Math 3140 — Fall 2012
Assignment #1

Due Weds., Sep. 5.

Exercise 1. (a) List all of the symmetries of a square, allowing all transformations made up of rotations, reflections, and translations. This group is called D_4.

Solution. Label the vertices 1, 2, 3, and 4 in counterclockwise order. The symmetries are:

1) e, the identity,
2) ρ, rotation by 90° counterclockwise,
3) ρ^2, rotation by 180°,
4) ρ^3, rotation by 270° counterclockwise,
5) γ_{13}, reflect through the line containing 1 and 3,
6) γ_{24}, reflect through the line containing 2 and 4,
7) α, reflect through the line connecting the midpoint of the side containing 1 and 2 to the midpoint of the side containing 3 and 4,
8) β, reflect through the line connecting the midpoint of the side containing 1 and 4 to the midpoint of the side containing 2 and 3.

□

(b) How many elements does D_4 have?

Solution. Eight. □

(c) Is D_4 abelian?

Solution. No, it is not, because we can compute $\rho\gamma_{13} = \alpha$ and $\gamma_{13}\rho = \beta$. □

Exercise 3. (a) Suppose that G is a group and x is an element of G. Show that if y is a right inverse of x (meaning that $xy = e$) and z is a left inverse of x (meaning that $zx = e$) then $y = z$.

Solution. If we multiply the equation $xy = e$ on the left by z we get $z(xy) = ze = z$ because e is the identity of G. By associativity, we therefore get $(zx)y = z$ and then since z is a left inverse of x, we get $ey = z$. Again because e is the identity we finally get $ey = y$ so $y = z$. □

(b) Conclude from this that each element of G has exactly one inverse. (Remember that the group axioms explicity guarantee every element has *at least one* inverse, but they do not say that the inverse must be unique. You are supposed to prove this uniqueness.)

Solution. If y and z are two inverses of x then in particular y is a left inverse and z is a right inverse. Hence $y = z$ by the previous part of the exercise. □

Comments. One mistake that occurred a few times was to prove that $z^{-1} = y^{-1}$ legitimately but then to conclude immediately from this that $z = y$. Implicitly, what this is saying is that $z = (z^{-1})^{-1} = (y^{-1})^{-1} = y$, but remember that we are in the process of *proving* that inverses are unique. Therefore, just knowing that $z^{-1} = y^{-1}$ does not tell us that the inverses of z^{-1} and y^{-1} have to be the same.

Many also attempted to use commutativity in one form or another while solving this exercise. You can't do that because not every group is commutative. That is, if x and y are elements of an abstract group then you generally cannot assume that $xy = yx$. Do not make this mistake!

This misunderstanding often takes the following form: suppose that $a = bc$ in a group; then $c = \frac{a}{b}$ so $a = cb$. The problem is in the notation $\frac{a}{b}$. This notation does not mean anything in most groups because it isn't clear if $\frac{a}{b}$ is supposed to mean ab^{-1} or $b^{-1}a$. These elements are usually different and it is essential not to confuse them. □

Exercise 4. Suppose that G is a group and x and y are elements of G. Show that $(xy)^{-1} = y^{-1}x^{-1}$.

Solution. We saw above that the inverse of xy is unique. Therefore if $xyz = e$ and $zxy = e$ then we can conclude that $z = (xy)^{-1}$. In particular, if $(xy)y^{-1}x^{-1} = e$ and $y^{-1}x^{-1}(xy) = e$ then we will deduce that $(xy)^{-1} = y^{-1}x^{-1}$. For this, we multiply using associativity and get

$$xyy^{-1}x^{-1} = xex^{-1} = xx^{-1} = e$$
$$y^{-1}x^{-1}xy = y^{-1}ey = y^{-1}y = e.$$

□

Solution. Here is another very nice solution that several people used:

$(xy)^{-1}xy = e$	definition of inverse
$(xy)^{-1}xyy^{-1} = y^{-1}$	multiply on right by y^{-1}
$(xy)^{-1}xe = y^{-1}$	$yy^{-1} = e$ by definition of inverse
$(xy)^{-1}x = y^{-1}$	e is the identity
$(xy)^{-1}xx^{-1}y^{-1}x^{-1}$	multiply on right by x^{-1}
$(xy)^{-1}e = y^{-1}x^{-1}$	$xx^{-1} = e$ by definition of inverse
$(xy)^{-1} = y^{-1}x^{-1}$	e is the identity.

