

## Solutions to Extra Practice Problems for Midterm Exam 2

• Find the order and the parity (even or odd) of each of the following elements of  $S_8$ :

(a):  $\sigma = (1, 4, 3)(3, 5)(2, 7, 5)(1, 6, 2, 4, 7)$

(b):  $\sigma = (3, 6, 4)(1, 5, 2, 4)(1, 6, 5, 3, 2)$

(c):  $\sigma$ ,  $\tau$ , and  $\sigma\tau$ , where  $\sigma = (1, 2, 3)(4, 5, 6)$  and  $\tau = (2, 7, 8, 5)(3, 4)$

**Solutions.** (a): Simplifying,  $\sigma = (1, 6, 7, 4)(2, 3, 5)$ , a disjoint 4-cycle and 3-cycle.

Thus,  $o(\sigma) = \text{lcm}(4, 3) = 12$  The 4-cycle is odd, and the 3-cycle is even, so adding gives  $\sigma$  is odd

(b): Simplifying,  $\sigma = (1, 4)(2, 5, 6)$ , a disjoint 2-cycle and 3-cycle. Thus,  $o(\sigma) = \text{lcm}(2, 3) = 6$

The 2-cycle is odd, and the 3-cycle is even, so adding gives  $\sigma$  is odd

(c):  $\sigma$  is two disjoint 3-cycles, so  $o(\sigma) = \text{lcm}(3, 3) = 3$  and since each cycle is even,  $\sigma$  is even

$\tau$  is a disjoint 4-cycle and 2-cycle, so  $o(\tau) = \text{lcm}(4, 2) = 4$  and since each cycle is odd,  $\tau$  is even

Simplifying,  $\sigma\tau = (1, 2, 7, 8, 6, 4)(3, 5)$ , a disjoint 6-cycle and 2-cycle. Thus,  $o(\sigma\tau) = \text{lcm}(6, 2) = 6$

Both cycles are odd, so  $\sigma\tau$  is even

[**Alternative for last step of (c):** Since we already saw that  $\sigma$  and  $\tau$  are both even, we have  $\sigma\tau$  is even + even = even.]

• In each part (a), (b), (c) of the previous problem, and for each  $k = 1, 2, 3, 4, 5, 6$ , find the parity (even or odd) of  $g_k\sigma$  and  $f_k\sigma$ , where  $f_k = (7, k)$  and  $g_k = (7, k, 8)$ .

**Solutions.** Every  $f_k$  is a 2-cycle and hence is odd; every  $g_k$  is a 3-cycle and hence even. Thus:

(a):  $\sigma f_k$  is odd + odd = even and  $\sigma g_k$  is odd + even = odd for every  $k$ .

(b):  $\sigma f_k$  is odd + odd = even and  $\sigma g_k$  is odd + even = odd for every  $k$ .

(a):  $\sigma f_k$  is even + odd = odd and  $\sigma g_k$  is even + even = even for every  $k$ .

Saracino #8.24: Let  $G$  be a group, and let  $H, K \subseteq G$  be subgroups. Let

$$HK = \{hk \mid h \in H, k \in K\}.$$

For  $G = S_3$ , find subgroups  $H, K \subseteq S_3$  such that  $HK$  is **not** a subgroup of  $S_3$ .

**Solution.** Let  $H = \langle(1, 2)\rangle = \{e, (1, 2)\}$  and  $K = \langle(1, 3)\rangle = \{e, (1, 3)\}$ . Then

$$HK = \{ee, (1, 2)e, e(1, 3), (1, 2)(1, 3)\} = \{e, (1, 2), (1, 3), (1, 3, 2)\},$$

which cannot be a subgroup of  $S_3$  because it has 4 elements, and  $4 \nmid 6$ , so  $S_3$ , which has  $|S_3| = 6$ , cannot have a subgroup of order 4, by Lagrange. QED

[Alternatively, you can check that  $HK$  is not closed under products, as  $(1, 3)(1, 2) = (1, 2, 3) \notin HK$ . It's also not closed under inverses, since  $(1, 3, 2)^{-1} = (1, 2, 3) \notin HK$ .]

