Math322 Midterm1 Solutions[1]
Shikun Nie

---

1. **Question:** Let G be the group S_6.

   (a) Prove or disprove: G contains an element of order 8.

   (b) Prove or disprove: the element $(12)(14)(23456)$ has order 4.

   Solution:

   (a) Assume there is an element of order 8, then this element can be written as a product of disjoint cycles. Each cycle has an order that divides 8. Since any cycle in S_6 has a length ranging from 1 to 6, so the only possible cycles are of length 1, 2 or 4. But any product of cycles with these lengths will have a maximum order of $\mathrm{lcm}(1, 2, 4) = 4$, a contradiction.

   (b) By rewriting the element into disjoint cycles, we have $(1456)(23)$. Each n-cycle has an order of n. The overall order of this element is the lcm of all orders of the disjoint cycles, thus the order is 4.

2. **Question:** Let G be a group and K a subgroup.

   (a) Show that the set G/K and $K\backslash G$ of left and right cosets have the same cardinality.

   (b) Prove that if $gKg^{-1} \subset K$ for all $g \in G$, then $gKg^{-1} = K$ for all $g \in G$.

   Solution:

   (a) Define

   $$f : G/K \to K\backslash G$$
   $$gK \mapsto f(gK) = Kg^{-1}$$

   f is well-defined since for $g, g' \in G$ such that

   $$g'K = gK \Leftrightarrow g^{-1}g' \in K \Leftrightarrow Kg^{-1} = K(g')^{-1}$$

   To prove injectivity, assume $f(gK) = f(g'K)$, then by the equivalence above from right to left we have $gK = g'K$. To prove surjectivity, for any $Kg \in K\backslash G$, $f(g^{-1}K) = K(g^{-1})^{-1} = Kg$. Therefore, f is bijective and $|G/K| = |K\backslash G|$.

   (b) Suppose the statement is not true, so $\exists g \in G$ such that $gKg^{-1} \neq K$. By the condition of the statement, gKg^{-1} is a proper subset of K. Now it is easy to show that the following map is injective but not surjective:

   $$f_g : K \to K$$
   $$k \mapsto f_g(k) = gkg^{-1}$$

   Then for any other element $g' \in G$, the map $f_{g'}$ is injective but not surjective too. To see this, first notice that $f_g(k') = g'g^{-1}f_g(k)(g'g^{-1})^{-1}$. Let's choose $k \in K \setminus gKg^{-1}$. Since $g'g^{-1}k(g'g^{-1})^{-1} \in K$ but there is no element $k' \in K$ such that $f_{g'}(k') = g'g^{-1}f_g(k')(g'g^{-1})^{-1}$, $f_{g'}$ is not surjective. Hence $\forall g \in G$, f_g is injective but not surjective on K. However, we know that f_e is a bijection on K, which is a contradiction.

   An alternative proof for (b):

   For any element $gk \in gK$, we have

   $$gk = gkg^{-1}g = k'g \in Kg$$

[1] If you find any typos, please send an email to kennethnye@math.ubc.ca

Therefore, $gK \subset Kg$. Similarly, for any $kg \in Kg$, we have

$$kg = gg^{-1}kg = gk' \in gK$$

Thus, $Kg \subset gK$ as well. In conclusion, $gK = Kg$, which means $gKg^{-1} = K$.

Here is another proof for (b):

It suffices to show that $\forall g \in G, K \subset gKg^{-1}$. For any $k \in K$, we know that $k' := g^{-1}kg \in K$ by the assumption of this question. Then $gk'g^{-1} = k$. Therefore, $K \subset gKg^{-1}$.

The shortest proof for (b):

For any $g \in G$

$$g^{-1}Kg \subset K \Leftrightarrow K \subset gKg^{-1}$$

Together with $gKg^{-1} \subset K$, we conclude that $gKg^{-1} = K$.

3. **Question:** Let G be a finite abelian group of order n, written with additive notation. Let q be any positive integer, and let $G_q = \{x \in G : qx = 0\}$ and $G^q = \{qx : x \in G\}$.

   (a) Show that G_q and G^q are subgroups of G, for all q.

   (b) Show that $(q, n) = 1 \Rightarrow G_q = \{0\}$.

   (c) Prove that $(q, n) = 1 \Rightarrow G^q = G$.

   Solution:

   (a) By the finite subgroup test, we only need to show that G_q is nonempty and if $x, y \in G_q$, then $x + y \in G_q$. For the first condition, it is easy to see that $0 \in G_q$. while for the second we see $q(x + y) = qx + qy = 0 + 0 = 0$, thus $x + y \in G_q$. Similarly, $0 \in G^q$ and $q(x + y) \in G^q$ since $x + y \in G$.

   (b) For any $x \in G_q$, the $\text{ord}(x)$ divides both $n := |G|$ and q. So $\text{ord}(x)|\text{gcd}(n, q) = 1$ and $\text{ord}(x) = 1$. The only such element is 0.

   (c) Define

$$f : G \to G$$
$$x \mapsto f(x) = qx$$

   and let's prove it is a bijection. Since n is finite, it suffices to show f is injective. Now suppose $f(x) = f(x')$, then

$$q(x - x') = 0$$

   By the result of part (b), the only possible scenario is $x - x' = 0$, i.e., $x = x'$.

