is abelian, then every element of P commutes with y. So, $P \subseteq C_G(y)$. Likewise, gPg^{-1} also contains y, so $gPg^{-1} \subseteq C_G(y)$.

As P and gPg^{-1} are both Sylow p-subgroups of $C_G(y)$, then by Sylow's second theorem, they are conjugates in $C_G(y)$. That is to say, there exists $z \in C_G(y)$ such that

$$zPz^{-1} = gPg^{-1}.$$

Since $z \in C_G(y)$, then $zyz^{-1} = y$.

We claim that $n = z^{-1}g$ normalizes P. To see why,

$$nPn^{-1} = z^{-1}gPg^{-1}z = z^{-1}zPz^{-1}z = P$$

so $n \in N_G(P)$. Next, we claim that $nxn^{-1} = y$. We have

$$\begin{aligned} nxn^{-1} &= z^{-1}gxg^{-1}z \quad \text{since } n = z^{-1}g \\ &= z^{-1}yz \quad \text{since } gxg^{-1} = y \text{ as mentioned in the question} \\ &= y \quad \text{since } z \in C_G(y) \end{aligned}$$

as desired. $\square$