

## Homework 5 Solutions

- (1) Suppose that  $X_1$  and  $X_2$  have the same number of elements (that is there exists a bijection from  $X_1$  to  $X_2$ ). Show that  $\text{Bij}(X_1)$  and  $\text{Bij}(X_2)$  are isomorphic. (**hint** If  $F$  is a bijection from  $X_1$  to  $X_2$  we want to take the function which takes  $x_1$  to  $x'_1$  to the function which takes  $F(x_1)$  to  $F(x'_1)$ . How did we do this for symmetric groups?) (this should be intuitive ... the ways one can permute a set a should not depend on what you call the elements of the set).

SOLUTION. Since  $X_1$  and  $X_2$  have the same number of elements there is a bijection

$$F : X_1 \longrightarrow X_2.$$

Associated to  $F$  we assign a function

$$F_* : \text{Bij}(X_1) \longrightarrow \text{Bij}(X_2)$$

defined by  $F_*(\sigma) := F \circ \sigma \circ F^{-1}$  for every bijection,  $\sigma$ , of  $X_1$ .<sup>1</sup> Now we need to show several things about  $F_*$ :

- $F_*(\sigma)$  really is a bijection of  $X_2$  for all bijections  $\sigma$  of  $X_1$  (in other words the map has the stated codomain).

PROOF. We need to show that  $F_*(\sigma)$  has an inverse. But since  $\sigma$  is a bijection, we know that  $\sigma^{-1}$  is a function. And we have that

$$\begin{aligned} F_*(\sigma) \circ F_*(\sigma^{-1}) &= F \circ \sigma \circ F^{-1} \circ F \circ \sigma^{-1} \circ F^{-1} \\ &= F \circ \sigma \circ \sigma^{-1} \circ F^{-1} \\ &= F \circ F^{-1} \\ &= Id_{X_2}. \end{aligned}$$

And similarly we also have that

$$F_*(\sigma^{-1}) \circ F_*(\sigma) = Id_{X_2}$$

Thus we have shown that  $F_*(\sigma)$  is a bijection (since we have shown that it has an inverse, namely  $F_*(\sigma^{-1})$ ).  $\square$

- $F_*$  is a homomorphism of groups (the bijections of any set forms a group).

PROOF. Let  $\sigma$  and  $\tau$  be bijections of  $X_1$ . Then

$$\begin{aligned} F_*(\sigma \circ \tau) &= F \circ \sigma \circ \tau \circ F^{-1} \\ &= F \circ \sigma \circ F^{-1} \circ F \circ \tau \circ F^{-1} \\ &= F_*(\sigma) \circ F_*(\tau). \end{aligned}$$

Thus applying  $F_*$  before or after composing gives the same result and  $F$  is a homomorphism of groups.  $\square$

- $F_*$  is a bijection.

---

<sup>1</sup>One should think of  $F_*$  as a renaming function in the sense that if  $\sigma$  takes  $x$  to  $x'$  and  $F$  takes  $x$  to  $y$  and  $x'$  to  $y'$ , then  $F_*(\sigma)$  takes  $y$  to  $y'$ .

PROOF. We show that  $F_*$  is a bijection by showing that  $F_*$  has an inverse, namely  $F_*^{-1}$  (defined by the same formula  $F_*$  is but replace  $F$  by  $F^{-1}$ ). Thus we need to show that  $F_* \circ F_*^{-1} = Id_{\text{Bij}(X_2)}$  and  $F_*^{-1} \circ F_* = Id_{\text{Bij}(X_1)}$ . We show these equalities by applying  $F_*^{-1} \circ F_*$  to an arbitrary  $\sigma \in \text{Bij}(X_1)$  and getting back  $\sigma$  (the proof of the other equality is the same).

$$\begin{aligned} F_*^{-1} \circ F_*(\sigma) &= F_*^{-1} (F \circ \sigma \circ F^{-1}) \\ &= F_*^{-1} \circ (F \circ \sigma \circ F^{-1}) \circ F \\ &= (F_*^{-1} \circ F) \circ \sigma \circ (F^{-1} \circ F) \\ &= \sigma. \end{aligned} \quad \square$$

- (2) Here we examine some basic properties of group homomorphisms. Here  $G, G_1, G_2$  and  $G_3$  are all groups. Also we consider  $\cong$  as a relation on the set of all groups. More precisely: define a relation  $\cong$  on the set (actually the class) of all groups via  $G_1 \cong G_2$  if and only if  $G_1$  and  $G_2$  are isomorphic.
- (a) Show that the identity map  $\text{Id}_G : G \rightarrow G$  is a group homomorphism (this should seem too obvious to prove. However, you should still have a string of equalities which start with  $\text{Id}_G(g_1 g_2)$  and end with  $\text{Id}_G(g_1) \text{Id}_G(g_2)$ ). Use this to prove that  $\cong$  is a reflexive relation (i.e. any group is isomorphic to itself).

