Math 3140 — Fall 2012
Assignment #4

Due Fri., Sept. 28. Remember to cite your sources, including the people you talk to.

In this problem set, we use the notation $\gcd\{a, b\}$ for the greatest common divisor of a and b.

My solutions will use the following proposition from class:

Proposition 1. *Let G be a group and $H \subset G$ a subset. If H is non-empty and for every $x, y \in H$ we have $xy^{-1} \in H$ as well then H is a subgroup of G.*

Exercise 27. [Fra, §6, #16]

1. [Arm, §5, #10]. Make a list of all elements of $\mathbf{Z}/12\mathbf{Z}$ that generate $\mathbf{Z}/12\mathbf{Z}$. Recall that an element g of a group G **generates** G if every element of G is of the form g^n for some integer n.

   Solution. The elements $1, 5, 7, 11$ generate $\mathbf{Z}/12\mathbf{Z}$. □

2. An **automorphism** of a group is an isomorphism from that group to itself. Find all automorphisms of the group $\mathbf{Z}/12\mathbf{Z}$. (Hint: if φ is an automorphism of $\mathbf{Z}/12\mathbf{Z}$, what values are possible for $\varphi(1)$?)

   Solution. Observe that because $\mathbf{Z}/12\mathbf{Z}$ is finite, a homomorphism $\varphi : \mathbf{Z}/12\mathbf{Z} \to \mathbf{Z}/12\mathbf{Z}$ is an automorphism if and only if it is bijective (bijectivity is equivalent to surjectivity for functions between finite sets of the same size). But φ is surjective if and only if every $x \in \mathbf{Z}/12\mathbf{Z}$ is $\varphi(n) = n\varphi(1)$ for some $n \in \mathbf{Z}/12\mathbf{Z}$; therefore φ is surjective if and only if $\varphi(1)$ generates $\mathbf{Z}/12\mathbf{Z}$.

   Therefore an automorphism of $\mathbf{Z}/12\mathbf{Z}$ will have to have $\varphi(1) \in \{1, 5, 7, 11\}$. This means that φ has to be one of the following functions:

   $$\varphi(n) = n$$
   $$\varphi(n) = 5n$$
   $$\varphi(n) = 7n$$
   $$\varphi(n) = 11n.$$

   We can also see directly that these are homomorphisms: the function $\varphi : \mathbf{Z}/12\mathbf{Z} \to \mathbf{Z}/12\mathbf{Z}$ given by $\varphi(n) = kn$ is well-defined because $\varphi(n + 12\ell) = kn + 12k\ell \equiv kn \pmod{12}$ and φ is a homomorphism because $\varphi(n + m) = k(n + m) = kn + km = \varphi(n) + \varphi(m)$. □

Exercise 30. Let X be a set and $Y \subset X$ a subset. Let G be the subset of all $g \in S_X$ such that $g(y) \in Y$ for all $y \in Y$ *and the function* $g|_Y : Y \to Y$ *is surjective*[1][2] then G is a subgroup of S_X. ←1 ←2

Solution. To check this is a subgroup, we have to check that G is non-empty (it contains the identity function) and that $gh^{-1} \in G$ whenever g and h are. We have to verify that if $y \in Y$ then $gh^{-1}(y) \in Y$. Suppose that $y \in Y$. Then because $h \in G$ we know that $h|_Y$ is surjective so there is some $y' \in Y$ such that $h(y) = y'$. Therefore $h^{-1}(y) = y' \in Y$. Then

$$g(h^{-1}(y)) = g(y')$$

is in Y as well because $y' \in Y$ and g takes elements of Y to elements of Y. Therefore $gh^{-1} \in G$. By Proposition 1, this means that G is a subgroup of S_X. □

Exercise 31. [Fra, §8, #21]

(a) Verify that the six matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

form a group in which the operation is multiplication of matrices. (Hint: one solution to this problem uses the last exercise; let $X = \mathbf{R}^3$ and let $Y = \{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ where $\mathbf{e}_1 = (1, 0, 0)$, $\mathbf{e}_2 = (0, 1, 0)$, and $\mathbf{e}_3 = (0, 0, 1)$ are the standard basis vectors.)

Solution. Let Y be as in the hint and let G be the set of elements of $S_{\mathbf{R}^3}$ that restrict to surjections $Y \to Y$. Let H be the set of 6 matrices above. By the previous exercise, G is a subgroup of $S_{\mathbf{R}^3}$. The group of invertible matrices $\mathrm{GL}(3, \mathbf{R})$ is also a subgroup of $S_{\mathbf{R}^3}$. Furthermore, $H = G \cap \mathrm{GL}(3, \mathbf{R})$ so H is also a subgroup of $S_{\mathbf{R}^3}$. Therefore H is in particular a group. □

(b) Show that this group is isomorphic to S_3.