4. **Question:** (a) Let G be a finite group and let H, K be subgroups. Let $x \in G$ and set $HxK = \{hxk | h \in H,\ k \in K\}$. Show that the cardinality of HxK is equal to $\frac{|H||K|}{|H \cap xKx^{-1}|}$.

   (b) Let G be a group and let H, K be subgroups of G with $H \subset K$. Let π_k denote the map $G \to G/K$ given by $g \mapsto gK$ and similarly define $\pi_H : G \to G/H$. Show that there exists a unique map $\pi : G/H \to G/K$ such that $\pi_K = \pi \circ \pi_H$.

   Solution:

   (a) Since K is a subgroup, it is easy to verify that the conjugation xKx^{-1} is also a subgroup. The intersection of two subgroups $I := H \cap xKx^{-1}$ is a subgroup of the group H. The number of left cosets of H to I is exactly $|H : I| = \frac{|H|}{|I|}$. Since $HxK = \bigcup_{h \in H} hxK$ and $\forall h \in H,\ |hxK| = |K|$, the cardinality of HxK is a multiple of $|K|$. Let's say $|HxK| = r|K|$. Finally, we show that $r = |H : I|$ via the following bijective map.

$$f : \{hI : h \in H\} \to \{hxK : h \in H\}$$

$$hI \mapsto f(hI) = hxK$$

f is well-defined and is injective (hence bijective) since for any $h, h' \in H$,

$$hI = h'I \Leftrightarrow h^{-1}h' \in I \Leftrightarrow x^{-1}h^{-1}h'x \in K \Leftrightarrow hxK = h'xK$$

Therefore,

$$|HxK| = |H : I||K| = \frac{|H||K|}{|H \cap xKx^{-1}|}$$

An alternative proof for (a): Denote $I := H \cap xKx^{-1}$. Consider the following map:

$$f : \{hxkK : h \in H,\ k \in K\} \to \{hI : h \in H\}$$

f is well-defined and is injective (hence bijective) since for any $h, h' \in H$,

$$hxkK = h'xk'K \Leftrightarrow k^{-1}x^{-1}h^{-1}h'xk' \in K \Leftrightarrow h^{-1}h' \in I \Leftrightarrow hI = h'I$$

Therefore,

$$|HxK : K| = |H : I|$$

which translates to

$$|HxK| = \frac{|H||K|}{|H \cap xKx^{-1}|}$$

(b) The preimage of gH under π_H is

$$\pi_H^{-1}(gH) = \{g' \in G : g^{-1}g' \in H\}$$

The image of this set under the map π_K is

$$\begin{aligned} \pi_K(\pi_H^{-1}(gH)) &= \pi_K(\{g' \in G : g^{-1}g' \in H \subset K\}) \\ &= gK \end{aligned}$$

Thus, the only way to construct π is

$$gH \mapsto \pi(gH) = gK$$

so that $\pi_K = \pi \circ \pi_H$.

5. **Question:** Let p denote a prime number and let G be a finite abelian group of order p^2. Show that G has a unique subgroup of order p if G is cyclic and that G has $p+1$ subgroups of order p if G is not cyclic.

   Solution: If G is cyclic, then there exists $g \in G$ with $\operatorname{ord}(g) = p^2$ such that $G = \{g^i : i = 0, 1, \cdots, p^2-1\}$. Recall that for a cyclic group G, $\operatorname{ord}(g^i) = \frac{|G|}{\gcd(|G|, i)} = \frac{p^2}{\gcd(p^2, i)}$. The subset $G^p = \{g^{pi} : i = 0, 1, \cdots, p-1\}$ containing all elements of order p together with the identity is a cyclic subgroup of G with cardinality p. There is no other cyclic subgroup of cardinality p since any element in $G \setminus G^p$ has order p^2, thus it cannot be an element of a subgroup with cardinality p. If G is not cyclic, we claim that $\forall g \in G \setminus \{e\}$, $\operatorname{ord}(g) = p$. Suppose not, then there exists an element $g \in G$ such that $\operatorname{ord}(g) = p^2$. It must be the case $\{g^i : i = 0, 1, \cdots, p^2-1\} = G$, which is a contradiction to that G is not cyclic. Now let's take any two elements $g, g' \in G \setminus \{e\}$, then either $\{g^i : i = 0, 1, \cdots, p-1\} \cap \{(g')^i : i = 0, 1, \cdots, p-1\} = \{e\}$ or $\{g^i : i = 0, 1, \cdots, p-1\} = \{(g')^i : i = 0, 1, \cdots, p-1\}$ since if there is another element g'' other than e in the intersection then it generates the entire subgroup of cardinality p. Since

   $$G \setminus \{e\} = \bigcup_{g \in G \setminus \{e\}} \{g^i : i = 1, \cdots, p-1\}$$

   and each $\{g^i : i = 1, \cdots, p-1\}$ has cardinality $p-1$, there must be $\frac{p^2-1}{p-1} = p+1$ distinct such sets. Each set equipped with the identity is a subgroup of cardinality p.