SOLUTION.

$$\begin{aligned} \text{Id}_G(g_1 g_2) &= g_1 g_2 \\ &= \text{Id}_G(g_1) \text{Id}_G(g_2). \end{aligned}$$

This prove that the identity is a group homomorphism. Moreover the identity is a bijection (since it is its own inverse). Thus the identity map gives an isomorphism from any group to itself and as such  $\cong$  is reflexive.

- (b) If  $\varphi : G_1 \rightarrow G_2$  is an isomorphism of groups, show that  $\varphi^{-1}$  is as well. (Need to answer the questions: why is  $\varphi^{-1}$  a bijection? Why does it preserve operations?) Use this to show that  $\cong$  is symmetric.

SOLUTION.  $\varphi^{-1}$  is a homomorphism since (we insert the binary operator  $\bullet$  for  $G_1$  and  $*$  for  $G_2$  for emphasis)

$$\begin{aligned} \varphi^{-1}(g * h) &= \varphi^{-1}(\text{Id}_{G_2}(g) * \text{Id}_{G_2}(h)) \\ &= \varphi^{-1}(\varphi(\varphi^{-1}(g)) * \varphi(\varphi^{-1}(h))) \\ &= \varphi^{-1}(\varphi[\varphi^{-1}(g) \bullet \varphi^{-1}(h)]) \quad (\text{since } \varphi \text{ is op}) \\ &= (\varphi^{-1} \circ \varphi)(\varphi^{-1}(g) \bullet \varphi^{-1}(h)) \\ &= \text{Id}_{G_1}(\varphi^{-1}(g) \bullet \varphi^{-1}(h)) \\ &= \varphi^{-1}(g) \bullet \varphi^{-1}(h). \end{aligned}$$

Thus  $\varphi^{-1}$  is op whenever  $\varphi$  is. Moreover we also know that  $\varphi^{-1}$  is a bijection since it has an inverse, namely  $\varphi$ . Hence  $\varphi^{-1}$  is an op bijection, aka an isomorphism.

This proves that  $\cong$  is symmetric since if  $G_1$  is isomorphic to  $G_2$  via  $\varphi$ , then  $G_2$  is isomorphic to  $G_1$  via  $\varphi^{-1}$ .

(c) Suppose that

$$\varphi_1 : G_1 \longrightarrow G_2 \text{ and } \varphi_2 : G_2 \longrightarrow G_3$$

are group homomorphisms (isomorphisms). Show that

$$\varphi_2 \circ \varphi_1 : G_1 \longrightarrow G_3$$

is also a group homomorphism (isomorphism). Use this to show that  $\cong$  is transitive.

SOLUTION. Since the composition of two bijections is a bijection, it suffices to prove that the composition of homomorphisms is a homomorphism. To avoid too many subscripts we prove this for homomorphisms  $\phi$  and  $\psi$ . Let  $a, b \in G_1$ . If we let  $\alpha = \psi \circ \phi$  then

$$\begin{aligned} \alpha(ab) &= (\psi \circ \phi)(ab) \\ &= \psi(\phi(ab)) \\ &= \psi(\phi(a)\phi(b)) && \text{since } \phi \text{ is a hom} \\ &= \psi(xy) && \text{set } x = \phi(a) \text{ and } y = \phi(b) \\ &= \psi(x) \cdot \psi(y) && \text{since } \psi \text{ is a hom} \\ &= \psi(\phi(a))\psi(\phi(b)) \\ &= (\psi \circ \phi)(a) \cdot (\psi \circ \phi)(b) \\ &= \alpha(a) \cdot \alpha(b). \end{aligned}$$

Thus  $\alpha$  is a homomorphism.

This proves that  $\cong$  is transitive since we have shown that if  $G \cong H$  via  $\phi$  and  $H \cong K$  via  $\psi$ , then  $G \cong K$  via  $\psi \circ \phi$ .

(d) Conclude that  $\cong$  is an equivalence relation.

SOLUTION. We have shown that  $\cong$  is reflexive, symmetric, and transitive.

(3) For any group  $G$ , a homomorphism from  $G$  to itself is called an *endomorphism*. The set of all endomorphisms of  $G$  is denoted by  $\text{End}(G)$ .

(a) Show that for any group  $G$ ,  $\text{End}(G)$  is a monoid under the operation of function composition. (don't forget closure!)

SOLUTION.

(i) If  $\phi$  and  $\psi$  are endomorphisms, then they are homomorphisms from  $G$  to  $G$ . By part (c) of the last problem this implies that  $\psi \circ \phi$  is also a homomorphism from  $G$  to  $G$ . That is  $\psi \circ \phi$  is an endomorphism which implies that  $\text{End}(G)$  is closed under the operation (composition of functions).

