

MIDTERM SOLUTIONS

[3] 1. (a) Is  $(\mathbb{Z} - \{0\}, \cdot)$  a group? Explain. ( $\cdot$  denotes multiplication.) If it is a group, determine whether or not it is isomorphic to  $(\mathbb{Z}, +)$ .

$(\mathbb{Z} - \{0\}, \cdot)$  is not a group, because there do not always exist inverse elements. For example, since 1 is the identity element, the inverse of  $2 \in \mathbb{Z} - \{0\}$  would have to be  $1/2$  which is not an integer.

[6] (b) Is  $(\mathbb{Q} - \{0\}, \cdot)$  a group? Explain. ( $\cdot$  denotes multiplication.) If it is a group, determine whether or not it is isomorphic to  $(\mathbb{Z}, +)$ .

Yes,  $(\mathbb{Q} - \{0\}, \cdot)$  is a group.

*Closure:* The product of any two nonzero rational numbers is a nonzero rational number.

*Associativity:* Ordinary multiplication of numbers is associative.

*Identity:* 1 is the identity element and is a nonzero rational number.

*Inverses:* The inverse of any nonzero rational number  $q$  is  $1/q$ , which is also nonzero and rational.

Therefore  $(\mathbb{Q} - \{0\}, \cdot)$  is a group.

No,  $(\mathbb{Q} - \{0\}, \cdot)$  is not isomorphic to  $(\mathbb{Z}, +)$ . To prove this we could use contradiction. Suppose that  $\phi : (\mathbb{Q} - \{0\}, \cdot) \rightarrow (\mathbb{Z}, +)$  is an isomorphism. Then

$$2\phi(-1) = \phi(-1) + \phi(-1) = \phi((-1)^2) = \phi(1) = 0,$$

so  $\phi(-1) = 0$  as well, which is a contradiction since  $\phi$  must be one-to-one. [This proof amounts to observing that  $(\mathbb{Q} - \{0\}, \cdot)$  has an element of order 2 (namely  $-1$ , since  $(-1)^2 = 1$ ), while  $(\mathbb{Z}, +)$  has no element of order 2 (in fact no nonzero element of any finite order), so no isomorphism between  $(\mathbb{Q} - \{0\}, \cdot)$  and  $(\mathbb{Z}, +)$  is possible.]

Another reason why  $(\mathbb{Q} - \{0\}, \cdot)$  is not isomorphic to  $(\mathbb{Z}, +)$  is because  $(\mathbb{Q} - \{0\}, \cdot)$  is not cyclic. To see this, suppose that  $(\mathbb{Q} - \{0\}, \cdot)$  were generated by the element  $q$ . Then  $q = a/b$  for some nonzero integers  $a$  and  $b$  with  $\gcd(a, b) = 1$ . Let  $p$  be a prime which is not a divisor of either  $a$  or  $b$ . Then  $p \in \mathbb{Q} - \{0\}$ , but  $p$  cannot equal any positive or negative integer power of  $q$ , so  $q$  does not generate  $p$ . Thus  $(\mathbb{Q} - \{0\}, \cdot)$  is not cyclic, but of course  $(\mathbb{Z}, +)$  is.

[3] (c) Is  $(\mathbb{Q} - \{0\}, \div)$  a group? Explain. ( $\div$  denotes division.) If it is a group, determine whether or not it is isomorphic to  $(\mathbb{Z}, +)$ .

No,  $(\mathbb{Q} - \{0\}, \div)$  is not a group. For example, the operation  $\div$  is not associative: for example,  $(1 \div 2) \div 2 = 1/4$  while  $1 \div (2 \div 2) = 1$ .

2. Let  $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 7 & 6 & 1 & 5 & 3 \end{bmatrix}$  and  $\tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & 6 & 1 & 5 & 4 & 3 \end{bmatrix}$ .

[2] (a) Find  $\sigma\tau$  in array form.

$$\sigma\tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 5 & 4 & 1 & 6 & 7 \end{bmatrix}.$$

[4] (b) Write  $\sigma$  as a product of disjoint cycles. Is  $\sigma$  even or odd? Explain.

$\sigma = (1465)(37)$ . Since  $(1465)$  is a cycle of length 4 and is therefore a product of three transpositions,  $\sigma = (1465)(37)$  will be a product of four transpositions and therefore is even.