□

Comments. In a proof like this, it is important to explain each step of your argument. Otherwise it is difficult to tell if you knew what you were doing or stumbled on the right step by accident. I will insist on this on the exam.

I saw things like $(xy)^{-1} = \frac{1}{xy} = \frac{1}{y}\frac{1}{x} = y^{-1}x^{-1}$ a lot. Remember, the fraction bar does not have a well-defined meaning in a group unless the group is known to be commutative!

A lot of people also did a "left side–right side" proof in which they started with the thing they wanted to prove ($(xy)^{-1} = y^{-1}x^{-1}$ or some similar variant and made a sequence of logical steps to arrive at a statement that was already known (usually $e = e$). Even though the ideas going into many of these proofs were sound, **this is not a legitimate proof techinique!** Many "proofs" along these lines are false. Only right side–left side proofs where every step is reversible are truly correct, and a right side–left side proof that does not explain why each step is reversible **is not a proof**. See this page for a thorough explanation of the dangers of right side–left side proofs: http://math.colorado.edu/~kstange/teach/rightleft.pdf. □

Exercise 5. [Fra, §4, #19]. Let S be the set of all real numbers except -1 with the composition law

$$a * b = a + b + ab.$$

(a) Show that S is a group.

Solution. First we must check that $*$ is well defined. That is, we must check that if a and b are real numbers other than -1 than $a * b \neq -1$. Suppose that $a * b = -1$. Then $a + b + ab = -1$ so $1 + a + b + ab = 0$. But this factors into $(1 + a)(1 + b) = 0$ so we get $a = -1$ or $b = -1$. By the contrapositive, if $a \neq -1$ and $b \neq -1$ then $a * b \neq -1$. Thus $*$ is well-defined.

We also have to check that $*$ is associative:

$$\begin{aligned} a * (b * c) &= a * (b + c + bc) \\ &= a + b + c + bc + a(b + c + bc) \\ &= a + b + c + bc + ab + bc + abc \end{aligned} \qquad \begin{aligned} (a * b) * c &= (a + b + ab) * c \\ &= a + b + ab + c + (a + b + ab)c \\ &= a + b + ab + c + ac + bc + abc \end{aligned}$$

and these are evidently the same.

The identity element is $e = 0$. Indeed $e * b = 0 + b + 0b = b$ and $a * e = a + 0 + a0 = a$.

We can solve for the inverse of $a \in S$: if $a * b = 0$ then $a + b + ab = 0$ so $b(1 + a) = -a$ and $b = \frac{-a}{1+a}$. We check that this is indeed a left inverse of a:

$$\frac{-a}{1+a} * a = \frac{-a}{1+a} + a - \frac{a^2}{1+a} = \frac{-a + a(1+a) - a^2}{1+a} = 0.$$

Since S is abelian (proof: $a * b = a + b + ab = b + a + ba = b * a$) this means $\frac{-a}{1+a}$ is also a right inverse of a. Thus S is a group. □

(b) Show that S is isomorphic to $\mathbf{R}^*$.

Solution. Let $f : S \to \mathbf{R}^*$ be the function $f(a) = a + 1$. Then f is a bijection since it has the inverse $f^{-1}(a) = a - 1$. (Notice that f is well-defined because no there is no $a \in S$ such that $f(a) = 0$; likewise f^{-1} is well-defined because there is no $a \in \mathbf{R}^*$ such that $f^{-1}(a) = -1$.)