Saracino #8.25: Let  $n \geq 3$ . Prove that if  $n$  is odd, then  $Z(D_n) = \{e\}$ , and if  $n$  is even, then  $|Z(D_n)| = 2$ .

**Proof. Odd case:** For any  $i = 1, \dots, n-1$ , observe that  $n \nmid i$ , and therefore, since  $n$  is odd, we also have  $n \nmid 2i$ . Therefore, since  $o(f) = n$ , we have  $f^{2i} \neq e$ , and hence  $f^i \neq f^{-i}$ . Thus,

$$gf^i = f^{-i}g \neq f^i g.$$

That is,  $g$  and  $f^i$  do not commute with one another, so  $f^i \notin Z(D_n)$ .

In addition, for any  $j = 0, \dots, n-1$ , we have

$$(f^j g)(f) = f^j f^{-1} g = f^{j-1} g \neq f^{j+1} g = f(f^j g),$$

where the inequality is because  $f^2 \neq e$ , since  $o(f) = n \geq 3$ . Thus,  $f^j g \notin Z(D_n)$ .

We have shown that none of the non-identity elements of  $D_n$  lie in the center, but  $e$  certainly does, since the identity commutes with everything. Thus,  $Z(D_n) = \{e\}$  QED Odd case

**Even case:** Write  $n = 2m$ . For any  $i = 1, \dots, m - 1$ , we have  $n \nmid 2i$ , since  $2 \leq 2i < n$ .

For any  $i = m + 1, \dots, n - 1$ , we also have  $n \nmid 2i$ , since  $n + 2 \leq 2i < 2n$ .

That is, for any  $i = 1, \dots, n - 1$  with  $i \neq m$ , we have  $n \nmid 2i$ . Therefore, for any such  $i$ , we have

$$gf^i = f^{-i}g \neq f^i g.$$

That is,  $g$  and  $f^i$  do not commute with one another, so  $f^i \notin Z(D_n)$ .

In addition, for any  $j = 0, \dots, n - 1$ , we have

$$(f^j g)(f) = f^j f^{-1}g = f^{j-1}g \neq f^{j+1}g = f(f^j g),$$

where the inequality is because  $f^2 \neq e$ , since  $o(f) = n \geq 3$ . Thus,  $f^j g \notin Z(D_n)$ .

Having eliminated all elements of  $D_n$  besides  $f^m$  and  $e$ , we have  $Z(D_n) \subseteq \{e, f^m\}$ . We claim the reverse inclusion also holds, in which case we will be done. Clearly  $e$  lies in the center, so it remains to show  $f^m \in Z(D_n)$ .

For any  $i \in \mathbb{Z}$ , we have  $f^i f^m = f^{i+m} = f^{m+i} = f^m f^i$ , and also

$$(f^i g)f^m = f^i f^{-m}g = f^{i-m}g = f^{i+m}g = f^m(f^i g),$$

where the third equality is because  $e = f^n = f^{2m}$ . Thus, we have shown  $f^m$  commutes with every element of  $D_n$ , so that  $f^m \in Z(D_n)$ , as desired. That is,  $Z(D_n) = \{e, f^m\}$  has two elements. QED Even case

Saracino #9.7: Find the right cosets of  $H = \{(0, 0), (1, 0), (2, 0)\}$  in  $C_3 \times C_2$ .

**Solution.** The full group  $G = C_3 \times C_2$  has  $3 \cdot 2 = 6$  elements, and this subgroup  $H = \langle(1, 0)\rangle$  has 3 elements.

We have  $H + (0, 0) = H$ , and we compute  $H + (0, 1) = \{(0, 1), (1, 1), (2, 1)\}$ , giving the other three elements of  $G$ . Thus, the (two) right cosets of  $H$  are

$$H + (0, 0) = \{(0, 0), (1, 0), (2, 0)\} \text{ and } H + (0, 1) = \{(0, 1), (1, 1), (2, 1)\}$$

Saracino #9.13: Let  $G$  be a group, and let  $A, B \subseteq G$  be subgroups. Define a relation  $R$  on  $G$  by

$$x R y \text{ iff } \exists a \in A \text{ and } b \in B \text{ such that } x = ayb$$

Prove that  $R$  is an equivalence relation on  $G$ .

