

## HOMEWORK 9

As usual  $G$  and  $H$  are assumed to be groups.

- (1) Let  $G_1, G_2$  be groups.  
(a) Show that the map

$$\begin{aligned}\pi_1 : G_1 \times G_2 &\rightarrow G_1 \\ (g_1, g_2) &\mapsto g_1\end{aligned}$$

and

$$\begin{aligned}\pi_2 : G_1 \times G_2 &\rightarrow G_2 \\ (g_1, g_2) &\mapsto g_2\end{aligned}$$

are surjective homomorphisms.

**Sol'n** We show this is true only for  $\pi_1$  since the proof for  $\pi_2$  is the same. Let  $(g_1, g_2)$  and  $(g'_1, g'_2) \in G_1 \times G_2$  be arbitrary. Then

$$(1) \quad \pi_1(g_1, g_2) \cdot \pi_1(g'_1, g'_2) = g_1 g'_1$$

and at the same time

$$(2) \quad \pi_1((g_1, g_2) \cdot (g'_1, g'_2)) = \pi_1(g_1 g'_1, g_2 g'_2) = g_1 g'_1.$$

Since (1) and (2) are equal,  $\pi_1$  is a homomorphism.

- (b) Show that  $\ker(\pi_1) \cong G_2$  and  $\ker(\pi_2) \cong G_1$ .

**Sol'n** Again, we show this only for  $\pi_1$ . We define a function  $\phi$

$$\begin{aligned}\phi : G_2 &\longrightarrow G_1 \times G_2 \\ g &\mapsto (1_{G_1}, g).\end{aligned}$$

It is trivial to verify that  $\phi$  is a one-to-one homomorphism from  $G_2$  to the kernel of  $\pi_1$ .

- (c) Conclude that  $(G_1 \times G_2)/G_2 \cong G_1$  (really we are not modding out by  $G_2$  here, but only a subgroup isomorphic to  $G_2$ ).

**Sol'n** Simply put together the previous two problems with the first homomorphism theorem (applied to  $\pi_1$ ) discussed in class.

- (2) In this problem set we show that  $D_4$  is not the direct product of two groups. Here we let  $H$  be an arbitrary proper (i.e.  $H \neq D_4$  and  $H \neq \{1\}$ ), normal subgroup of  $D_4$ .

- (a) **Sol'n** Show that  $D_4/H$  is abelian. (**hint** what is the order of such of group and what do we know about groups of this order) Such a group must have order a divisor of 8 but not 8 or 1. This leaves 2 and 4 and we already know that all such groups are abelian.

- (b) Use a problem from homework 8 to show that  $[D_4, D_4] \subset H$ .

**Sol'n** This was proven in the previous homework (more precisely it was shown that if  $G/H$  is abelian, then  $[G, G] \subset H$ .)

- (c) Show that any two proper, normal subgroups must contain the element  $a^2$  in their intersection.

**Sol'n** The previous problem showed that  $[D_4, D_4] \subset H$  for any non-trivial normal subgroup of  $D_4$ . But in the previous homework set it was shown that  $[D_4, D_4] = 1, a^2$ .

- (d) Conclude that  $D_4$  is not a non-trivial direct product of two groups.

**Sol'n** If a group  $D_4 \cong H_1 \times H_2$  then  $H_1$  and  $H_2$  would be two normal subgroups which would intersect only at the identity. This is not possible since we have just shown that both  $H_1$  and  $H_2$  must contain  $a^2$ . (A more direct proof of this uses the fact that product of two abelian groups is abelian.)

- (3) For  $H$  a normal subgroup of  $G$ , show that  $G \rightarrow G/H$  is a surjective homomorphism of groups (this is true almost by definition).

**Sol'n** Let's call the map  $\pi$ . Then for any  $g_1, g_2 \in G$  we have that  $\pi(g_1 g_2) = g_1 g_2 H = g_1 H g_2 H = \pi(g_1) \pi(g_2)$ . Thus  $\pi$  is a homomorphism. Also  $\pi$  is surjective since every element of  $G/H$  has the form  $gH$  for some  $g \in G$ . But this is simply  $\pi(g)$ .

- (4) Show that  $D_6 \cong D_3 \times \mathbb{Z}_2$ .