(ii) The identity,  $Id_G$ , is a homomorphism from  $G$  to  $G$  (by part (a) of the last problem) thus  $\text{End}(G)$  contains an identity.

(iii) Composition of functions in general is associative.

Thus  $(\text{End}(G), \circ)$  is a monoid.

(b) For an endomorphism  $\varphi : G \longrightarrow G$  show that the set

$$F^\varphi := \{g \in G : \varphi(g) = g\}$$

forms a subgroup of  $G$  called the *fixed point subgroup* of  $\varphi$ .

SOLUTION.

- (i) Since  $\varphi(e) = e$  the identity is in  $F^\varphi$ .
  - (ii) If  $a, b$  are fixed by  $\varphi$ , then  $\varphi(ab) = \varphi(a)\varphi(b) = ab$  which implies that  $ab$  is also fixed by  $\varphi$ . Hence  $a, b \in F^\varphi$  implies that  $ab \in F^\varphi$ . Hence  $F^\varphi$  is closed under multiplication.
  - (iii) If  $a \in F^\varphi$  then  $\varphi(a) = a$ . But this means that  $\varphi(a^{-1}) = \varphi(a)^{-1} = a^{-1}$ . Hence  $a^{-1} \in F^\varphi$  whenever  $a$  is.
- (4) An invertible endomorphism (i.e. an isomorphism from a group to itself) is called an automorphism and the set of all automorphisms is denoted  $\text{Aut}(G)$ . This set is called the *automorphism group* of  $G$ .
- (a) Show that the automorphism group of  $G$  is (ironically!!) a group (since  $\text{Aut}(G) \subset \text{Bij}(G)$  you could use a subgroup test, or simply note that the automorphism group is the set of units in the monoid of endomorphisms and state a theorem proven in class).

SOLUTION. The set of invertible endomorphisms are automorphisms and the set of invertible elements in any monoid is always a group.

- (b) For any  $g \in G$ , define the function  $c_g : G \rightarrow G$  via  $k \mapsto gkg^{-1}$ . Show that  $c_g \in \text{Aut}(G)$  (i.e. show that  $c_g$  is an isomorphism).

SOLUTION. We first show that  $c_g$  is a homomorphism and then we show that it has an inverse.

- Let  $a, b \in G$ . Then

$$\begin{aligned} c_g(ab) &= g(ab)g^{-1} \\ &= gag^{-1}gbg^{-1} \\ &= c_g(a)c_g(b). \end{aligned}$$

Thus  $c_g$  is an endomorphism.

- Just like problem 1 of this hw assignment it's easy to see that  $c_g^{-1} = c_{g^{-1}}$ .

- (c) Show that the assignment  $g \mapsto c_g$  is a homomorphism of groups  $G \rightarrow \text{Aut}(G)$ . (The image of this group is denoted  $\text{Inn}(G)$  and such automorphisms are called *inner*).

SOLUTION. For clarity let's call the function  $g \mapsto c_g$   $F$  (so that  $F(g)(h) = ghg^{-1}$ ). We need to show that  $F$  preserves operations. To stress the situation we explicitly denote the operation in  $G$  by  $*$ . So we need to show that

$$F(g_1 * g_2) = F(g_1) \circ F(g_2).$$

Indeed, since both sides are functions we simply need to show that they do the same thing to all elements of the domain, in this case  $G$ .

To that end let  $g \in G$  be arbitrary, then

$$\begin{aligned}
 F(g_1 * g_2)(g) &= c_{g_1 g_2}(g) \\
 &= (g_1 * g_2) * g * (g_1 * g_2)^{-1} \\
 &= (g_1 * g_2) * g * (g_2^{-1} * g_1^{-1}) \\
 &= g_1 * (g_2 * g * g_2^{-1}) * g_1^{-1} \\
 &= g_1 * c_{g_2}(g) * g_1^{-1} \\
 &= c_{g_1}(c_{g_2}(g)) \\
 &= (F(g_1) \circ F(g_2))(g).
 \end{aligned}$$

Hence

$$F(g_1 * g_2) = F(g_1) \circ F(g_2)$$

holds as desired.

- (d) Show that the kernel of this homomorphism,  $g \mapsto c_g$ , is equal to the center of  $G$  (the center of  $G$ , denoted by  $Z(G)$ , is the intersection of all the centralizers of  $G$ , i.e. it is the set of elements of  $G$  which commute with every element of  $G$ ).

