Math 30710
Exam 1 Solutions
October 3, 2018 **Name** _____

1. Let $S = \{a, b, c\}$ be a set consisting of three elements. S is not necessarily a group (yet). Consider a table of the form

$*$	a	b	c
a			
b			
c			

For each of the following, clearly explain your answer. In this problem I'm only looking for a number (with explanation), not a list of tables.

How many binary operations $*$ are possible (i.e. in how many ways can you fill this table) if ...

(a) (5 points) there are no conditions other than $*$ being a binary operation?

Solution:
There are 9 blanks to fill and 3 choices for each blank, with no other constraints, so there are 3^9 possibilities.

(b) (5 points) a is an identity element (no other conditions)?

Solution:
Now the first row and first column are determined and there are four blanks remaining, with no other conditions, for a total of $3^4 = 81$ possibilities.

(c) (5 points) a is not necessarily an identity element but $*$ is commutative?

Solution:
Commutativity means that the table should be symmetric about the main diagonal. Thus the bottom three leftmost entries are determined and we have to choose entries for the remaining six. There are 3^6 ways to do this.

(d) (5 points) S is a group with identity element a?

Solution:
Using the fact that we have left and right cancellation and a is an identity element, there is only one way to fill the group table:

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

2. (6 points) Consider the cycle $\sigma = (1, 2, 3, 4)$. Write σ as a product of transpositions in two different ways.

Solution:

$$(1, 2, 3, 4) = (1, 4)(1, 3)(1, 2) = (1, 2)(2, 3)(3, 4).$$

3. (10 points) The following is the group table for S_3 (with a reminder of the book's notation). To the right is a set of six vertices. Complete it to a Cayley digraph, labelling all six vertices, and using

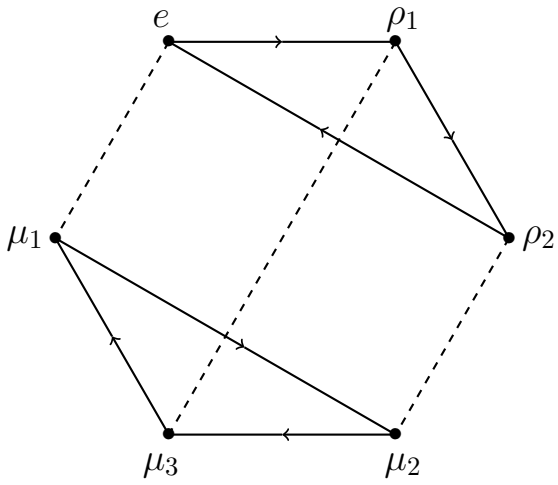
$\longrightarrow$ for ρ_1 and - - - - - - - - - - - - - - - for μ_1

as your generators. **Note that the solid line has an arrow and the dashed line doesn't!! Pay attention to the direction of the arrow.** Don't draw any unjustified conclusions from the fact that I put the vertices in the shape of a regular hexagon!

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$
$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$
$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \qquad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Solution:

	e	ρ_1	ρ_2	μ_1	μ_2	μ_3
e	e	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	e	μ_3	μ_1	μ_2
ρ_2	ρ_2	e	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	e	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	e	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	e



4. (10 points) True or false? If true, give a proof. If false, give a counterexample.

If G is an infinite group then G has infinitely many **distinct** *subgroups.*

[Hint: think about cyclic subgroups.]

Solution:

Two cases. If $\langle a \rangle$ is finite for all $a \in G$ then clearly we can find infinitely many elements a for which $\langle a \rangle$ are all distinct (just keep choosing a outside the union of all the subgroups found so far; this union is always a finite set).

So assume that for some $a \in G$, $\langle a \rangle$ is infinite. By a theorem proved in class, then $\langle a \rangle$ is isomorphic to $\mathbb{Z}$, with the isomorphism given by $\phi(a^m) = m$. Then $\langle a^p \rangle$ for p prime gives an infinite set of distinct subgroups of $\langle a \rangle$, hence distinct subgroups of G.

5. Consider the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 9 & 5 & 4 & 10 & 3 & 1 & 6 & 7 & 8 \end{pmatrix}$$

(a) (5 points) Write σ as a product of disjoint cycles.

Solution:

$$(1, 2, 9, 7)(3, 5, 10, 8, 6)$$

(b) (5 points) Write σ as a product of transpositions.

One Solution:

$$(1, 2)(2, 9)(9, 7)(3, 5)(5, 10)(10, 8)(8, 6).$$

(c) (5 points) Is σ an element of A_{10}? Why or why not?