**Proof. (Ref1):** Given  $x \in G$ , we have  $e \in A$  and  $e \in B$ , so because  $x = exe$ , we have  $x R x$ .

**(Symm):** Given  $x, y \in G$  such that  $x R y$ , we have  $x = ayb$  for some  $a \in A$  and  $b \in B$ . But then  $a^{-1} \in A$  and  $b^{-1} \in B$ , and we have  $y = a^{-1}xb^{-1}$ . Thus,  $y R x$ .

**(Trans):** Given  $x, y, z \in G$  such that  $x R y$  and  $y R z$ , we have  $x = ayb$  and  $y = a'zb'$  for some  $a, a' \in A$  and  $b, b' \in B$ .

Then  $aa' \in A$  and  $b'b \in B$ , so  $x = ayb = aa'zb'b$ , so that  $x R z$ . QED

Saracino #9.14: Let  $G$  be a group. Define a relation  $R$  on  $G$  by:  $a R b$  means  $ab = ba$ . Decide for which groups  $R$  is an equivalence relation on  $G$ .

**Answer/Proof.** We claim that  $R$  is an equivalence relation on  $G$  if and only if  $G$  is abelian.

**( $\Rightarrow$ ):** Given  $x, y \in G$ , observe that  $x R e$  because  $xe = x = ex$ , and that  $e R y$  because  $ey = y = ye$ . Because  $R$  is transitive, it follows that  $x R y$ , which means  $xy = yx$ . QED ( $\Rightarrow$ )

**( $\Leftarrow$ ): (Ref1):** Given  $g \in G$ , we have  $gg = gg$ , so that  $g R g$ .

**(Symm):** Given  $x, y \in G$  such that  $x R y$ , we have  $xy = yx$ . Therefore,  $yx = xy$ , i.e.,  $y R x$ .

**(Trans):** Given  $x, y, z \in G$  such that  $x R y$  and  $y R z$ , then [ignoring those assumptions] we have  $xz = zx$  since  $G$  is abelian, and hence  $x R z$ . QED

**[Note:** In this case, then entire set  $G$  is a single equivalence class; everything is equivalent to everything else. So this relation  $R$  is either *not* an equivalence relation (when  $G$  is not abelian), or else a very boring equivalence relation (where *everything* is related to everything else, when  $G$  is abelian).]

---

Saracino #10.2(a): Find  $[G : H]$  where  $G = C_{48}$  and  $H = \langle 32 \rangle$ .

**Solution.** By a couple of old results,  $|H| = o(32) = 48/(32, 48) = 48/16 = 3$ . Therefore, by Lagrange,

$$[G : H] = |G|/|H| = 48/3 = 16$$

---

Saracino #10.3(a): Find  $[G : H]$  for  $G = C_6 \times C_4$  and  $H = \{0\} \times C_4$ .

**Solution.** We have  $|G| = 6 \cdot 4 = 24$  and  $|H| = 1 \cdot 4 = 4$ . Therefore, by Lagrange,

$$[G : H] = |G|/|H| = 24/4 = 6$$

---

Saracino #10.7: Let  $p$  and  $q$  be prime numbers, and let  $G$  be a group of order  $pq$ . Prove that every proper subgroup of  $G$  is cyclic.

**Proof.** Given  $H \subseteq G$  a proper subgroup, let  $m = |H|$ . Then by Lagrange, we have  $m|pq$ , and hence  $m$  is one of  $1, p, q, pq$ .

If  $m = pq$ , then  $|H| = |G|$ , so since  $H \subseteq G$  and  $G$  is finite, we have  $H = G$ , contradicting our assumption. Thus,  $m$  is one of  $1, p, q$ .

If  $m = 1$ , then  $H = \{e\}$  is trivial and hence cyclic (generated by  $e$ ).

If  $m = p$  or  $m = q$ , then  $|H|$  is prime, so by a corollary to Lagrange,  $H$  is cyclic. QED

---

Saracino #10.9: Let  $G$  be a group, let  $H, K \subseteq G$  be subgroups, and suppose that  $|H| = 39$  and  $|K| = 65$ . Prove that  $H \cap K$  is cyclic.

**Proof.** We know from an old homework that  $H \cap K$  is a subgroup of  $G$  and hence, being contained in  $H$  and in  $K$ , is also a subgroup of both  $H$  and  $K$ .