**Sol'n** Let  $H := \langle a^2, b \rangle = \{1, a^2, a^4, b, ba^2, ba^4\}$  and  $K := \langle a^3 \rangle = \{1, a^3\}$ . It is clear from inspection that  $H \cap K = \{1\}$ . Since  $H$  is an index 2 subgroup it is normal. Since  $K$  is contained in the center of  $D_4$  it is also normal. Lastly,  $HK = D_6$  since  $H < HK$  and the order of  $HK$  is larger than the order of  $H$ . But there is only one divisor of 12 bigger than 6, namely 12 itself (we are inspecting only divisors by LaGrange's theorem).

- (5) Show that if  $H$  is a normal subgroup of  $G$  of order 2, then  $H$  is contained in the center of  $G$ .

**Sol'n** Let  $H$  be the subgroup  $= 1_G, h$  where  $h \neq 1_G \in G$  which we assume is normal. Let  $g \in G$  be arbitrary. We need to show that  $g$  commutes with  $h$  since we already know that  $g$  commutes with  $1_G$ . Since  $H$  is assumed normal we have that  $ghg^{-1} \in H$ . But this means that  $ghg^{-1} = 1_G$  or  $ghg^{-1} = h$ . The second case clearly implies that  $g$  and  $h$  commute. Moreover the first case cannot happen since

$$\begin{aligned} ghg^{-1} = 1_G &\Rightarrow \\ gh = g &\Rightarrow \\ h = g^{-1}g = 1_G & \end{aligned}$$

- (6) Let  $T$  be a subset of  $\{1, \dots, n\}$ .

- (a) Show that the set of permutations  $\sigma \in S_n$  which satisfy  $\sigma(T) = T$  is a subgroup of  $S_n$  which we denote by  $S_T$ .

**Sol'n**

This is the usual proof using the two step subgroup test ( $S_T$  is clearly nonempty since  $\epsilon \in S_T$ ).

- Suppose that  $\sigma, \tau \in S_T$ . Then  $\sigma\tau(T) = \sigma(T) = T$  and thus  $S_T$  is closed.
- Suppose that  $\sigma \in S_T$ . Then

$$T = \sigma(T) = \sigma^{-1}\sigma(T) = \sigma^{-1}(T).$$

Thus  $\sigma^{-1} \in S_T$  and hence  $S_T$  is a subgroup of  $S_n$ .

- (b) Let  $T^c := \{1, \dots, n\} \setminus T$  (the complement of  $T$ ). Show that  $S_{T^c} = S_T$  (i.e. the two groups are equal, not just isomorphic).

**Sol'n** Let  $\sigma \in S_T$  and let  $i \in T^c$ . To show that  $\sigma \in S_{T^c}$  we must show that  $\sigma(i) \in T^c$ . By way of contradiction we assume that  $\sigma(i) \notin T^c$ . But this would mean that  $\sigma(i) \in T$ . But since  $\sigma^{-1} \in S_T$  we would have that  $\sigma^{-1}\sigma(i) \in T$  as well ( $\sigma^{-1}$  takes any element of  $T$  to a different element of  $T$  and  $\sigma(i)$  is assumed to be an element of  $T$ ). But  $\sigma^{-1}\sigma(i) = i$  and thus  $i \in T \cap T^c = \emptyset$ , a contradiction. Thus we have that  $S_T \subset S_{T^c}$  and the opposite inclusion is symmetric.

- (c) Show that  $S_T \cong S_m \times S_{n-m}$  where  $m$  is the number of elements in  $T$ . (**hint**, consider the subgroup of  $S_T$  defined as the set of permutations,  $\sigma$ , which satisfy  $\sigma(i) = i$  for every  $i \in T^c$ .)

**Sol'n**

Let  $A := \{\sigma \in S_n : \sigma(i) = i \text{ for all } i \in T^c\}$  and  $B := \{\sigma \in S_n : \sigma(i) = i \text{ for all } i \in T\}$ . Note that both  $A$  and  $B$  preserve  $T$ , so both  $A \subset S_T$  and  $B \subset S_T$  as well. Moreover  $A \cong S_m$  and  $B \cong S_{n-m}$  since  $A$  is the permutation group on  $T$  while  $B$  is the permutation group on  $T^c$ . We use the recognition theorem on  $A$  and  $B$ . That is we need to show three facts.

- $A \cap B = \{\epsilon\}$  If  $\sigma$  were in both, then  $\sigma$  would send every element of  $T$  to itself and every element of  $T^c$  to itself as well. But every element of  $\{1, \dots, n\}$  is either in  $T$  or  $T^c$  so such a  $\sigma$  would have to be the identity permutation, i.e.  $\sigma = \epsilon$ .
- $\langle A \cup B \rangle = S_T$  Any permutation which preserves  $T$  can be gotten by first permuting  $T$  (and fixing  $T^c$ ) and then permuting  $T^c$  (and fixing  $T$ ). This is exactly this statement. (One could/should make this more rigorous)
- $A, B \triangleleft S_T$  (Be careful! Neither of these are normal in  $S_n$  itself, as a matter of fact one can show that in general, ( $n > 4$ ) the only proper, normal subgroup of  $S_n$  is  $A_n$ !)