[5] (c) Find the subgroup  $\langle \sigma \rangle$  (of the symmetric group  $S_7$ ) generated by  $\sigma$  and write each of its elements as a product of disjoint cycles. What is the order of  $\sigma$ ?

$$\langle \sigma \rangle = \{\sigma, \sigma^2, \sigma^3, \sigma^4 = e\}, \text{ where}$$

- $\sigma = (1465)(37)$
- $\sigma^2 = (1465)(37)(1465)(37) = (16)(45)$
- $\sigma^3 = (16)(45)(1465)(37) = (1564)(37)$
- $\sigma^4 = (16)(45)(16)(45) = e$

Thus the order of  $\sigma$  is 4.

[2] (d) Find  $n$  so that  $\mathbb{Z}_n$  is isomorphic to  $\langle \sigma \rangle$ , and give an isomorphism from  $\mathbb{Z}_n$  to  $\langle \sigma \rangle$ .

Since  $\langle \sigma \rangle$  has order 4, it is isomorphic to  $\mathbb{Z}_4$ . An isomorphism is generated by  $\phi(\sigma) = 1$ , so that  $\phi(\sigma^2) = 2$ ,  $\phi(\sigma^3) = 3$ ,  $\phi(\sigma^4) = \phi(e) = 0$ .

3. Recall that the centre  $Z(G)$  of a group  $G$  is defined by:

$$Z(G) = \{a \in G \mid ag = ga \ \forall g \in G\}.$$

We know that  $Z(G)$  is a subgroup of  $G$ .

[3] (a) Prove that  $Z(G)$  is Abelian for any group  $G$ .

Let  $G$  be a group and let  $a, b \in Z(G)$  be arbitrary. Then  $ab = ba$  since  $a \in Z(G)$  and  $b \in G$  (or because  $b \in Z(G)$  and  $a \in G$ ). Therefore  $Z(G)$  is Abelian.

[4] (b) Let  $G$  be a group, and suppose that some element  $a \in G$  has order 2. Prove that for any  $g \in G$ ,  $gag^{-1}$  also has order 2.

First,

$$(gag^{-1})^2 = gag^{-1}gag^{-1} = ga(g^{-1}g)ag^{-1} = gaeag^{-1} = ga^2g^{-1} = geg^{-1} = gg^{-1} = e,$$

where  $a^2 = e$  since  $a$  has order 2. Thus  $gag^{-1}$  must have order 2 or 1. But if  $gag^{-1}$  had order 1 it would mean that  $gag^{-1} = e$ , so  $ga = g$ , so  $a = e$ , which is not true since  $a$  has order 2 and is therefore not the identity. Therefore  $gag^{-1}$  must have order 2.

[3] (c) Suppose that  $a$  is the only element of  $G$  which has order 2. Prove that  $a \in Z(G)$ .

To prove that  $a \in Z(G)$ , we need to prove that  $ag = ga$  for all  $g \in G$ . Let  $g \in G$  be arbitrary. From part (b),  $gag^{-1}$  has order 2, so  $gag^{-1} = a$  since  $a$  is the only element of  $G$  with order 2. Thus  $ga = gag^{-1}g = ag$ . Done.

[3] 4. (a) State Lagrange's Theorem.

For any finite group  $G$  and any subgroup  $H$  of  $G$ , the order of  $H$  divides into the order of  $G$ .

[2] (b) Find a subgroup of  $\mathbb{Z}_{315}$  with between 10 and 100 elements.

Since  $315 = 5 \times 63$ , we could use the subgroup  $\langle 5 \rangle = \{0, 5, 10, 15, \dots, 310\}$  generated by the element  $5 \in \mathbb{Z}_{315}$  which has order  $315/5 = 63$ . Other correct answers would be  $\langle 7 \rangle$  which has order  $315/7 = 45$ ,  $\langle 9 \rangle$  which has order  $315/9 = 35$ ,  $\langle 15 \rangle$  which has order  $315/15 = 21$ , and  $\langle 21 \rangle$  which has order  $315/21 = 15$ .

Note that  $\mathbb{Z}_{63}$  for instance is **not** a subgroup of  $\mathbb{Z}_{315}$ , because the operation in  $\mathbb{Z}_{63}$  (addition mod 63) is not the same as the operation in  $\mathbb{Z}_{315}$ : for example,  $32 + 32 = 1$  in  $\mathbb{Z}_{63}$  while  $32 + 32 = 64$  in  $\mathbb{Z}_{315}$ . However it is true that  $\mathbb{Z}_{63}$  is *isomorphic* to a subgroup of  $\mathbb{Z}_{315}$ , namely  $\mathbb{Z}_{63} \approx \langle 5 \rangle$ .