

# Past Paper: Group Theory I

Midterm Exam, 2024

Rashid M. Talha

**Disclaimer:** Use at your own risk. Errors possible.

## Question 1 (i).

Prove that the order of a cyclic group is equal to the order of its generator.

*Solution.* If  $O(a)$  is infinite then  $a^n$  and  $a^m$  are distinct for all  $n \neq m$ , because otherwise,

$$a^n = a^m \implies a^{n-m} = 1 \implies O(a) \leq |n - m|$$

which is a contradiction. Now, since each  $a^n$  is different from  $a^{n+1}$ , we have infinitely many elements in the set  $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ . Consequently,  $G = \langle a \rangle$  has infinitely many elements; i.e.  $|G|$  is also infinite.

Next, consider the case when  $O(a) = n$  is finite. By definition  $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ . We can write  $k = qn + r$  for  $q, r \in \mathbb{Z}$  and  $0 \leq r < n$ . So, for all  $k \in \mathbb{Z}$ ,

$$a^k = a^{qn+r} = a^{qn}a^r = (a^n)^q = ea^r = a^r.$$

Therefore,  $\langle a \rangle = \{a^r \mid 0 \leq r < n\} = \{e, a, a^2, \dots, a^{n-1}\}$ . Again, take any  $a^p, a^q \in \langle a \rangle$  with  $p \neq q$ , then

$$a^p = a^q \implies a^{p-q} = 1 \implies O(a) \leq |p - q| \leq n - 1$$

which is not possible because  $O(a) = n$ . Therefore, each element in this set is distinct, and we get  $|G| = |\langle a \rangle| = n$ .

## Question 1 (ii).

Let  $G = \langle a \rangle$  be a finite cyclic group of order  $n$ . Then prove that an element  $a^k$  is a generator if and only if  $\gcd(n, k) = 1$ .

*Solution.* Suppose  $a^k$  is a generator of  $G$ . Then, we can write  $a$  as a power of  $a^k$ , say  $a = (a^k)^m = a^{km}$  for some  $m \in \mathbb{Z}$ .

Then,  $a = a^{km} \implies aa^{-km} = e \implies a^{1-km} = e$ . So,  $n \mid 1 - km$ . That is  $\exists q \in \mathbb{Z}$  such that  $1 - km = qn$ . We can re-arrange this to get  $qn + km = 1$ . From number theory (Bezout's lemma) we know that this implies  $\gcd(n, k) = 1$ .

Conversely, suppose  $\gcd(n, k) = 1$ . Then, there exist integers  $x, y$  such that  $xk + yn = 1$ . So,  $a = a^{xk+yn} \implies a = (a^k)^x (a^n)^y \implies a = (a^k)^x e^y \implies a = (a^k)^x$ .

Now for all  $b \in G = \langle a \rangle$ , we have  $b = a^r$  for some  $r \in \mathbb{Z}$ . Therefore, we can write it as a power of  $a^k$  as  $b = a^r = ((a^k)^x)^r = (a^k)^{xr}$ . So,  $a^k$  also generates  $G$ .

## Question 2 (i).

Let  $H$  be a subgroup of  $G$ . Let  $\sim$  be a relation on  $G$  defined by  $a \sim b$  if and only if  $a^{-1}b \in H$ . Then show that  $\sim$  is an equivalence relation on  $G$ . Also prove that  $[a] = aH$ .

*Solution.* We check that  $\sim$  satisfies the three conditions of being an equivalence relation.

(Reflexive.) Take  $a \in G$ . Then,  $a^{-1}a = e$  and  $e \in H$  because  $H \leq G$ . So,  $a \sim a$ .

(Symmetric.) Suppose  $a \sim b$ . That means  $a^{-1}b \in H$ . As  $H \leq G$ , the element  $(a^{-1}b)^{-1} \in H$ . And  $(a^{-1}b)^{-1} = b^{-1}a$ . That is,  $b^{-1}a \in H$ . So,  $b \sim a$ .

(Transitive.) Suppose  $a \sim b$  and  $b \sim c$ . That is  $a^{-1}b \in H$  and  $b^{-1}c \in H$ . As  $H$  is a subgroup, closure and associativity gives  $(a^{-1}b)(b^{-1}c) = a^{-1}c \in H$ . So,  $a \sim c$ .

Next,  $[a] = \{b \in G \mid b \sim a\} = \{b \in G \mid a \sim b\} = \{b \in G \mid a^{-1}b \in H\}$ . And,  $a^{-1}b \in H$  means  $a^{-1}b = h$  for some  $h \in H$ . As a result,  $b = ah$  and we can write

$$[a] = \{b \in G \mid a^{-1}b \in H\} = \{ah \in G \mid h \in H\} = aH.$$

**Question 2 (ii).**

Let  $G$  be a group and  $H$  be a subgroup of  $G$ . If  $a, b \in G$ , then prove that  $aH = bH$  if and only if  $a^{-1}b \in H$ .

TBC

**Question 2 (iii).**

Let  $G$  be a group and  $a \in G$  such that  $o(a) = n$ . If  $m$  is an integer such that  $a^m = e$ , then prove that  $n$  divides  $m$ .

*Solution.* By the division algorithm,  $m = qn + r$  for  $q, r \in \mathbb{Z}$  and  $0 \leq r < n$ . So,

$$a^m = a^{nq+r} = (a^{nq})(a^r) = (e^q)(a^r) = e(a^r) = a^r.$$

Now,  $a^m = e \implies a^r = e$ . However,  $r < n$  and  $n$  is the least positive integer for which  $a^n = e$ . Therefore,  $r$  must be zero (if it was positive then it would contradict the minimality of  $n$ ). Therefore,  $m = qn$ . That is  $n \mid m$ .

