

# Homework 3

Ravi Kini

October 24, 2023

## Exercise 1

Let  $\varphi : G \rightarrow H$  be an isomorphism. For some  $g \in G$ , we first show that  $\phi(g^n) = \phi(g)^n$ . Since  $\phi(g^1) = \phi(g) = \phi(g)^1$ , the assertion clearly holds for  $n = 1$ . Assume this assertion holds for some  $n$ . Then:

$$\begin{aligned}\phi(g^{n+1}) &= \phi(g^n g) = \phi(g^n) \phi(g) \\ &= \phi(g)^n \phi(g) = \phi(g)^{n+1}\end{aligned}\tag{1}$$

By the Principle of Mathematical Induction,  $\phi(g^n) = \phi(g)^n$  for all  $n \in \mathbb{N}$ . Suppose  $\text{ord}(g) = \infty$  and  $\text{ord}(\varphi(g)) = n < \infty$ . Then:

$$\begin{aligned}\varphi(g)^n &= 1_H \\ \varphi(g^n) &= \varphi(1_G)\end{aligned}\tag{2}$$

Since  $\varphi$  is an isomorphism and therefore bijective, this means  $g^n = 1_G$ , which is a contradiction. Now suppose  $\text{ord}(g) = n < \infty$  and  $\text{ord}(\varphi(g)) = \infty$ . Then:

$$\begin{aligned}\varphi(g^n) &= \varphi(1_G) = 1_H \\ \varphi(g)^n &= \end{aligned}\tag{3}$$

This means  $\text{ord}(\varphi(g)) = n < \infty$ , which is a contradiction.  $\text{ord}(g)$  and  $\text{ord}(\varphi(g))$  are then either both finite or both infinite. If both are infinite, then  $\text{ord}(g) = \text{ord}(\varphi(g))$ . Now suppose both are finite, such that  $\text{ord}(g) = n$  and  $\text{ord}(\varphi(g)) = m$ . Then:

$$\varphi(g)^n = \varphi(g^n) = \varphi(1_G) = 1_H\tag{4}$$

Since  $m$  is the smallest positive integer such that  $\varphi(g)^m = 1_H$ ,  $m \leq n$ . Furthermore:

$$\varphi(g^m) = \varphi(g)^m = 1_H = \varphi(1_G)\tag{5}$$

Since  $\varphi$  is an isomorphism and therefore bijective, this means  $g^m = 1_G$ . Since  $n$  is the smallest positive integer such that  $g^n = 1_G$ ,  $n \leq m$ . Consequently,  $m = n$  and  $\text{ord}(g) = \text{ord}(\varphi(g))$ . In all cases,  $\text{ord}(g) = \text{ord}(\varphi(g))$ .

## Exercise 2

### Part (a)

Let  $(A, \star)$  and  $(B, \diamond)$  be groups, and let  $A \times B$  be their direct product. Let  $a_1, a_2, a_3 \in A$  and  $b_1, b_2, b_3 \in B$ . Then:

$$\begin{aligned} ((a_1, b_1) (a_2, b_2)) (a_3, b_3) &= (a_1 \star a_2, b_1 \diamond b_2) (a_3, b_3) \\ &= (a_1 \star a_2 \star a_3, b_1 \diamond b_2 \diamond b_3) \\ (a_1, b_1) ((a_2, b_2) (a_3, b_3)) &= (a_1, b_1) (a_2 \star a_3, b_2 \diamond b_3) \\ &= (a_1 \star a_2 \star a_3, b_1 \diamond b_2 \diamond b_3) \end{aligned} \tag{6}$$

Since  $((a_1, b_1) (a_2, b_2)) (a_3, b_3) = (a_1, b_1) ((a_2, b_2) (a_3, b_3))$  for all  $a_1, a_2, a_3 \in A$  and  $b_1, b_2, b_3 \in B$ , multiplication is associative.

### Part (b)

Let  $1_A$  be the identity element in  $A$  and  $1_B$  be the identity element in  $B$ . Then:

$$\begin{aligned} (a, b) (1_A, 1_B) &= (a \star 1_A, b \diamond 1_B) \\ &= (a, b) \end{aligned} \tag{7}$$

Since  $(a, b) (1_A, 1_B) = (a, b)$ , the identity element in  $A \times B$  is  $(1_A, 1_B)$ .

### Part (c)

Let  $a^{-1}$  be the inverse of  $a$  in  $A$  and  $b^{-1}$  be the inverse of  $b$  in  $B$ . Then:

$$\begin{aligned} (a, b) (a^{-1}, b^{-1}) &= (a \star a^{-1}, b \diamond b^{-1}) \\ &= (1_A, 1_B) \end{aligned} \tag{8}$$

Since  $(a, b) (a^{-1}, b^{-1}) = (1_A, 1_B)$ , the inverse of  $(a, b)$  in  $A \times B$  is  $(a^{-1}, b^{-1})$ .

## Exercise 3

### Part (a)

Let  $g$  be the generator of the cyclic group  $C_p$  and  $\varphi$  be an automorphism of  $C_p$ . Let  $\varphi(g) = g^i$ . Then, as automorphisms are a type of isomorphism and using the result found as part of Exercise 1:

$$\varphi(g^j) = \varphi(g)^j = (g^i)^j \quad (9)$$

Since  $\varphi$  is an automorphism,  $C_p = \{(g^i)^j : j \in \mathbb{Z}\}$ , which means that  $g^i$  is a generator of  $C_p$ . Evidently  $C_p$  has as many automorphisms as there are ways to map  $g$  to a generator of  $C_p$ , which is equal to the number of generators of  $C_p$ .