- (7) Use the fundamental theorem of finitely generated abelian groups to show that every finitely generated subgroup of  $\mathbb{Z}^n$  is isomorphic to  $\mathbb{Z}^m$  for some integer  $m$  (one can moreover show that we get the finitely generated bit for free, and that  $m \leq n$ , but this is harder).

**Sol'n** The FTOFGAG says that such a subgroup, call it  $A$ , (any finitely-generated abelian group!) would have the form  $\mathbb{Z}^m \times T$  where  $T$  is some finite abelian group (direct product of cyclic groups) and  $m$  is some non-negative integer. Now if  $T$  were non-trivial it would contain a non-identity element which would necessarily have finite order (since  $T$  is finite). Since  $T$  is (isomorphic) to a subgroup of  $A$ ,  $A$  would also contain a non-trivial element of finite order. Finally, since  $A < \mathbb{Z}^n$  by assumption the same can be said about  $\mathbb{Z}^n$ . But  $\mathbb{Z}^n$  clearly has no such element (let  $(a_1, \dots, a_n)$  be an element of order  $k$  and WAWLOG that  $a_1 \neq 0$ . Then  $k(a_1, \dots, a_n) = (ka_1, \dots, ka_n) = (0, \dots, 0) \Rightarrow ka_1 = 0$ , contradicting the fact that  $a_1 \neq 0$ ).

- (8) Suppose that  $H_1$  is a normal subgroup of  $G_1$  and  $H_2$  is a normal subgroup of  $G_2$ . Then show that  $H_1 \times H_2$  is a normal subgroup of  $G_1 \times G_2$ .

**Sol'n**

Let  $(h_1, h_2) \in H_1 \times H_2$  and let  $(g_1, g_2) \in G_1 \times G_2$ . Then since  $H_1 \triangleleft G_1$ ,  $g_1 h_1 g_1^{-1} = h'_1$  for some  $h'_1 \in H_1$  and since  $H_2 \triangleleft G_2$ ,  $g_2 h_2 g_2^{-1} = h'_2$  for some  $h'_2 \in H_2$ . Hence

$$\begin{aligned} (g_1, g_2)(h_1, h_2)(g_1, g_2)^{-1} &= (g_1, g_2)(h_1, h_2)(g_1^{-1}, g_2^{-1}) \\ &= (g_1 h_1 g_1^{-1}, g_2 h_2 g_2^{-1}) \\ &= (h'_1, h'_2) \in H_1 \times H_2 \end{aligned}$$

which implies that  $H_1 \times H_2$  is normal in  $G_1 \times G_2$  as desired.

- (9) Suppose that  $\varphi_i : G_i \rightarrow H$  ( $i = 1, 2$ ) are homomorphisms of groups. For  $\varphi := (\varphi_1, \varphi_2)$  Define

$$G_1 \times_{\varphi} G_2 := \{(g_1, g_2) \in G_1 \times G_2 : \varphi_1(g_1) = \varphi_2(g_2)\}.$$

(In parts (c)-(e) we assume that  $\varphi_1$  is surjective)

- (a) Show that  $G_1 \times_{\varphi} G_2$  is a subgroup of  $G_1 \times G_2$ .

**Sol'n** Noting that  $(1_{G_1}, 1_{G_2}) \in G_1 \times_{\varphi} G_2$  (both go to the identity of  $H$ ) we use the two step subgroup test to show that  $G_1 \times_{\varphi} G_2$  is a subgroup of  $G_1 \times G_2$ . Let  $(g_1, g_2)$  and  $(h_1, h_2)$  be elements in  $G_1 \times_{\varphi} G_2$ . Then in order for  $(g_1 h_1, g_2 h_2) \in G_1 \times_{\varphi} G_2$  we need that  $\varphi_1(g_1 h_1) = \varphi_2(g_2 h_2)$ . But

$$\begin{aligned} \varphi_1(g_1 h_1) &= \varphi_1(g_1)\varphi_1(h_1) && (\varphi_1 \text{ is a homomorphism}) \\ &= \varphi_2(g_2)\varphi_2(h_2) && (\text{Since } (g_1, h_1) \text{ and } (g_2, h_2) \in G_1 \times_{\varphi} G_2.) \\ &= \varphi_2(g_2 h_2) && (\varphi_2 \text{ is a homomorphism}). \end{aligned}$$

