Homework 3

Due: May 22nd (Friday), 11:59 pm

- Please submit your work on Blackboard.
- You are required to submit your work as a single pdf.
- Please make sure your handwriting is clear enough to read. Thanks.
- No late work will be accepted.
- There are five randomly picked questions (2 pts for each) that will be graded.
  (2), (8), (9), (10), (12)

---

(1) In $\mathrm{GL}_2(\mathbf{R})$, find the order of each of the following elements.

(a) $\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}$ $\quad \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$,

$$\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}^3 = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -I_2$$

$\Rightarrow \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}^6 = (-I_2)^2 = I_2$. Thus, the matrix $\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}$ has order 6.[1]

(b) $\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$ $\quad \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix}$ for all n.

Thus, the matrix $\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$ has infinite order.

(2) For each of the following groups, find all cyclic subgroups of the group.

(a) $\mathbf{Z}_8$

$\mathbf{Z}_8 = \langle [1] \rangle = \langle [3] \rangle = \langle [5] \rangle = \langle [7] \rangle$ since $\mathbf{Z}_8^\times = \{[1], [3], [5], [7]\}$.
$\langle [2] \rangle = \langle [6] \rangle = \{[0], [2], [4], [6]\}$
$\langle [4] \rangle = \{[0], [4]\}$
$\langle [0] \rangle = \{[0]\}$

(b) $\mathbf{Z}_{12}^\times$

$\mathbf{Z}_{12}^\times = \{[1], [5], [7], [11]\} = \{[1], [5], [-5], [-1]\}$
$\langle [1] \rangle = \{[1]\}$
$\langle [5] \rangle = \{[1], [5]\}$
$\langle [7] \rangle = \{[1], [7]\}$
$\langle [11] \rangle = \{[1], [11]\}$
This implies that $\mathbf{Z}_{12}^\times$ is not a cyclic group.

(3) Find the cyclic subgroup of S_6 generated by the element $(123)(456)$.

$[(123)(456)]^2 = (123)^2(456)^2 = (132)(465)$ since (123) and (456) are disjoint.
$[(123)(456)]^3 = (123)^3(456)^3 = (1)$ since (123) and (456) are cycles of length 3
Thus, $\langle (123)(456) \rangle = \{(1), (123)(456), (132)(465)\}$.

---

[1] It easily follows from the direct computations to see that its order cannot be 4 or 5.

(4) Let $G = \mathrm{GL}_3(\mathbf{R})$. Show that

$$H = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix} \right\}$$

is a subgroup of G.

(i) Closure: $\begin{bmatrix} 1 & 0 & 0 \\ a_1 & 1 & 0 \\ b_1 & c_1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ a_2 & 1 & 0 \\ b_2 & c_2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ a_1 + a_2 & 1 & 0 \\ b_1 + c_1 a_2 + b_2 & c_1 + c_2 & 1 \end{bmatrix} \in H.$

(ii) The identity matrix $I_3 \in H$ by letting $a = b = c = 0$.

(iii) Inverses: By part (i): $\begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ -a & 1 & 0 \\ -b + ca & -c & 1 \end{bmatrix} \in H.$

(5) Let S be a set, and let a be a fixed element of S. Show that

$$\{\sigma \in \mathrm{Sym}(S) \mid \sigma(a) = a\}$$

is a subgroup of $\mathrm{Sym}(S)$.

(a) Closure: If $\sigma(a) = a, \tau(a) = a$, then $\sigma\tau(a) = \sigma(a) = a$.

(b) The identity permutation $1_S(a) = a$.

(c) The inverse σ^{-1} of σ: $\sigma^{-1}\sigma(a) = 1_S(a) = a \Rightarrow \sigma^{-1}(a) = a$.

(6) Prove that any cyclic group is abelian.

Let $\langle g \rangle$ be a cyclic group G. For any two elements $a, b \in G$, there exist $m, n \in \mathbf{Z}$ such that $a = g^m$ and $b = g^n$. Thus,

$$ab = g^m g^n = g^{m+n} = g^{n+m} = g^n g^m = ba.$$

(7) Prove that the intersection of any collection of subgroups of a group is again a subgroup.

Let G be a group and H_i be a subgroup of G for $i \in I$. (I is an index set) Then we need to show that $K = \cap_{i \in I} H_i$ is again a subgroup of G.

(a) Take any $a, b \in K \subseteq H_i$, for each i. Then $ab \in H_i$ since H_i is a subgroup. Thus, $ab \in K$ since i is arbitrary.

(b) The identity element $e \in H_i$ for each i, so $e \in K$.

(c) Take any $a \in K \subseteq H_i$, for each i. Then $a^{-1} \in H_i$ since H_i is a subgroup. Thus, $a^{-1} \in K$ since i is arbitrary.

(8) Let G be a group, and let $a \in G$. The set

$$C(a) = \{x \in G \mid xa = ax\}$$

of all elements of G that commute with a is called the **centralizer** of a.