To check that f is an isomorphism, we also need to check that

$$f(a * b) = f(a)f(b).$$

We evaluate both sides:

$$\begin{aligned} f(a * b) &= f(a + b + ab) & f(a)f(b) &= (a + 1)(b + 1) \\ &= 1 + a + b + ab & &= ab + a + b + 1 \end{aligned}$$

and these are evidently the same. Therefore f is an isomorphism. □

(c) Solve the equation $2 * x * 3 = 7$ in S. (Suggestion: While it is possible to solve this problem directly using the definition of the group law, try making use of the previous part of this exercise.)

Solution. Notice that

$$2 * x * 3 = 7$$

if and only if

$$f(2)f(x)f(3) = f(7)$$

because f is an isomorphism. We solve the second equation:

$$f(x) = \frac{f(7)}{f(2)f(3)} = \frac{8}{3 \cdot 4} = \frac{2}{3}.$$

Therefore

$$x = f^{-1}(f(x)) = f^{-1}(\frac{2}{3}) = \frac{2}{3} - 1 = -\frac{1}{3}.$$

□

Comments. Many people successfully demonstrated that S is a group except for checking that the element $b = \frac{-a}{1+a}$ is a 2-*sided inverse* of b: recall that for G to be a group, for each element $a \in G$ there must be an element $b \in G$ such that $a * b = e$ and $b * a = e$. Many of you only verified that $a * b = e$. (Of course the multiplication is commutative here, so $a * b = b * a$, but if you want to rely on that fact you should say you are doing so.) There will be an exercise on a later problem set to emphasize this.

Some people also did some of part (a) "backwards". When you prove that a group has an identity element, you should say "The identity is e" and then verify that $e * x = x$ and $x * e = x$. Likewise you should say "The inverse of x is x'"—and explain what x' is—and then verify that $x * x' = e$ and $x' * x = e$.

Some people neglected to check that the multiplication operation is well-defined. This should always be the first thing you look at when you are checking if something is a group!

For the sake of clarity, it is a good idea to use a special symbol for the composition law in a group when the addition and multiplication symbols are being used for other things. That was the case on this problem: $a*b = a+b+ab$. Many people dropped the $*$ symbol and wrote $ab = a + b + ab$. I understood what you meant when you did this, but doing this can rapidly become very confusing. As a general rule, you should never use the same symbol for two different operations!

Several people also seemed to be confused about the definition of a group, especially the meaning of associativity: it was frequently confused with commutativity. Make sure to get the definition straight now, or it will be a very unpleasant semester. □

Exercise 6. [Fra, §4, #35]. Show that if G is a group containing elements a and b and $(ab)^2 = a^2b^2$ then $ab = ba$.

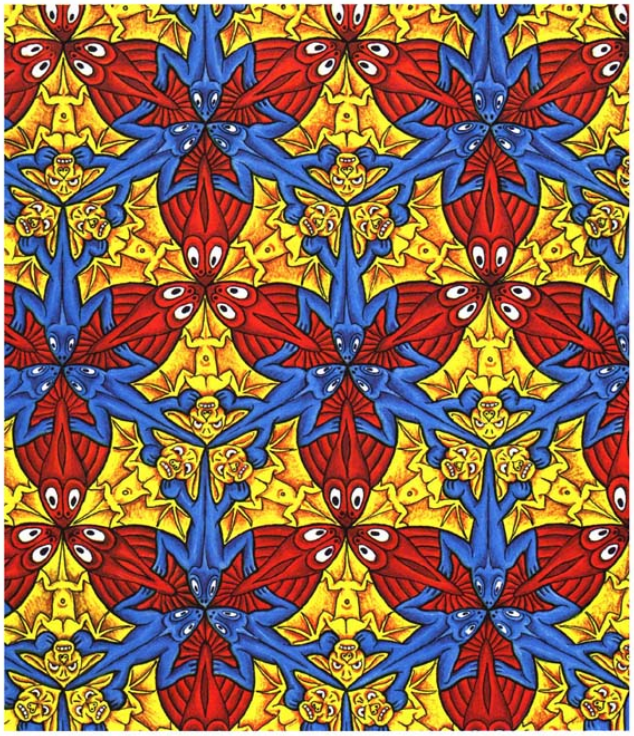
Solution. Note that $(ab)^2 = abab$ and $a^2b^2 = aabb$. If $(ab)^2 = a^2b^2$ then

$$\begin{aligned} abab &= aabb && \\ a^{-1}ababb^{-1} &= a^{-1}aabbb^{-1} && \text{multiply both sides by } a^{-1} \text{ on left and } b^{-1} \text{ on right} \\ ebae &= eabe && a^{-1}a = e \text{ and } bb^{-1} = e \\ ba &= ab && e \text{ is the identity} \end{aligned}$$