Let  $m = |H \cap K|$ . By Lagrange applied to  $H \cap K \subseteq H$ , we have  $m|39$ . By Lagrange applied to  $H \cap K \subseteq K$ , we have  $m|65$ . Thus,  $m|(39, 65)$ , i.e.,  $m|13$ . So either  $m = 1$  or  $m = 13$ .

If  $m = 1$ , then  $H \cap K = \{e\} = \langle e \rangle$  is cyclic.

If  $m = 13$ , then because 13 is prime, we have that  $H \cap K$  is cyclic by a corollary to Lagrange. QED

---

Saracino #11.4: Let  $H \triangleleft G$  and  $K \triangleleft G$ . Prove that  $H \cap K \triangleleft G$ .

**Proof.** We already know  $H \cap K$  is a subgroup of  $G$ , from some old homework.

Given  $x \in H \cap K$  and  $g \in G$ , we have  $g x g^{-1} \in H$  since  $x \in H$  and  $H \triangleleft G$ . We also have  $g x g^{-1} \in K$  since  $x \in K$  and  $K \triangleleft G$ . Thus,  $g x g^{-1} \in H \cap K$ . QED

---

Saracino #11.7: Let  $H \triangleleft G$  and  $K \triangleleft G$ , and assume that  $H \cap K = \{e\}$ . Prove that for any  $x \in H$  and  $y \in K$ , we have  $xy = yx$ .

**Proof.** Given  $x \in H$  and  $y \in K$ , let  $g = xyx^{-1}y^{-1}$ . We will show that  $g \in H \cap K$ .

Indeed,  $yx^{-1}y^{-1} \in H$  because  $x^{-1} \in H$  and  $y \in G$ , with  $H \triangleleft G$ . Therefore,  $g = x(yx^{-1}y^{-1}) \in H$  because it is a product of two elements of  $H$ .

Similarly,  $xyx^{-1} \in K$  because  $y \in K$  and  $x \in G$ , with  $K \triangleleft G$ . Because  $y^{-1} \in K$ , we have that  $g = (xyx^{-1})y^{-1}$  is a product of two elements of  $K$  and hence lies in  $K$ .

Because  $g \in H \cap K$ , we have  $g = e$ , i.e.,  $xyx^{-1}y^{-1} = e$ , so that  $xy = yx$ . QED

---

Saracino #11.9: Recall from Exercise 11.8 that for subgroups  $H, N \subseteq G$  with  $N \triangleleft G$ , you proved that the subset  $NH = \{nh \mid n \in N, h \in H\}$  is a subgroup of  $G$ . Suppose further that  $H \triangleleft G$ . Prove that  $NH$  is also normal in  $G$ .

**Proof.** We already know  $NH$  is a subgroup of  $G$ . Given  $nh \in NH$  (i.e., with  $n \in N$  and  $h \in H$ ), and given  $g \in G$ , we have

$$g(nh)g^{-1} = (gng^{-1})(ghg^{-1}) \in NH,$$

because  $gng^{-1} \in N$  and  $ghg^{-1} \in H$ , because both subgroups are normal in  $G$ . QED

---

Saracino #11.13: Suppose that  $A \triangleleft G$  and  $B \triangleleft H$ . Prove that  $A \times B \triangleleft G \times H$ .

**Proof.** Given  $(a, b) \in A \times B$  and  $(g, h) \in G \times H$ , we have

$$(g, h)(a, b)(g, h)^{-1} = (gag^{-1}, hbh^{-1}) \in A \times B,$$

where the inclusion is because  $gag^{-1} \in A$  since  $A \triangleleft G$ , and because  $hbh^{-1} \in A$  since  $B \triangleleft H$ . QED

Saracino #11.14(a): Let  $G = C_{12} \times C_{12}$  and  $H = \langle (2, 2) \rangle$ . Find the order of the element  $H + (5, 8)$  in  $G/H$ .