We assert that  $g^i$  is a generator of  $C_p$  iff  $i$  and  $p$  are relatively prime. Let  $g^i$  be a generator of  $C_p$  and suppose  $i$  and  $p$  are not relatively prime. There then exists some integer  $n > 1$  such that  $an = i$  and  $bn = p$  for  $a, b \in \mathbb{Z}$ . Then:

$$\begin{aligned} (g^i)^b &= g^{ib} = g^{anb} = g^{ap} = (g^p)^a \\ &= 1_G^a = 1_G \end{aligned} \quad (10)$$

The order of the cyclic subgroup generated by  $g^i$  is then at most  $b$ . However, since  $b < bn = p$ , the cyclic subgroup generated by  $g^i$  cannot be  $C_p$ , which has order  $p$ . Consequently,  $g^i$  cannot be a generator of  $C_p$ . This is a contradiction; therefore,  $i$  and  $p$  are relatively prime. Now let  $g^i \in C_p$  such that  $i$  and  $p$  are relatively prime. The order of the cyclic subgroup generated by  $g^i$  is obviously at most  $p$ , as otherwise  $G$  would no longer be a group. Let  $\langle g^i \rangle$  have order  $j < p$ . Then  $(g^i)^j = g^{ij}$ , which means that  $ij = kp$  for some  $k \in \mathbb{Z}$ . Since  $i$  and  $p$  are relatively prime,  $p$  must divide  $j$ . This is a contradiction, as  $j < p$ ; therefore  $\text{ord}(\langle g^i \rangle) \geq p$ . Consequently,  $\text{ord}(\langle g^i \rangle) = p$ , which means that  $g^i$  is a generator of  $C_p$ . Evidently,  $g^i$  is a generator of  $C_p$  iff  $i$  and  $p$  are relatively prime.

For prime  $p$ , there are  $p-1$  relatively prime integers less than  $p$ .  $C_p$  therefore has  $p-1$  automorphisms.

### Part (b)

From the results of Part (a), since there are 8 integers less than 24 that are relatively prime to 24, there are 8 automorphisms of  $C_{24}$ .

## Exercise 4

*Algebra* (Artin, 2e) Exercise 2.5.2

---

### Part (a)

Let  $K, H \leq G$  for some group  $G$ . Since the identity of a group is the identity of the subgroup,  $1_G$  is the identity element in both  $K$  and  $H$ , and is therefore an element of  $K \cap H$ . Let  $a, b \in K \cap H$ . Since  $a, b \in K \cap H$ ,  $a, b \in K$  and therefore, since  $K$  is a subgroup of  $G$ ,  $ab \in K$ . Similarly,  $ab \in H$ , which means  $ab \in K \cap H$ . Let  $c \in K \cap H$ . Since  $c \in K \cap H$ ,  $c \in K$  and therefore, since  $K$  is a subgroup of  $G$ ,  $c^{-1} \in K$ . Similarly,  $c^{-1} \in H$ , which means  $c^{-1} \in K \cap H$ . Since the identity, closure, and inverse properties hold,  $K \cap H$  is a subgroup of  $G$ .

### Part (b)

From Part (a), since  $K \cap H \subseteq H$  and the identity, closure, and inverse properties hold,  $K \cap H$  is a subgroup of  $H$ . Let  $k' \in K \cap H$  and  $h \in H$ . Since  $k' \in K$  and  $h \in G$ ,  $hk'h^{-1} \in K$  since  $K \trianglelefteq G$ . Furthermore, since  $k' \in H$ ,  $hk'h^{-1} \in H$  due to the closure of subgroups. Therefore  $hk'h^{-1} \in K \cap H$  and  $K \cap H \trianglelefteq H$ .

## Exercise 5

*Algebra* (Artin, 2e) Exercise 2.6.4

---

Let  $a, b \in G$  for some group  $G$ . Since  $G$  is a group,  $a^{-1}, b^{-1} \in G$ . Then:

$$\begin{aligned} a^{-1} (ab) a &= (a^{-1} a) (ba) \\ &= ba \\ b^{-1} (ba) b &= (b^{-1} b) (ab) \\ &= ab \end{aligned} \tag{11}$$

Since  $a^{-1}, b^{-1} \in G$ ,  $ba$  is the conjugate of  $ab$  by  $a^{-1}$  and  $ab$  is the conjugate of  $ba$  by  $b^{-1}$ , which means  $ab$  and  $ba$  are conjugate elements.

## Exercise 6

*Algebra (Artin, 2e) Exercise 2.8.10 (partial)*

---

Let  $H \leq G$  for some group  $G$  such that  $[G : H] = 2$ .  $H$  then has two left cosets and two right cosets in  $G$ . Let  $g \in G$ . Suppose  $g \in H$ . Then  $gH = H = Hg$ . Now suppose  $g \in G \setminus H$ . Then  $gH = G \setminus H$  since the two cosets of  $H$  partition  $G$ . Similarly,  $Hg = G \setminus H$ , which means  $gH = Hg$  for all  $g \in G$ . Consequently,  $gHg^{-1} = H$ , which means  $H \trianglelefteq G$ .