□

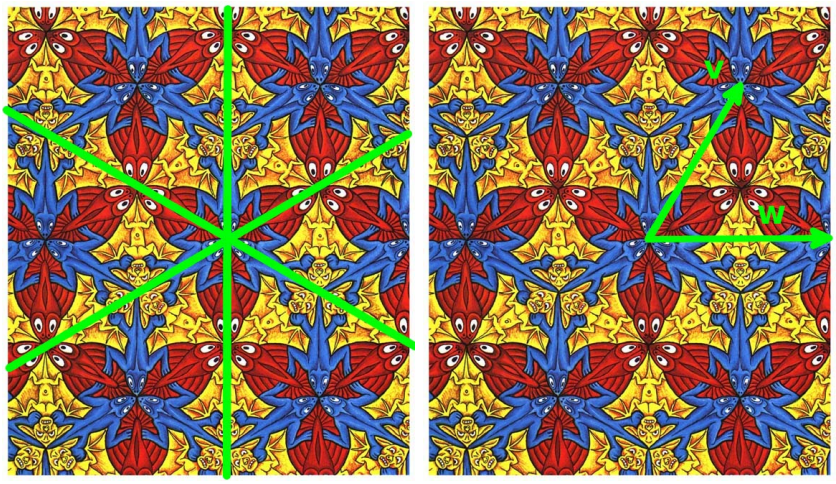
Comments. The most common mistake was some version of assuming the group was abelian. Note that the notation $\frac{x}{y}$ for $x, y \in G$ is bad unless G is known to be an abelian group, because xy^{-1} and $y^{-1}x$ can be different elements of G and $\frac{x}{y}$ doesn't distiguish the order of multiplication. □

Exercise 7. Describe all of the symmetries of the picture below (assume that it repeats to infinity in all directions):



M. C. Escher, Tessellation 85.
Source: http://britton.disted.camosun.bc.ca/jbsymteslk.htm

Solution. We may begin by performing any symmetry in D_3: rotation by a multiple of 120° or reflection along any of the axes indicated below on the left; then we can perform a translation by any integer linear combination of the vectors v and w indicated in the picture on the right.



Thus for any element of $(\sigma, n, m) \in D_3 \times \mathbf{Z} \times \mathbf{Z}$ we obtain a symmetry: first apply σ to rotate around the center point of the picture on the left and/or reflect the image about one of the axes indicated on the left. Then translate the image by $n\mathbf{v}+m\mathbf{w}$, where $\mathbf{v}$ and $\mathbf{w}$ are the vectors indicated in the image on the right.

To prove that this is the set of all symmetries, suppose that σ is a symmetry of the image. Then σ transforms the central point O (the intersection of the axes above) to some other point P where three lizards' faces meet. There is a unique pair $(n, m) \in \mathbf{Z}^2$ such that $\vec{OP} = n\mathbf{v} + m\mathbf{w}$. Let τ be translation by $n\mathbf{v} + m\mathbf{w}$. Then $\tau^{-1}\sigma$ is a symmetry of the image that takes O to O. The symmetries of the image that preserve O are the same as the symmetries of an equilateral triangle: D_3. Thus $\tau^{-1}\sigma \in D_3$. If we let μ be this symmetry then $\mu = \tau^{-1}\sigma$ so $\sigma = \tau\mu$. That is, σ is the composition of a symmetry in D_3 followed by the translation τ.