Now we need to show that  $(g_1^{-1}, g_2^{-1}) \in G_1 \times_{\varphi} G_2$  assuming that  $(g_1, g_2)$  is. That is we need to show that  $\varphi_1(g_1^{-1}) = \varphi_2(g_2^{-1})$  assuming that  $\varphi_1(g_1) = \varphi_2(g_2)$ .

$$\begin{aligned} \varphi_1(g_1^{-1}) &= \varphi_1(g_1)^{-1} && (\varphi_1 \text{ is a homomorphism}) \\ &= \varphi_2(g_2)^{-1} && (\text{Since } (g_1, h_1) \in G_1 \times_{\varphi} G_2) \\ &= \varphi_2(g_2^{-1}) && (\varphi_2 \text{ is a homomorphism}). \end{aligned}$$

- (b) Show that if  $G_1 \times_{\varphi} G_2 = G_1 \times G_2$  if and only if both  $\varphi_i$ 's are trivial (i.e. send every element to  $1_H$ ).

**Sol'n**

$\Rightarrow$  If  $G_1 \times_{\varphi} G_2 = G_1 \times G_2$  then for every  $g \in G_1$  we have that  $(g, 1_{G_2}) \in G_1 \times_{\varphi} G_2$ . But this means that  $\varphi_1(g) = \varphi_2(1_{G_2}) = 1_H$  for every  $g \in G_1$  which means that  $\varphi_1$  is trivial. A similar calculation shows that  $\varphi_2$  is trivial.

$\Leftarrow$  Since for every  $g_1 \in G_1$  and  $g_2 \in G_2$  we have that  $\varphi_1(g_1) = 1_H = \varphi_2(g_2)$  by assumption, we have that  $(g_1, g_2) \in G_1 \times_{\varphi} G_2$  which shows that  $G_1 \times G_2 \subset G_1 \times_{\varphi} G_2$ . The  $G_1 \times G_2 \supset G_1 \times_{\varphi} G_2$  inclusion holds by definition of  $G_1 \times_{\varphi} G_2$ .

- (c) Show that the map  $\pi_2$  from the first question in this assignment restricts to a surjective homomorphism

$$\pi_2| := \pi_2|_{G_1 \times_{\varphi} G_2}: G_1 \times_{\varphi} G_2 \longrightarrow G_2.$$

**Sol'n** Let  $g_2 \in G_2$  be arbitrary. We need to find a  $g \in G_1 \times_{\varphi} G_2$  with  $\pi_2(g) = g_2$ . Now the only thing we know about  $g_2$  is that it is in  $G_2$  and so we know that  $\varphi_2(g_2) \in H$ , and we call  $\varphi_2(g_2)$ ,  $h$ . But since  $\varphi_1$  is assumed to be surjective there exists a  $g_1 \in G_1$  so that  $\varphi_1(g_1) = h$ . But this means that  $\varphi_1(g_1) = h = \varphi_2(g_2)$ . Thus by the very definition of  $G_1 \times_{\varphi} G_2$  we know that  $(g_1, g_2) \in G_1 \times_{\varphi} G_2$ , and we call this element of  $G_1 \times_{\varphi} G_2$   $g$ . But then by definition of  $\pi_2$  we know that  $\pi_2(g) = \pi_2(g_1, g_2) = g_2$  which is what we wanted in the first place.

- (d) Show that  $\ker(\pi_2|) \cong \ker(\varphi_1)$

**Sol'n** I claim the map  $\pi_1$  restricted to the kernel of  $\pi_2$  (which we also call  $\pi_1|$ ) gives us an isomorphism

$$\ker(\pi_2|) \longrightarrow \ker(\varphi_1).$$

(This problem is not as bad as it seems as long as one keeps themselves organized! It may be helpful to draw a diagram (directed graph) in the shape of a square with the four functions we are considering as directed edges and the four groups we are considering as the vertices).