**Proof.** We have  $H = \{(0, 0), (2, 2), (4, 4), (6, 6), (8, 8), (10, 10)\}$ . The order of  $H + (5, 8)$  is the smallest positive integer  $n$  such that  $H + n(5, 8) = H + (0, 0)$ , i.e., such that  $n(5, 8) \in H$ . We compute:

$$2(5, 8) = (10, 4), \quad 3(5, 8) = (3, 0), \quad 4(5, 8) = (8, 8) \in H.$$

Thus,  $o(H + (5, 8)) = 4$  in  $G/H$ . QED

Saracino #11.14(b): With  $G$  and  $H$  as in the previous problem, is  $G/H$  cyclic?

**Answer/Proof.** NO,  $G/H$  is not cyclic

We have  $|G| = 12 \cdot 12$  and  $|H| = 6$ , so by Lagrange,  $|G/H| = |G|/|H| = 12 \cdot 2 = 24$ . If  $G/H$  were cyclic, then  $G/H$  would have an element of order 24. It suffices to show that no such element exists.

Given an arbitrary  $H + a \in G/H$ , the element  $a \in G$  is of the form  $a = (x, y)$  with  $x, y \in C_{12}$ . Thus,  $12a = (12x, 12y) = (0, 0)$  is the identity element of  $G$ . Therefore,  $12(H + a) = H + (12a) = H + (0, 0)$  is the identity element of  $G/H$ . Hence,  $H + a$  has order at most 12, so  $o(H + a) \neq 24$ . QED

Saracino #11.21: Let  $G$  be an abelian group, and let  $H$  be the subgroup consisting of all elements of  $G$  that have finite order. [Note from RLB: you may take my word for it that  $H$  is indeed a subgroup of  $G$ .] Prove that every non-identity element of  $G/H$  has infinite order.

**Proof.** Given an arbitrary element  $Ha \in G/H$ , i.e., the coset containing some  $a \in G$ , suppose that  $Ha$  has finite order. It suffices to show that  $Ha$  is the identity element of  $G/H$ .

By our supposition, there is a positive integer  $n \geq 1$  such that  $(Ha)^n = He$ , i.e.,  $Ha^n = He$ , i.e.,  $a^n = a^n e^{-1} \in H$ .

By definition of  $H$ , then, the element  $a^n$  has finite order, so there is some  $m \geq 1$  such that  $(a^n)^m = e$ , i.e.,  $a^{mn} = e$ . But then  $a$  itself has finite order, so that  $a \in H$ . Therefore,  $ae^{-1} = a \in H$ , so that  $Ha = He$  is the identity element of  $G/H$ . QED

[**Note:** You may have noticed that we didn't seem to use the hypothesis that  $G$  is abelian. Well, actually, that fact is needed to show the part I said you could take my word for, that  $H$  itself, the set of elements of finite order, is a subgroup.]

Saracino #11.23: Let  $G$  be a group, and let  $H$  be a subgroup of index 2. Prove that for every  $a \in G$ , we have  $a^2 \in H$ .

**Proof.** By a theorem, we have  $H \triangleleft G$  because  $[G : H] = 2$ . Thus,  $G/H$  is defined and is a group of order  $[G : H] = 2$ .

Given  $a \in G$ , the coset  $Ha \in G/H$  has  $(Ha)^2 = He$  by a corollary to Lagrange because  $G/H$  is a group of order 2 with identity element  $He$ . That is,  $Ha^2 = He$ , which means  $a^2 = a^2 e^{-1} \in H$ . QED

Saracino #11.28: Let  $G$  be a group and let  $N \triangleleft G$ . Assume that  $N$  is cyclic. Prove that every subgroup of  $N$  is normal in  $G$ .

**Proof.** Let  $a$  be a generator for  $N$ . Let  $H$  be a subgroup of  $N$ . By an old theorem, we have that  $H$  is also cyclic, and specifically,  $H = \langle a^n \rangle$  for some integer  $n \in \mathbb{Z}$ .

