MATH 150A Winter 2020 - **Problem Set 3 solutions**

due January 31

1. Let G be a group generated by set A. Prove that if a and b commute for all $a, b \in A$, then G is abelian.

   First note that $ab = ba$ implies $ba^{-1} = a^{-1}b$. Let B be the set of inverses of the elements in A. Then all of the elements in $A \cup B$ commute with each other.

   Since A generates G, for any $g, h \in G$, g and h can be expressed as

$$g = a_1 a_2 \cdots a_k,$$

$$h = b_1 b_2 \cdots b_\ell,$$

   with $a_1, \ldots, a_k, b_1, \ldots, b_\ell \in A \cup B$. Since each a_i commutes with each b_j, we have

$$gh = a_1 \cdots a_k b_1 \cdots b_\ell = b_1 \cdots b_\ell a_1 \cdots a_k = hg.$$

   So G is abelian.

2. Prove that if group G has order 4 then G is cyclic or G is isomorphic to the Klein four group.

   Let $G = \{e, a, b, c\}$ with e the identity. The elements of G can have order 1, 2 or 4. If G has any elements of order 4, it is cyclic. Otherwise, a, b, c each have order 2, so $a^2 = b^2 = c^2 = e$. Now consider the product ab. Since a and b are not the identity, ab cannot be equal to a or b. And since $aa = e$, $ab \neq e$. The only possible value then is $ab = c$. Similarly, we get $ba = c$, $ac = ca = b$ and $bc = cb = a$. Therefore all values of the operation table are determined, so there is only one isomorphism class for groups with order 4 that are not cyclic. The Klein four group also has order 4 and is not cyclic, so it must be isomorphic to G.

3. For group G, $\mathrm{Aut}(G)$ denotes the *automorphism group* of G, whose elements are all automorphisms $G \to G$ and with composition as the operation.

   (a) Prove that $\mathrm{Aut}(G)$ is in fact a group.

   The composition of two isomorphisms is an isomorphism, so $\mathrm{Aut}(G)$ is closed under the operation. Function composition is associative, and the identity function $\mathrm{id}_G : G \to G$ is in $\mathrm{Aut}(G)$ so $\mathrm{Aut}(G)$ has an identity element. For any automorphism φ, we proved that φ^{-1} is also an isomorphism, so $\varphi^{-1} \in \mathrm{Aut}(G)$. Therefore $\mathrm{Aut}(G)$ is a group.

   (b) Let $\gamma : G \to \mathrm{Aut}(G)$ be defined by $g \mapsto \varphi_g$ where $\varphi_g : G \to G$ is the map that conjugates by g, $\varphi_g(x) = gxg^{-1}$. Prove that γ is a group homomorphism.
   For all $g, h, x \in G$,

$$\gamma(gh)(x) = (gh)x(gh)^{-1} = ghxh^{-1}g^{-1} = \gamma(g)(hxh^{-1})$$

$$= \gamma(g)(\gamma(h)(x)) = (\gamma(g) \circ \gamma(h))(x).$$

Therefore $\gamma(gh) = \gamma(g) \circ \gamma(h)$ so γ is a homomorphism.

4. (2.5.2) Find all automorphisms of

   (a) the cyclic group of order 10.

   Let C_{10} be generated by x. An automorphism of C_{10} must send the generator x to a generator. The other generators of C_{10} are x^3, x^7, x^9. Therefore the four automorphisms of C_{10} are

   $$x^k \mapsto x^k,$$
   $$x^k \mapsto x^{3k},$$
   $$x^k \mapsto x^{7k},$$
   $$x^k \mapsto x^{9k}.$$

   (b) the symmetric group S_3.

   S_3 has 3 elements of order 2, which are the swaps $(1\ 2), (1\ 3), (2\ 3)$ (written in cycle notation), and the set of swaps generates S_3. There are six automorphisms of S_3 obtained by conjugating by each of the six elements in S_3. It can be checked that these six maps permute the three swaps in all possible ways. Any automorphism of S_3 must send degree 2 elements to degree 2 elements so it must permute the swaps. Since the swaps generate S_3, any automorphism is determined by how it acts on swaps. Therefore every automorphisms of S_3 is equal to one of the six conjugation maps.

5. (2.7.1) Let G be a group and define the relation $\sim$ on G by $a \sim b$ if $b = gag^{-1}$ for some $g \in G$ (in which case we say a and b are *conjugates*).

   (a) Prove that $\sim$ is an equivalence relation. Reflexive: For any $a \in G$, $a = 1a1^{-1}$ so $a \sim a$.