**Question 3 (i).**

Let  $\mathbb{Z}_{12} = \{0, 1, \dots, 11\}$  be the group of integers modulo 12. Then find the order of each element of  $\mathbb{Z}_{12}$ .

*Solution.* The order of each element in  $\mathbb{Z}_{12}$  is

$$\begin{array}{llll} O(0) = 1 & O(1) = 12 & O(2) = 6 & O(3) = 4 \\ O(4) = 3 & O(5) = 12 & O(6) = 2 & O(7) = 12 \\ O(8) = 3 & O(9) = 4 & O(10) = 6 & O(11) = 12 \end{array}$$

**Question 3 (ii).**

Find all subgroups of the cyclic group  $C_{12} = \{1, a, a^2, \dots, a^{11} \mid a^{12} = 1\}$ .

*Solution.* We arrange these by the GCD of  $n = 12$  and the order of the generator.

$$\begin{array}{ll} \gcd = 1: & \langle 1 \rangle = \{1\} \\ \gcd = 2: & \langle a^6 \rangle = \{1, a^6\} \\ \gcd = 3: & \langle a^4 \rangle = \langle a^8 \rangle = \{1, a^4, a^8\} \\ \gcd = 4: & \langle a^3 \rangle = \langle a^9 \rangle = \{1, a^3, a^6, a^9\} \\ \gcd = 6: & \langle a^2 \rangle = \langle a^{10} \rangle = \{1, a^2, a^4, a^6, a^8, a^{10}\} \\ \gcd = 12: & \langle a \rangle = \langle a^{11} \rangle = \langle a^5 \rangle = \langle a^7 \rangle = C_{12} \end{array}$$

**Question 3 (iii).**

Let  $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$  be a group under addition of matrices, and take  $H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a + b + c + d = 1 \in \mathbb{Z} \right\}$ . Prove or disprove that  $H$  is a subgroup of  $G$ .

*Solution.*  $H$  is not a subgroup of  $G$  because it doesn't contain the identity element. That is

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \notin H$$

since  $0 + 0 + 0 + 0 \neq 1$ .

**Question 4 (i).**

Let  $*$  be a binary operation on  $\mathbb{Q}^+$  defined by  $a * b = \frac{ab}{2}$ . Then show that  $\mathbb{Q}^+$  is an Abelian group with respect to  $*$ . ( $\mathbb{Q}^+$  denotes the set of positive rational numbers.)

*Solution.* We check the group axioms.

(Closure.) Take  $a, b \in \mathbb{Q}^+$ . Then, in particular,  $a, b \in \mathbb{Q}$  and  $a, b > 0$ . So,  $ab \in \mathbb{Q}$  and  $\frac{ab}{2} \in \mathbb{Q}$ . Moreover,  $ab > 0$  and  $\frac{ab}{2} > 0$ . That means  $\frac{ab}{2} \in \mathbb{Q}^+$ . Therefore,

$$a * b = \frac{ab}{2} \in \mathbb{Q}^+$$

(Associativity.) Take  $a, b, c \in \mathbb{Q}^+$ . Then,

$$\begin{aligned} a * (b * c) &= a * \left( \frac{bc}{2} \right) = \frac{a(\frac{bc}{2})}{2} = \frac{abc}{4}, \\ (a * b) * c &= \left( \frac{ab}{2} \right) * c = \frac{(\frac{ab}{2})c}{2} = \frac{abc}{4}. \end{aligned}$$

As a result,  $a * (b * c) = (a * b) * c$ .

(Identity.) The element  $e = 2 \in \mathbb{Q}^+$  serves as the identity element because

$$a * 2 = \frac{(a)(2)}{2} = a \quad \text{and} \quad 2 * a = \frac{(2)(a)}{2} = a.$$

(Inverse.) For  $a \in \mathbb{Q}^+$  take  $a^{-1} = 4/a$ . Then,  $a^{-1} \in \mathbb{Q}^+$  because  $a > 0$ , and

$$a * \frac{4}{a} = \frac{(a)(\frac{4}{a})}{2} = 2 = e \quad \text{and} \quad \frac{4}{a} * a = \frac{(\frac{4}{a})(a)}{2} = 2 = e.$$

(Commutativity.) For any  $a, b \in \mathbb{Q}^+$ ,

$$a * b = \frac{ab}{2} = \frac{ba}{2} = b * a$$

because the usual multiplication of rational numbers is commutative,  $ab = ba$ .

**Question 4 (ii).**

Find all cyclic subgroups of  $D_4 = \{1, a, a^2, a^3, b, ba, ba^2, ba^3\}$  with  $a^4 = b^2 = 1$ ,  $ab = ba^3$ .

*Solution.* The cyclic subgroups of  $D_4$  are

$$\begin{aligned} \langle 1 \rangle &= \{1\}, & \langle a \rangle &= \langle a^3 \rangle = \{1, a, a^2, a^3\}, & \langle a^2 \rangle &= \{1, a^2\}, \\ \langle b \rangle &= \{1, b\}, & \langle ba \rangle &= \{1, ba\}, & \langle ba^2 \rangle &= \{1, ba^2\}, & \langle ba^3 \rangle &= \{1, ba^3\}. \end{aligned}$$