Given  $g \in G$  and  $h \in H$ , there is an integer  $m \in \mathbb{Z}$  such that  $h = (a^n)^m$ , i.e.,  $h = a^{mn}$ . In addition, since  $N \triangleleft G$ , we have  $gag^{-1} \in N$ , so there is some integer  $k \in \mathbb{Z}$  such that  $gag^{-1} = a^k$ . Thus,

$$ghg^{-1} = ga^{mn}g^{-1} = (gag^{-1})^{mn} = (a^k)^{mn} = a^{kmn} = (a^n)^{km} \in H$$

where the final inclusion is because  $H$  is generated by  $a^n$  and  $km \in \mathbb{Z}$ . QED

Saracino #12.2: Define  $\varphi : G \rightarrow G$  by  $\varphi(x) = x^{-1}$ . If  $G$  is abelian, prove that  $\varphi$  is an automorphism of  $G$ . If  $G$  is not abelian, prove that  $\varphi$  is *not* a homomorphism.

**Proof.** For any group  $G$ , we note that  $\varphi$  is one-to-one and onto, as follows:

**1-1:** Given  $x, y \in G$  with  $\varphi(x) = \varphi(y)$ , we have  $x^{-1} = y^{-1}$ , so taking inverses of both sides, we get  $x = y$ .  
QED 1-1

**Onto:** Given  $y \in G$ , let  $x = y^{-1} \in G$ . Then  $\varphi(x) = x^{-1} = y$ . QED Onto

It remains to check whether  $\varphi$  is a homomorphism:

**Abelian case.** For  $G$  abelian, then given  $x, y \in G$ , we have

$$\varphi(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \varphi(x)\varphi(y),$$

proving that  $\varphi$  is a homomorphism, and hence (since it is bijective) an isomorphism in this case.

**Non-abelian case.** For  $G$  non-abelian, there exist  $a, b \in G$  with  $ab \neq ba$ . Let  $x = a^{-1}$  and  $y = b^{-1}$ . Then

$$\varphi(xy) = (xy)^{-1} = y^{-1}x^{-1} = ba \neq ab = x^{-1}y^{-1} = \varphi(x)\varphi(y),$$

which shows that  $\varphi$  is *not* a homomorphism in this case. QED

Saracino #12.4(e): Determine whether  $C_3 \times C_3$  and  $C_9$  are isomorphic.

**Answer/Proof.** NO, not isomorphic

$C_9$  is cyclic, but by an earlier theorem,  $C_3 \times C_3$  is not cyclic, since  $\gcd(3, 3) = 3 \neq 1$ . However, any group isomorphic to a cyclic group must be cyclic, so  $C_9$  cannot be isomorphic to  $C_3 \times C_3$  QED

Saracino #12.4(k): Determine whether  $D_3 \times C_4$  and  $D_4 \times C_3$  are isomorphic.

**Answer/Proof.** NO, not isomorphic

Let  $G = D_3 \times C_4$  and  $H = D_4 \times C_3$ . Let's find all the elements of order 6 in each.

Consider  $G$ . For any  $x \in D_3$ , the order of  $x$  is one of 1, 2, 3, so the order of  $(x, 0) \in G$  is  $\text{lcm}(o(x), 1) = o(x) \neq 6$ . Similarly, since 1 and 3 have order 4 in  $C_4$ , the order of  $(x, 1) \in G$  is  $\text{lcm}(o(x), 4)$  is divisible by 4 and hence does not equal 6. Lastly, the order of  $(x, 2) \in G$  is  $\text{lcm}(o(x), 2)$ , which is 6 if and only if  $o(x) = 3$ , which happens exactly when  $x = f$  or  $x = f^2$ . Thus,  $G$  has exactly two elements of order 6, namely  $(f, 2)$  and  $(f^2, 2)$ .

Consider  $H$ . Note that  $D_4$  has five elements of order 4, namely the  $180^\circ$  rotation  $f^2$ , and the four flips  $f^i g$  for  $i = 0, 1, 2, 3$ . In addition,  $C_3$  has two elements of order 3, namely 1 and 2. Thus,  $H$  has  $5 \cdot 2 = 10$  elements of order 6, namely each element of the form  $(x, j)$  where  $x \in D_4$  is one of the elements of order 2, and  $j$  is 1 or 2.

If the two groups were isomorphic, then there would be an isomorphism  $\varphi : H \rightarrow G$ . Because  $\varphi$  is 1-1, the ten elements of  $H$  of order 6 would map to ten different elements of  $G$ , and because isomorphisms preserve order of elements, each of these ten elements of  $G$  would have order 6. But  $G$  has only two elements of order 6, a contradiction. Thus, the groups are not isomorphic. QED

Saracino #12.7: Suppose  $A \cong G$  and  $B \cong H$ . Prove that  $A \times B \cong G \times H$ .