SOLUTION. First note that as a set

$$Z(G) = \{g \in G : gh = hg \forall h \in G\}.$$

Since the identity of  $\text{Aut}(G)$  is the identity function,  $Id_G$ , we are looking for the set

$$\begin{aligned}
 \text{Ker}(g \mapsto c_g) &= \{g \in G : c_g = Id_G\} \\
 &= \{g \in G : c_g(h) = h \forall h \in G\} \\
 &= \{g \in G : ghg^{-1} = h \forall h \in G\} \\
 &= \{g \in G : gh = hg \forall h \in G\} \\
 &= Z(G).
 \end{aligned}$$

- (5) Suppose that  $G$  and  $H$  are groups. Show that  $G \times H \cong H \times G$ .

SOLUTION. Define a map  $t : G \times H \rightarrow H \times G$  via  $t(g, h) = (h, g)$ .

Then

- The inverse of  $t$  is the map which takes  $(h, g)$  to  $(g, h)$ .
- If  $g, g' \in G$  and  $h, h' \in H$  then

$$\begin{aligned}
 t((g, h)(g', h')) &= t((gg', hh')) \\
 &= (hh', gg') \\
 &= (h, g)(h', g') \\
 &= t(g, h)t(g', h').
 \end{aligned}$$

Hence  $t$  is a homomorphism.

Since  $t$  is a bijective homomorphism it is an isomorphism.

- (6) Recall from homework 3 problem (3) that the set of matrices

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

with coefficients in any commutative ring with identity forms a group (this group is typically called the Heisenberg group). We denote this group  $UT(3, R)$ .

- (a) Show that all 26 non-identity elements of  $UT(3, \mathbb{Z}_3)$  have order 3 (just cube an arbitrary element of this group).

$$\begin{aligned} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^3 &= \begin{pmatrix} 1 & 3a & 3ac + 3b \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (\text{since } 3 = 0 \pmod{3}) \end{aligned}$$

- (b) Show that all 26 non-identity elements of  $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$  also have order 3.

SOLUTION.

$$(a, b, c)^3 = (3a, 3b, 3c) = (0, 0, 0).$$

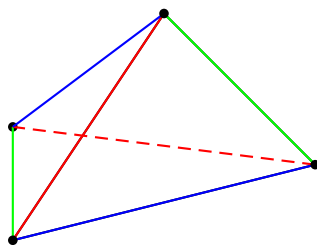
- (c) Show that despite this that  $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$  and  $UT(3, \mathbb{Z}_3)$  are not isomorphic.

SOLUTION.  $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$  is abelian but  $UT(3, \mathbb{Z}_3)$  is not.

- (d) True or False. If two groups,  $G$  and  $H$  have the same number of elements of any given order, then  $G$  and  $H$  are isomorphic.

SOLUTION. **False** This problem shows an explicit example where this is not true.

- (7) Let  $S(\Delta^3)$  be the set of (orientation preserving) rigid motions of a (3-dimensional) tetrahedron. A tetrahedron has 6 edges. We can pair these edges (edges with the same color are paired)



- (a) Show that an element of  $S(\Delta^3)$  preserves this pairing (**hint** note that two edges are colored the same if and only if they do not touch).

SOLUTION. If  $e$  is an edge, then  $g(e)$  is an edge for every  $g \in S(\Delta^3)$  and two edges intersect at a point  $p$  if and only if their images under  $g$  intersect at  $g(p)$ .

- (b) If we label the green edges with a 1, red with a 2, and blue with a 3 we can a homomorphism from  $S(\Delta^3)$  to  $S_3$ . What is the image of this homomorphism? What is the kernel? (For instance a right-handed rotation through line from the middle three vertices the upper vertex

takes the pair of green edges to the set of blue edges, the set of blue edges to the set of red edges and the set of red edges back to the set of green edges and thus corresponds to the permutation  $(1\ 3\ 2)$ . )

SOLUTION. There are two kinds of elements of  $S(\Delta^3)$ : there are 3 180 degree rotations along the axis connecting the midpoint of two edges and 4 120 degree and 4 negative 120 degree rotation along the axes connecting vertices to midpoints of triangular faces (this along with the identity make up the 12 elements of  $S(\Delta^3)$ ). Since these 120 degree rotations permute the three edges along a face which are all colored differently, all 120 degree rotations go to 3-cycles in  $S_3$ . On the other hand, the first kind of rotation fix no vertices. Thus every edge not fixed by such a rotation must go to an edge sharing no vertex with the original. Hence to an edge of the same color implying that the image of such a rotation is the identity.

In summary (if we call the homomorphism by our favorite symbol  $\varphi$ ):

$$\text{Ker}(\varphi) = \{Id, 180 \text{ rots}\} \subset S(\Delta^3)$$

$$\text{Im}(\varphi) = \{(1), (1\ 2\ 3), (1\ 3\ 2)\} \subset S_3.$$