Solution:
No, because it is the product of an odd number of transpositions.

(d) (5 points) Is σ an element of D_{10} (the 10^{th} dihedral group, i.e. the group of symmetries of a regular 10-gon)? Explain your answer. (It does not have to be a rigorous proof.)

Solution:
No. A symmetry of a regular 10-gon can't cycle four vertices one way and five another and keep one fixed. In fact, in order to keep 4 fixed it would need to keep 9 fixed too (the one directly opposite it) and be a reflection about this diagonal.

(e) (5 points) Find σ^{-1}.

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 1 & 6 & 4 & 3 & 8 & 9 & 10 & 2 & 5 \end{pmatrix}$$

6. (a) (5 points) Let $G = \langle a \rangle$ be a cyclic group and let $\phi : G \to G'$ be a group homomorphism. Suppose that $\phi(a)$ is known. Explain how you then know $\phi(x)$ for any $x \in G$.

Solution:
Since $G = \langle a \rangle$ is cyclic, any element of G is of the form $x = a^m$ for some m. Then

$$\phi(x) = \phi(a^m) = (\phi(x))^m$$

so if we know $\phi(a)$ then we know $\phi(x)$.

(b) (5 points) Give an example of a one-to-one homomorphism ϕ from $(\mathbb{Z}_4, +)$ to $(\mathbb{C}^*, \times)$. Thanks to part (a), you can answer this question by just giving me $\phi(1)$. But be sure to explain why this ϕ is well-defined.

Solution:
We have to satisfy the equation

$$1 = \phi(0) = \phi(1 + 1 + 1 + 1) = \phi(1)^4.$$

(remember that for a homomorphism $\phi : G \to G'$ we have to have $\phi(e) = e'$ and here $e = 0$ and $e' = 1$). So we need to find a non-zero complex number whose 4th power is 1. So we have $\phi(1) = i$ or $\phi(1) = -i$. We can't take $\phi(1) = -1$ because then $\phi(2) = \phi(1 + 1) = \phi(1)^2 = 1$ so $\phi(0) = \phi(2)$ and ϕ isn't 1-1.

7. Let G be a finite group of even order $2n$.

   (a) (5 points) Prove that G must contain at least one element of order 2. [Hint: explain why another way to say this is that other than the identity element e, G has to contain at least one other element that is equal to its own inverse. Then pair off each element with its inverse.]

   Solution:
   If x has order 2 then $x^2 = e$ so x is its own inverse. Order 2 also means x is not itself the identity. Suppose that G does not have any elements of order 2, so other than the identity no element is its own inverse. Then we can pair off each element other than e with its inverse, and so
   $$\{g_1, g_1^{-1}, g_2, g_2^{-1}, \dots\} = G \backslash \{e\}$$
   is a set with an even number of elements. The only element missing is e, so G must have an odd number of elements. Contradiction.

   (b) (9 points) Suppose that G is an **abelian** group. If a and b are distinct elements of order 2, prove the following. [Remember that the identity element has order 1, not 2. The fact that G has order $2n$ is not relevant to this part.]

   Solution:
   - First note $(ab)^2 = abab = aabb = a^2b^2 = e$. (We used the fact that G is abelian here.) This shows either $ab = e$ or ab has order 2. We'll show $ab \neq e$ in the third bullet.
   - $ab \neq a$ by left cancellation, since otherwise $b = e$ and this contradicts the assumption that b has order 2 (and not 1). Similarly $ab \neq b$ by right cancellation.
   - $ab \neq e$ since if $ab = e$ we would have $b = a^{-1} = a$ and we assumed that a and b were distinct.

   (c) (5 points) Now suppose that G is an **abelian** group of order $2n$, **where n is odd**. Using the previous parts of this problem (whether you were able to solve them or not), show that G contains *exactly* one element of order 2. [Hint: Lagrange's theorem.]

   Solution:
   We saw in (a) that G has at least one element of order 2. Suppose that b is another element of order 2. By (b), we have that ab also has order 2, and is not equal to either a or b. Then $\{e, a, b, ab\}$ is a subgroup (isomorphic to the Klein group) of order 4. Thus $|G|$ has to be divisible by 4 by Lagrange's theorem. Since G has order $2n$ with n odd, this is impossible.

   A number of people said that since 2 divides $2n$ only once (since n is odd), it follows that there is only one subgroup of order 2. This is not true. For example, $G = S_3$ has order $6 = 2 \cdot 3$ but S_3 has three elements of order 2, hence three subgroups of order 2. Namely
   $$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

(Extra sheet.)