**Proof.** By hypothesis, there are isomorphisms  $\varphi : A \rightarrow G$  and  $\psi : B \rightarrow H$ . Define  $\Phi : A \times B \rightarrow G \times H$  by  $\Phi(a, b) = (\varphi(a), \psi(b)) \in G \times H$ .

**Homom:** Given  $(a_1, b_1), (a_2, b_2) \in A \times B$ , we have

$$\begin{aligned} \Phi((a_1, b_1)(a_2, b_2)) &= \Phi(a_1 a_2, b_1 b_2) = (\varphi(a_1 a_2), \psi(b_1 b_2)) = (\varphi(a_1)\varphi(a_2), \psi(b_1)\psi(b_2)) = \\ &= (\varphi(a_1), \psi(b_1))(\varphi(a_2), \psi(b_2)) = \Phi((a_1, b_1))\Phi((a_2, b_2)) \end{aligned}$$

**1-1:** Given  $(a_1, b_1), (a_2, b_2) \in A \times B$  such that  $\Phi((a_1, b_1)) = \Phi((a_2, b_2))$ , we have  $(\varphi(a_1), \psi(b_1)) = (\varphi(a_2), \psi(b_2))$ .

Thus,  $\varphi(a_1) = \varphi(a_2)$  and  $\psi(b_1) = \psi(b_2)$ . Since  $\varphi$  and  $\psi$  are 1-1, we have  $a_1 = a_2$  and  $b_1 = b_2$ , so  $(a_1, b_1) = (a_2, b_2)$ .

**Onto:** Given  $(g, h) \in G \times H$ , there exist  $a \in A$  and  $b \in B$  such that  $\varphi(a) = g$  and  $\psi(b) = h$ , since  $\varphi$  and  $\psi$  are onto. Thus,  $\Phi((a, b)) = (\varphi(a), \psi(b)) = (g, h)$ . QED

Saracino #12.8: Is  $C_{14}$  isomorphic to a subgroup of  $C_{35}$ ? Of  $C_{56}$ ?

**Solution.** NO,  $C_{14}$  is not isomorphic to a subgroup of  $C_{35}$

If it were, then the subgroup  $H$  of  $C_{35}$  would have  $|H| = |C_{14}| = 14$ . But  $|C_{35}| = 35$  and  $14 \nmid 35$ , so by Lagrange's Theorem,  $C_{35}$  has no subgroup of order 14.

YES,  $C_{14}$  is isomorphic to a subgroup of  $C_{56}$

Since  $56 = 14 \cdot 4$ , note that  $H = \langle 4 \rangle$  is a cyclic subgroup of  $C_{56}$ , and by an old theorem, its order is  $56/(4, 56) = 56/4 = 14$ . By a recent theorem (Theorem 12.2), since the groups  $C_{14}$  and  $H$  are both cyclic of order 14, they are isomorphic. QED

Saracino #12.20(a): Let  $G$  be a finite abelian group, and let  $n$  be a positive integer relatively prime to  $|G|$ . Let  $\varphi : G \rightarrow G$  by  $\varphi(x) = x^n$ . Show that  $\varphi$  is an isomorphism from  $G$  to  $G$ .

**Proof.** Let  $m = |G|$ . Since  $(m, n) = 1$ , there are integers  $a, b \in \mathbb{Z}$  such that  $am + bn = 1$ .

**Homom:** Given  $x, y \in G$ , then  $\varphi(xy) = (xy)^n = x^n y^n = \varphi(x)\varphi(y)$ .

**1-1:** Given  $x, y \in G$  such that  $\varphi(x) = \varphi(y)$ , we have  $x^n = y^n$ . In addition, by Lagrange, we have  $x^m = e$  and  $y^m = e$ . Therefore,

$$x = x^{am+bn} = (x^m)^a (x^n)^b = e^a (x^n)^b = (y^m)^a (y^n)^b = y^{am+bn} = y$$

**Onto:** We have that  $\varphi$  is a one-to-one function from the finite set  $G$  to itself. By the pigeonhole principle, it is also onto. QED