- We first need to show that the restriction of  $\pi_1$  to  $\ker(\pi_2|)$  (which we call  $\pi|$ ) actually lands inside of the intended target,  $\ker(\varphi_1)$ . What does an element of  $\ker(\pi_2|)$  actually look like? We it is an ordered pair  $(g_1, 1_{G_2})$  with  $\varphi_1(g_1) = \varphi_2(1_{G_2})$ . But since the RHS of this equation equals  $1_H$  so does the LHS. That is we know that  $\varphi_1(g_1) = 1_H$ . But this is exactly the statement that  $g_1 \in \ker(\varphi_1)$ . Finally note that  $\pi_1(g_1, 1_{G_2}) = g_1$  and this shows that  $\pi_1$  applied to any element of  $\ker(\pi_2|)$  is actually an element of  $\ker(\varphi_1)$ .
- This map,  $\pi_1|$ , is a homomorphism since it is the restriction of a homomorphism ( $\pi_1$  is a homomorphism by what you showed in the first problem of this assignment).
- We next show that the  $\pi_1|$  is one to one. We use our usual trick of showing that only the identity goes to the identity (i.e. that  $\ker(\pi_1|) = \{(1_{G_1}, 1_{G_2})\}$ ). Suppose that  $(g_1, g_2) \in \ker(\pi_1|)$  and is in the domain of  $\pi_1|$ . Then we must have that  $g_1 = 1_{G_1}$  (in the kernel of  $\pi_1$ ) and  $g_2 = 1_{G_2}$  since the domain of  $\pi_1|$  is the kernel of  $\pi_2$ .
- Lastly, we need to show that  $\pi_1|$  is surjective. We let  $g_1$  be in the codomain of  $\pi_1|$ , which is  $\ker(\varphi_1)$ . We need to find an element of  $\ker(\pi_2|)$  whose first coordinate is  $g_1$ . I claim that  $g := (g_1, 1_{G_2})$  works. We need to show that it is both an element of  $G_1 \times_{\varphi} G_2$  and an element of  $\ker(\pi_2|)$ . The second fact is clear since the second coordinate of  $g$  is the identity of  $G_2$ . The first statement is also true, because

$$\begin{aligned} \varphi_1(g_1) &= 1_H && (g_1 \in \ker(\varphi_1) \text{ by assumption}) \\ &= \varphi_2(1_{G_2}) && (\varphi_2 \text{ is a homomorphism}). \end{aligned}$$

- (e) Use Lagrange's theorem and the first homomorphism theorem to show that

$$|G_1 \times_{\varphi} G_2| = \frac{|G_1||G_2|}{|H|}.$$

**Sol'n** We have the following two facts from the first homomorphism theorem and the previous problems:

- $G_1/\ker(\varphi_1) \cong H$  (since  $\varphi_1$  is assumed to be surjective).
- $(G_1 \times_{\varphi} G_2)/\ker(\pi_2|) \cong G_2$  (since  $\pi_2|$  was proven to be surjective).

So by Lagrange's theorem, and 9d we have that

$$\frac{|G_1|}{|H|} = \frac{|G_1 \times_{\varphi} G_2|}{|G_2|}$$

and cross multiplying gives the desired formula.

- (f) Let

$$\varphi_1 := \text{sgn} : S_3 \longrightarrow \mathbb{Z}_2$$

and

$$\begin{aligned} \varphi_2 &:= \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2 \\ a \pmod 4 &\mapsto a \pmod 2 \end{aligned}$$

and define  $T := S_3 \times_{\varphi} \mathbb{Z}_4$ . Show that  $T$  is a non abelian group of order 12 which is not isomorphic to  $D_6$  or  $A_4$ . (**hint** to show it is not isomorphic to  $D_6$  show that  $T$  has an element of order 4, but  $D_6$  does not; to show it is not isomorphic to  $A_4$  show that  $T$  has an index 2 subgroup and use a previous homework problem to conclude that  $A_4$  does not).

**Sol'n**  $T$  is clearly non-abelian (we are about to show that it admits a surjective homomorphism onto a non-abelian group). Moreover the formula derived in part (9e) shows that  $T$  has order 12.

Since  $\varphi_1(123) = 0 \pmod 2 = \varphi_2(2 \pmod 4)$  we know that  $((123), 2 \pmod 4) \in T$ . Moreover,

$$|((123), 2 \pmod 4)| = \text{lcm}(|(123)|, |2 \pmod 4|) = \text{lcm}(3, 2) = 6.$$

But in the previous homework assignment, you showed that  $A_4$  contains no subgroup of order 6, so in particular it can not contain an element of order 6. Thus  $T$  and  $A_4$  are not isomorphic.