   Symmetric: If $a \sim b$ then $b = gag^{-1}$ for some $g \in G$. Then $a = g^{-1}b(g^{-1})^{-1}$ so a the conjugation of b by $g^{-1} \in G$. Therefore $b \sim a$.

   Transitive: If $a \sim b$ and $b \sim c$, then $b = gag^{-1}$ and $c = hbh^{-1}$ for some $g, h \in G$. Then $c = hgag^{-1}h^{-1} = (hg)a(hg)^{-1}$ so c is the conjugation of a by $hg \in G$. Therefore $a \sim c$.

   (b) The equivalence classes of $\sim$ are called *conjugacy classes*. For $a \in G$, prove that a is in the center of G if and only if its conjugacy class is $\{a\}$.

   If the conjugacy class of a is $\{a\}$ then $gag^{-1} = a$ for all $g \in G$, so $ga = ag$ for all $g \in G$, meaning that a commutes with everything.

   If a is in the center of G, then $ga = ag$ for all $g \in G$, so $gag^{-1} = a$. Therefore a is only conjugate to itself, so its conjugacy class is $\{a\}$.

6. Let H be the *quaternion group*, which can be represented as the group of matrices

$$H = \{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$$

where

$$\mathbf{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \ \mathbf{i} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \ \mathbf{j} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \ \mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

The elements of H satsify the relations

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}, \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \quad \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \quad \mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

Find the conjugacy classes of H, and the center of H.

It can be checked that $\mathbf{1}$ and $-\mathbf{1}$ commute with the other elements, so $\{\mathbf{1}\}$ and $\{-\mathbf{1}\}$ are conjugacy classes. Then $\mathbf{i}$ commutes with $\pm\mathbf{1}$ and $\pm\mathbf{i}$ so to find the conjugacy class of $\mathbf{i}$ we only have to check what happens when conjugated by $\mathbf{j}$ or $\mathbf{k}$.

$$\mathbf{jij}^{-1} = \mathbf{ji}(-\mathbf{j}) = -\mathbf{ij}(-\mathbf{j}) = -\mathbf{i1} = -\mathbf{i}.$$

$$\mathbf{kik}^{-1} = \mathbf{ki}(-\mathbf{k}) = -\mathbf{ik}(-\mathbf{k}) = -\mathbf{i1} = -\mathbf{i}.$$

Therefore $\{\pm\mathbf{i}\}$ is a conjugacy class. A similar computation shows that $\{\pm\mathbf{j}\}$ and $\{\pm\mathbf{k}\}$ are also conjugacy classes. The center of H is $\{\pm\mathbf{1}\}$ since these elements have singleton conjugacy classes.

7. (2.8.4) Let G be a group of order 35.

   (a) Prove that G contains an element a of order 5.

   The possible orders of elements of G are 1, 5, 7 or 35. If G has an element x of order 35, then x^7 has order 5.

   Assume that G has no elements of order 5. Then all 34 non-identity elements must have order 7. Let x be a non-identity element, so

   $$\langle x \rangle = \{1, x, x^2, x^3, x^4, x^5, x^6\}.$$

   Each of the non-identity elements in $\langle x \rangle$ generates the same cyclic subgroup $\langle x \rangle$. On the other hand for any $y \notin \langle x \rangle$, the cycles have $\langle x \rangle \cap \langle y \rangle = \{1\}$. Therefore the cycles partition the non-identity elements of G into sets of size 6. However 34 is not a multiple of 6, so this is a contradiction. G must have an element a of order 5.

   (b) Prove that G contains an element b of order 7.

   Run the same argument as in part (a) with 5 and 7 switched. 34 is not a multiple of 4, so G must contain an element b of order 7.

   (c) Prove that $\langle a, b \rangle = G$.

   [Hint: show that the elements $a^n b^m$ with $0 \le n < 5$ and $0 \le m < 7$ are distinct.]

   Suppose $a^{n_1} b^{m_1} = a^{n_2} b^{m_2}$ with $0 \le n_1, n_2 < 5$ and $0 \le m_1, m_2 < 7$. Then $a^{n_1 - n_2} = b^{m_2 - m_1}$. If $n_1 \ne n_2$ then $0 < |n_1 - n_2| < 5$ so $a^{n_1 - n_2}$ has order 5. However since b has order 7, $b^{m_2 - m_1}$ cannot have order 5 which is a contadiction.

   Therefore $n_1 = n_2$. By left-cancellation, $b^{m_1} = b^{m_2}$ so $b^{m_2 - m_1} = 1$. Since b has order 7, $m_2 - m_1$ must be a multiple of 7. Note that $|m_2 - m_1| < 7$ so then $m_1 = m_2$.

   The above shows that $\langle a, b \rangle$ has 35 distinct elements so it must equal to G.