(a) Show that $C(a)$ is a subgroup of G.

(b) Show that $\langle a \rangle \subseteq C(a)$.

(c) Computer $C(a)$ if $G = S_3$ and $a = (123)$.

(d) Computer $C(a)$ if $G = S_3$ and $a = (12)$.

(a) (i) Closure: Let $x, y \in C(a)$. Then $xy \in C(a)$ since
$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy).$$
(ii) The identity element $e \in C(a)$ since $ea = a = ae$.
(iii) If $x \in C(a)$, then $x^{-1} \in C(a)$. We know that $a = ea = (xx^{-1})a$ and $a = ae = a(xx^{-1})$, this implies that $(xx^{-1})a = a(xx^{-1}) = (ax)x^{-1} = (xa)x^{-1}$ since $x \in C(a)$. So
$$\begin{aligned}(xx^{-1})a =&(xa)x^{-1}\\ x(x^{-1}a) =&x(ax^{-1})\\ x^{-1}a =&ax^{-1}.\end{aligned}$$

(b) It is clear that $a \in C(a)$. Thus, $\langle a \rangle \subset C(a)$ by Proposition 2 (b).

(c) It follows from part (b) that $\langle (123) \rangle = \{(1), (123), (132)\} \subseteq C((123))$. By the direct computations, we can see that there is no other element in S_3 belong to $C((123))$.[2] Thus, $C((123)) = \langle (123) \rangle = \{(1), (123), (132)\}$.

(d) Similarly, we can see that $C((12)) = \langle (12) \rangle = \{(1), (12)\}$.

(9) Let G be a group. The set
$$Z(G) = \{x \in G \mid xg = gx \text{ for all } g \in G\}$$
of all elements that commute with every other element of G is called the **center** of G.

(a) Show that $Z(G)$ is a subgroup of G.

(i) If $x, y \in Z(G)$, then $xy \in Z(G)$ since by definition we have
$$(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy) \text{ for all } g \in G.$$
(ii) The identity element $e \in Z(G)$ since $eg = g = ge$ for all $g \in G$.
(iii) If $x \in Z(G)$, then $x^{-1} \in Z(G)$. In fact, for all $g \in G$ we have
$$g = eg = (x^{-1}x)g = x^{-1}(xg) = x^{-1}(gx) = (x^{-1}g)x.$$
Thus, $gx^{-1} = x^{-1}g$ for all $g \in G$.

(b) Show that $Z(G) = \cap_{a \in G} C(a)$.

$Z(G) \subseteq \cap_{a \in G} C(a)$: For any $x \in Z(G)$, it is clear that $x \in C(a)$ for any $a \in G$ since $xa = ax$ by definition. So, $x \in \cap_{a \in G} C(a)$ since a is arbitrary. Thus, $Z(G) \subseteq \cap_{a \in G} C(a)$.
$\cap_{a \in G} C(a) \subseteq Z(G)$: For any $x \in \cap_{a \in G} C(a)$, then $x \in C(a)$ for all $a \in G$. That is, $xa = ax$ for all $a \in G$. This implies that $x \in Z(G)$ by definition. Thus, $\cap_{a \in G} C(a) \subseteq Z(G)$.

(c) Computer the center of S_3.

By Question 8 (c) and (d), we know that
$$C((123)) = \{(1), (123), (132)\} \text{ and } C((12)) = \{(1), (12)\}.$$
This implies that $C((123)) \cap C((12)) = \{(1)\}$. It follows from part (b) that $Z(G) = \cap_{a \in S_3} C(a) \subseteq (C((123)) \cap C((12))) = \{(1)\}$. It is also clear that the identity element $(1) \in Z(G)$. Therefore, $Z(G) = Z(S_3) = \{(1)\}$.

[2] You can also see this by looking at the multiplication table for S_3.

(10) Show that if a group G has a unique element a of order 2, then $a \in Z(G)$.

To show $a \in Z(G)$, it is equivalent to show that $ab = ba$ for all $b \in G$. Consider the element bab^{-1} for each $b \in G$, since $a^2 = e$ we have

$$(bab^{-1})^2 = (bab^{-1})(bab^{-1}) = bab^{-1}bab^{-1} = ba^2b^{-1} = beb^{-1} = e.$$

We omit the parentheses in the above calculations. There are two possibilities:

(a) If $bab^{-1} = e$, then $ba = b$. This implies $a = e$. We obtain a contradiction since $o(a) = 2$.

(b) If $bab^{-1} \neq e$, then $o(bab^{-1}) = 2$. So $bab^{-1} = a$ since the element a is the unique one in G with order 2. This implies $ba = ab$ for all $b \in G$. Thus, $a \in Z(G)$.

(11) Let G be a group with $a, b \in G$.

(a) Show that $o(a^{-1}) = o(a)$.