Now since  $\varphi_1(12) = 1 \pmod 2 = \varphi_2(1 \pmod 4)$  we know that  $((12), 1 \pmod 4) \in T$ . A similar calculation to the one done above shows that this element has order 4. On the other hand, every element of  $D_6$  is either in  $\langle a \rangle \cong \mathbb{Z}_6$  or it is a reflection (and hence has order 2). Thus  $D_6$  only contains elements of order 1, 2, 3 or 6 and not 4 and so  $D_6$  and  $T$  can not be isomorphic.

- (g) Show that  $T$  from the previous problem does not contain a subgroup isomorphic to  $S_3$  (count the number of elements of order 2!) but it does have a quotient isomorphic to  $S_3$ .

**Sol'n**

For completeness let us write down the 12 elements of  $T$  along with their order (we omit the  $\pmod 4$  everywhere to make things look a bit neater).

element	$(\epsilon, 0)$	$(\epsilon, 2)$	$((123), 0)$	$((123), 2)$	$((132), 0)$	$((132), 2)$
order	1	2	3	6	3	6
element	$((12), 1)$	$((12), 3)$	$((13), 1)$	$((13), 3)$	$((23), 1)$	$((23), 3)$
order	4	4	4	4	4	4

Now inspection of the table(s) tell(s) us that  $T$  has only 1 element of order 2. However if  $T$  contained  $S_3$  (which has 3 elements of order 2), then  $T$  would need to contain at least 3 elements of order 2. Thus  $T$  does not contain a subgroup isomorphic to  $S_3$ .

Since  $\varphi_2$  is surjective, we get from problem 9c that  $\pi_1$  restricts to a surjective homomorphism from  $T$  to  $S_3$  (in that problem we actually showed this for  $\pi_2$  and  $\varphi_1$ , but the proof in this case is obviously symmetric).

(10) Show that

**Sol'n** What is this “that” of which I speak?

(11) Suppose that  $H$  and  $K$  are normal subgroups of  $G$ . Show that

$$HK/H \cong K/H \cap K.$$

(**hint**, define a map from  $K$  to  $HK/H$  by sending  $k \in K$  to  $kH \in HK/H$ . Then show its surjective and compute its kernel).

**Sol'n** We call the map defined in the hint (what else?!)  $\varphi$ . Now  $\varphi$  is the composition of homomorphisms, and so it is an homomorphism. We first compute the kernel. Now

$$\varphi(k) = H \quad (H = 1_{HK/H})$$

if and only if  $k \in H$ . Hence since we started with the fact that  $k \in K$ , we know that  $k \in \ker(\varphi)$  if and only if  $k \in H \cap K$ . It remains only to show that  $\varphi$  is surjective. To that end let  $g \in HK$ . Then  $g = hk$  for some  $h \in H$  and  $k \in K$ . But then  $gH = hkH = Hhk = Hk = kH = \varphi(k)$  and thus  $\varphi$  is surjective.

(12) As a corollary of the previous problem, show that for any two integers  $n$  and  $m$ , that  $nm = \text{lcm}(n, m)\text{gcd}(n, m)$  (hint, take  $H = n\mathbb{Z}$  and  $K = m\mathbb{Z}$  and compute the orders of both sides of the isomorphism in the previous problem).

**Sol'n** Written in additive notation the previous problem says that

$$(3) \quad (n\mathbb{Z} + m\mathbb{Z})/m\mathbb{Z} \cong n\mathbb{Z}/(m\mathbb{Z} \cap n\mathbb{Z}).$$

Moreover, we have previously shown (in lecture) that  $(n\mathbb{Z} + m\mathbb{Z}) = \text{gcd}(n, m)\mathbb{Z}$  and that (in a quiz)  $(n\mathbb{Z} \cap m\mathbb{Z}) = \text{lcm}(n, m)\mathbb{Z}$ . Thus (3) reduces to

$$(4) \quad \text{gcd}(n, m)\mathbb{Z}/m\mathbb{Z} \cong n\mathbb{Z}/\text{lcm}(n, m)\mathbb{Z}.$$

Now we have that the index of  $m\mathbb{Z}$  in  $\mathbb{Z}$  is  $m$  and the index of  $\text{gcd}(n, m)\mathbb{Z}$  in  $\mathbb{Z}$  is  $\text{gcd}(n, m)$ . Thus since  $m\mathbb{Z} < \text{gcd}(n, m)\mathbb{Z}$  and by multiplicativity (if  $K < H < G$ , then  $[G : K] = [G : H][H : K]$ ) of the index, we have that the LHS of (4) has order  $m/\text{gcd}(n, m)$  and similarly the RHS has order  $\text{lcm}(n, m)/n$  and cross-multiplying gives the desired result.