Note that we have not described the group of all symmetries—we have just described the set of those symmetries. We will examine the group structure later. □

Comments. Many people omitted the relfections or the translations. A large number listed all three possibilities but forgot that they can be composed to yield other symmetries. □

Exercise 8. How many symmetries does a set with n elements have? (How many permutations are there of a set with n elements?)

Solution. A symmetry of a set is a permutation. There are n choices for where to move the first element, $n-1$ choices for where to move the next one, $n-2$ choices for where to move the third, etc. In all, the choices multiply and we get $n!$ permutations. □

Comments. Almost everyone got this one. A few people added or combined the choices according to other rules and got incorrect answers. □

Exercise 9. Consider the following six functions:

$$f_1(x) = x \qquad f_2(x) = 1 - x \qquad f_3(x) = \frac{1}{x}$$
$$f_4(x) = \frac{1}{1-x} \qquad f_5(x) = \frac{x}{x-1} \qquad f_6(x) = \frac{x-1}{x}.$$

(a) Show that these functions form a group where the group operation is *composition of functions*.

Solution. Let G be the set $\{f_1, f_2, f_3, f_4, f_5, f_6\}$. First we have to check that the composition of any two elements in G is also in G. This is a lot of checking. We build the whole multiplication table:

	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_5	f_6	f_2	f_1
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_5	f_2	f_1	f_3	f_4 .

This shows that composition is well-defined. Checking associativity with the multiplication table would be tedious, but fortunately we know that associativity holds for composition of functions in general. As we have already remarked, f_1 is the left- and right-sided identity for G. Furthermore, we can read from the multiplication table that

$$f_1^{-1} = f_1 \qquad f_2^{-1} = f_2 \qquad f_3^{-1} = f_3$$
$$f_4^{-1} = f_6 \qquad f_5^{-1} = f_5 \qquad f_6^{-1} = f_4$$

so every element has a 2-sided inverse. □

(b) Show that this group is isomorphic to S_3 by constructing an isomorphism.

Solution. We can construct an isomorphism by finding a set that is permuted by the f_i. Let X be the set $\{-1, \frac{1}{2}, 2\}$. Notice that

$$f_1(-1) = -1 \qquad f_1(1/2) = 1/2 \qquad f_1(2) = 2$$
$$f_2(-1) = 2 \qquad f_2(1/2) = 1/2 \qquad f_2(2) = -1$$
$$f_3(-1) = -1 \qquad f_3(1/2) = 2 \qquad f_3(2) = 1/2$$
$$f_4(-1) = 1/2 \qquad f_4(1/2) = 2 \qquad f_4(2) = -1$$
$$f_5(-1) = 1/2 \qquad f_5(1/2) = -1 \qquad f_5(2) = 2$$
$$f_6(-1) = 2 \qquad f_6(1/2) = -1 \qquad f_6(2) = 1/2.$$

Therefore if we label -1 as "1", and we label $1/2$ as "2", and we label 2 as "3" then we get a map $G \to S_3$. This must preserve composition because

we are restricting functions to a subset. Therefore to see that φ is an isomorphism we only have to check that φ is a bijection. Since G and S_3 are both sets of the same size, it is enough to verify that φ is surjective. For this we can observe that

$$\begin{array}{lll} \varphi(f_1) = e & \varphi(f_2) = g_2 & \varphi(f_3) = g_1 \\ \varphi(f_4) = a & \varphi(f_5) = g_3 & \varphi(f_6) = b, \end{array}$$

using the notation from class for S_3. □

Comments. A surprisingly common mistake was to assume that $f_i^{-1} = \frac{1}{f_i}$. The group operation here isn't multiplication, so the inverse is not the same thing as the reciprocal. Remember, the inverse of the identity is always the identity, and almost everyone recognized that f_1 is the identity. So f_1^{-1} should be f_1, not f_3. □

Exercise 10. Let S_4 be the group of symmetries of a set with 4 elements. Let G be the group of rigid symmetries (compositions of translations, rotations, and reflections are allowed) of a regular tetrahedron. Show that G and S_4 are isomorphic. (Hint: there is a more efficient way to do this than writing down both multiplication tables!)