Let $o(a) = n > 0$. By $a^n = e$, we have $(a^n)^{-1} = e$. Thus $(a^{-1})^n = e$. It implies that $o(a^{-1})|n$. If $m = o(a^{-1}) < n$, there exists a positive integer q such that $n = mq$. Then $(a^{-1})^m = (a^m)^{-1} = e$. This means that $a^m = e$. We obtain a contradiction since $o(a) = n > m$.
If $o(a)$ is infinite, so is $o(a^{-1})$. Otherwise, suppose that $m = o(a^{-1}) > 0$, we can conclude that $a^m = e$ by applying the similar argument as above. Again we obtain a contradiction since $o(a)$ is infinite.

(b) Show that $o(ab) = o(ba)$.

Let $o(ab) = n$ and so we have $(ab)^n = e$. This implies that

$$(ab)^n = a(ba)^{n-1}b = e \Rightarrow (ba)^{n-1}b = a^{-1} \Rightarrow (ba)^{n-1}(ba) = (ba)^n = e.$$

Thus, $o(ba)|n$. Similarly, let $o(ba) = m$ and so $(ba)^m = e$. Then

$$(ba)^m = b(ab)^{m-1}a = e \Rightarrow (ab)^{m-1}a = b^{-1} \Rightarrow (ab)^{m-1}(ab) = (ab)^m = e.$$

Thus, $o(ab)|m$. We can conclude that $m = n$ since $m|n$ and $n|m$.
Again, a similar argument shows that if $o(ab)$ is infinite, then so is $o(ba)$.

(c) Show that $o(aba^{-1}) = o(b)$.

Let $o(aba^{-1}) = n$ and so $(aba^{-1})^n = e$. In particular, we have

$$(aba^{-1})^n = (aba^{-1})(aba^{-1}) \cdots (aba^{-1}) = ab^na^{-1} = e.$$

This implies $b^n = e$. On the other hand, let $o(b) = m$ and so $b^m = e$. So

$$b^m = a^{-1}(aba^{-1})^m a = e \Rightarrow (aba^{-1})^m = e.$$

It follows from above discussions that $m|n$ and $n|m$. Again, $m = n$.
A similar argument shows that if $o(aba^{-1})$ is infinite, then so is $o(b)$.
An easier way to show it: Let $A = ab$ and $B = a^{-1}$. By part (b), we have

$$o(AB) = o(BA) \Rightarrow o(aba^{-1}) = o(a^{-1}(ab)) = o((a^{-1}a)b) = o(b).$$

(12) Let G be a group with $a, b \in G$. Assume that $o(a)$ and $o(b)$ are finite and relatively prime, and that $ab = ba$. Show that $o(ab) = o(a)o(b)$.

Let $o(a) = n$ and $o(b) = m$ with $(n, m) = 1$. To show $o(ab) = nm$.
First, it follows from $ab = ba$ that $(ab)^{nm} = a^{nm}b^{nm} = (a^n)^m(b^m)^n = e^me^n = e$.
Assume that $o(ab) = k$, then $k|nm$. We are done if we can also show $nm|k$.
Write $k = nq_1 + r_1$ and $k = mq_2 + r_2$ for some $q_1, q_2 \in \mathbf{Z}$, where $0 \leq r_1 < n$ and $0 \leq r_2 < m$. By definition of n, m, k and $ab = ba$, we have

$e = (ab)^k = a^k b^k = a^{nq_1+r_1} b^{mq_2+r_2} = (a^n)^{q_1} a^{r_1} (b^m)^{q_2} b^{r_2} = e^{q_1} a^{r_1} e^{q_2} b^{r_2} = a^{r_1} b^{r_2}$.
Claim: $r_1 = r_2 = 0$.
Proof of Claim: It suffices to show one of these two values is zero, say $r_1 = 0$. If $r_1 = 0$, then $r_2 = 0$ since $e = b^{r_2}$ and $0 \leq r_2 < m = o(b)$. The same argument can be applied for the other side: i.e., if $r_2 = 0$, then $r_1 = 0$.
Since $e = a^{r_1} b^{r_2}$, we have $b^{r_2} = a^{-r_1}$. It follows from $b^m = e$ that

$$(b^{r_2})^m = (b^m)^{r_2} = e^{r_2} = e \Rightarrow (a^{-r_1})^m = (a^{r_1 m})^{-1} = e \Rightarrow a^{r_1 m} = e.$$

It implies that $n | r_1 m$. Thus, $n | r_1$ since $(n, m) = 1$. We can conclude that $r_1 = 0$ since $0 \leq r_1 < n$. This means that we finish the proof of the claim, i.e., $r_1 = r_2 = 0$.
It implies that $k = nq_1 = mq_2$ for some $q_1, q_2 \in \mathbf{Z}$. So $n | k$ and $m | k$, thus $nm | k$ since $(m, n) = 1$. Finally, we obtain $k = nm$ since $k | nm$ and $nm | k$. $\square$