Solution. We construct a bijective homomorphism. Let $\varphi : S_3 \to H$ be the function that sends σ to the matrix $\varphi(\sigma) = T_\sigma$

$$T_\sigma = \begin{pmatrix} \mathbf{e}_{\sigma(1)} & \mathbf{e}_{\sigma(2)} & \mathbf{e}_{\sigma(3)} \end{pmatrix}.$$

[1] Correction! I left out this important hypothesis originally; thanks Tyler
[2] second correction: the original correction broke the sentence in the wrong place

I claim φ is a homomorphism. To check this, we have to check that $T_\sigma T_\tau = T_{\sigma\tau}$. These are matrices, so it's the same to check that $T_\sigma T_\tau(\mathbf{e}_i) = T_{\sigma\tau}(\mathbf{e}_i)$ for all i. We have

$$T_\sigma T_\tau(\mathbf{e}_i) = T_\sigma(\mathbf{e}_{\tau(i)}) = \mathbf{e}_{\sigma(\tau(i))}$$
$$T_{\sigma\tau}(\mathbf{e}_i) = \mathbf{e}_{\sigma\tau(i)}.$$

These are the same so φ is a homomorphism.

Also, if $\varphi(\sigma) = \varphi(\tau)$ then $T_\sigma(\mathbf{e}_i) = T_\tau(\mathbf{e}_i)$ for all i. But $T_\sigma(\mathbf{e}_i) = \mathbf{e}_{\sigma(i)}$ and $T_\tau(\mathbf{e}_i) = \mathbf{e}_{\tau(i)}$ so this means that $\sigma(i) = \tau(i)$ for all $i = 1, 2, 3$. Therefore $\sigma = \tau$. So φ is injective. Since both S_3 and H have 6 elements, this means that φ is bijective, hence is an isomorphism. □

Exercise 32. In the **fifteen puzzle** you are given a 4×4 grid containing 15 square tiles and one empty space. Any tile adjacent to the empty space can be slid into the empty space. The goal is, given a scrambled puzzle like the one on the left below

2	13	4	8
5	1	3	7
9	12	6	15
10	14	11	

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

to return it to the starting position on the right. If you haven't played with a fifteen puzzle before, you may want to practice online before doing this exercise: migo.sixbit.org/puzzles/fifteen/.

(a) Explain a correspondence between every position of the fifteen puzzle and the elements of the group S_{16}.

Solution. Label the positions of the tiles in the 15-puzzle by the numbers $1, 2, \ldots, 16$ (with 16 corresponding to the blank square). Then any rearrangement of the tiles moves the tile with number i to some position $\sigma(i)$. Thus σ is a rearrangement of the set $\{1, 2, \ldots, 16\}$ so $\sigma \in S_{16}$. □

(b) Write down the permutation corresponding to the unsolved fifteen puzzle above, using cycle notation.

Solution.

$$(1, 6, 11, 15, 12, 10, 13, 2)(3, 7, 8, 4)(5)(9)(14)$$

□

(c) Demonstrate that under this correspondence each move on a 15-puzzle corresponds is a transposition.

Solution. The only legal moves correspond to exchanging the position of the blank square (16) and an adjacent tile. The legal moves all therefore correspond to transpositions $(16, a)$ where $a \in \{1, 2, \ldots, 15\}$. □

(d) Show that a sequence of moves beginning with the empty tile in the upper left and ending with it in the lower right must consist of an even number of moves.

Solution. Suppose that σ is a position of the 15-puzzle. Let $a(\sigma)$ be the number of rows away from the bottom row the blank square is; let $b(\sigma)$ be the number of columns away from the rightmost column blank square is. Let $n(\sigma) = a(\sigma) + b(\sigma)$. If the blank tile is in the upper left then $n(\sigma) = 6$; if it is in the lower right then $n(\sigma) = 0$.

Consider the number $(-1)^{n(\sigma)}$. Notice that if we make any move, the value of $n(\sigma)$ will change by exactly one because the blank tile will **either** change row or column **but not both**. Therefore if we achieve the permutation σ with an odd number of moves we will have to get $n(\sigma) = -1$. But if σ is a permutation that moves the blank tile from the upper left to the lower right then $n(\sigma)$ is even so $(-1)^{n(\sigma)} = 1$, which means that σ could not have been achieved with an odd number of moves. That is, σ must have taken an even number of moves. □

(e) Write down the permutation correpsonding to the unsolved fifteen puzzle below:

	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

Solution. Let 16 represent the blank tile. The permutation is

$$(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16).$$

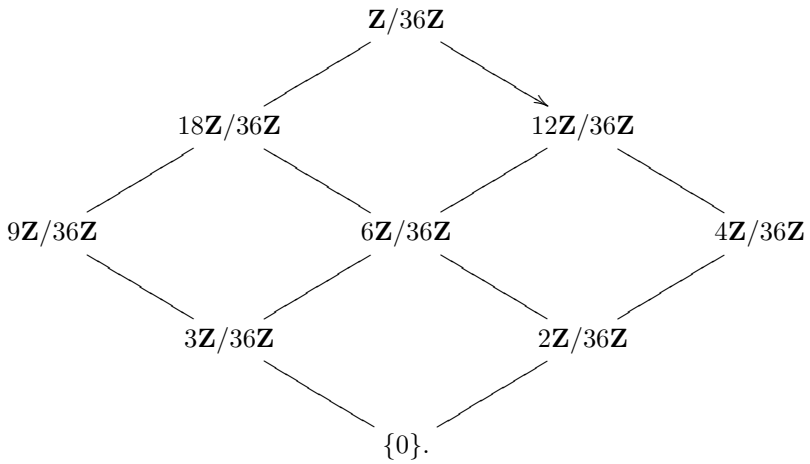
□

(f) Show that the fifteen puzzle shown above cannot be solved.

Solution. The sign of the permutation above is $(-1)^{16-1} = -1$, but any sequence of moves that moves the blank square from the upper left to the lower right involves an even number of moves (as we just saw). Thus a solvable puzzle must correspond to an even permutation, with sign $+1$. □

Exercise 33. (a) [Fra, §6, #23]. List all subgroups of $\mathbf{Z}/36\mathbf{Z}$ and indicate which subgroups are contained in which others.

Solution.



Here $a\mathbf{Z}/36\mathbf{Z}$ is the subgroup generated by a in $\mathbf{Z}/36\mathbf{Z}$. □

(b) Describe all subgroups of $\mathbf{Z}/n\mathbf{Z}$.

Solution. If $n = cd$ for some positive integers c and d then we have a subgroup

$$\langle d \rangle = \big\{0, d, 2d, 3d, 4d, \ldots, (c-1)d\big\}.$$

Every subgroup of $\mathbf{Z}/n\mathbf{Z}$ is of this form. □

Exercise 34. (a) Let n be an integer. Show that the order of $k \in \mathbf{Z}/n\mathbf{Z}$ is $n/\gcd\{k, n\}$.

Solution. If $mk \equiv 0 \pmod{n}$ then $mk = \ell n$ so n divides mk. Therefore $n/\gcd\{k, n\}$ divides m. Conversely, if $n/\gcd\{k, n\}$ divides m hen $nk/\gcd\{k, n\}$ divides mk. Since $k/\gcd\{k, n\}$ is an integer, this means that n divides mk so $mk \equiv 0 \pmod{n}$. □

(b) Let m and n be integers. Show that there is a homomorphism $\varphi : \mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ such that $\varphi(1) = k$ if and only if $n/\gcd\{k, n\}$ divides m.

Solution. We know that homomorphisms $\varphi : \mathbf{Z}/m\mathbf{Z} \to G$, for any group G, correspond to the elements of G such that $g^m = 1$. In the case of $\mathbf{Z}/n\mathbf{Z}$, the homomorphisms $\varphi : \mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ correspond to the $k \in \mathbf{Z}/n\mathbf{Z}$ such that $mk = 0$. But $mk = 0$ if and only if the order of k divides m. We saw above that $\mathrm{ord}(k) = n/\gcd n, k$ so we deduce that $n/\gcd n, k$ divides m. □

Exercise 35. Show that if G is an **abelian** group and n is a positive integer then

$$H = \left\{ g \in G \middle| g^n = 1 \right\}$$

is a subgroup of G. (Hint: One way to solve this exercise is to show that $\varphi(g) = g^n$ is an homomorphism from G to itself.)

Solution. Let $\varphi : G \to G$ be the function $\varphi(g) = g^n$. Then $\varphi(gh) = (gh)^n = g^n h^n = \varphi(g)\varphi(h)$ because g is abelian. Therefore φ is a homomorphism so the kernel of φ (the set of all $g \in G$ such that $\varphi(g) = 1$) is a subgroup of G. But the kernel of G is precisely H. □

Solution. A second solution verifies the assertion directly, using Proposition 1: H contains 1 since $1^n = 1$; therefore H is non-empty. Also, if $g, h \in H$ then $g^n = 1$ and $h^n = 1$ so $g^n h^{-n} = 1 \cdot 1 = 1$ and $(gh^{-1})^n = g^n h^{-n}$ (because G is abelian). Thus $(gh^{-1})^n = g^n h^{-n} = 1$ so $gh \in H$. □

References

[Arm] M. A. Armstrong. *Groups and symmetry*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1988.

[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.