Solution. First we note that a rigid symmetry of the tetrahedron must permute the vertices. If we choose a labelling of the vertices of the tetrahedron, then any rigid symmetry permutes the labels. This determines a function $\varphi : G \to S_4$. Notice that φ must preserve composition (it is a homomorphism) because it is simply restriction of a function. Therefore we can prove φ is an isomorphism by showing it is bijective.

To see that φ is injective, notice that a rigid symmetry of the tetrahedron is determined by how it permutes the vertices: two rigid symmetries that permute the vertices in the same way must be the same symmetry.

To see that φ is surjective, we let σ be a permutation in S_4 and construct a rigid symmetry s of the tetrahedron such that $\varphi(s) = \sigma$.

First, choose a rotation a of the tetrahedron that puts the vertex labelled 1 in the right place; let $\alpha = \varphi(a)$. Then $\alpha(1) = \sigma(1)$. Thus $\alpha^{-1}\sigma$ is a permutation that fixes 1.

Let b be a rotation of the tetrahedron around the axis connecting the vertex labelled 1 to the midpoint of the opposite side such that if we define $\beta = \varphi(b)$ then $\beta(2) = \alpha^{-1}\sigma(2)$. Notice that $\beta(1) = 1$. Thus $\beta^{-1}\alpha^{-1}\sigma$ is an element of S_4 that fixes both 1 and 2.

This means that either $\beta^{-1}\alpha^{-1}\sigma = e$, in which case $\sigma = \alpha\beta = \varphi(ab)$ and we can take $s = ab$ to show that σ is in the image of φ, or else $\beta^{-1}\alpha^{-1}\sigma$ is the permutation that exchanges 3 and 4 and leaves 1 and 2 fixed. In this case, let c be the reflection through the plane containing the vertices labelled 1 and 2 and the midpoint of the line connecting the vertices labelled 3 and 4. Then $\gamma = \varphi(c)$ exchanges 3 and 4 and leaves 1 and 2 fixed. Therefore $\gamma = \beta^{-1}\alpha^{-1}\sigma$. Therefore $\sigma = \alpha\beta\gamma = \varphi(abc)$ is once again in the image of φ.

We conclude from the above argument that φ is surjective. As we have already seen that it is injective, it follows that φ is bijective, hence an isomorphism. □

Comments. I was pleased to see that many of you realized the homomorphism $G \to S_4$ could be obtained by labelling the vertices and restricting a symmetry of the tetrahedron to them. This is still a long way from a proof, so the observation alone didn't get a lot of credit, but it was still the main thing I wanted you to get from this problem.

One mistake that turned up several times was to assert that S_4 and G have the same size (the correct size is 24; there were a few incorrect calculations of this number) and therefore must be isomorphic. On the second assignment you will see an example of two groups of the same size that are not isomorphic. In fact there are a large number of non-isomorphic groups of order 24. *Just checking that two groups have the same size is not enough to deduce that they are isomorphic.* □

Exercise 11. Suppose that A and B are groups and $f : A \to B$ is a function that satisfies the property

$$f(xy) = f(x)f(y).$$

(Functions of this type are called **homomorphisms** and will be very important later.)

(a) Show that $f(e) = e$.

Solution. Since $ee = e$ we have $f(e) = f(ee) = f(e)f(e)$. But B is a group, so we get

$$e = f(e)^{-1}f(e) = f(e)^{-1}f(e)f(e) = f(e)$$

as desired. □

(b) Show that if x is in A then $f(x^{-1}) = f(x)^{-1}$.

Solution. We have $f(xx^{-1}) = f(x)f(x^{-1})$. But $xx^{-1} = e$ so (making use of the previous part of this exercise)

$$f(x)f(x^{-1}) = f(e) = e.$$

Thus $f(x^{-1})$ is the inverse of $f(x)$. □

References

[Fra] John B. Fraleigh. *A first course in abstract algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., seventh edition edition, 2002. ISBN-10: 0201763907, ISBN-13: 978-0201763904.