**THE CHINESE UNIVERSITY OF HONG KONG**
**Department of Mathematics**
**MATH 3030 Abstract Algebra 2023-24**
**Homework 6**
**Due Date: 26th October 2023**

## Compulsory Part

1. Let $X$ be a $G$-set. Show that $G$ acts faithfully on $X$ if and only if no two distinct elements of $G$ have the same action on each element of $X$.

   *Proof.* ($\Rightarrow$) Suppose that $G$ acts faithfully on $X$, and if $g_1, g_2$ have the same action on every element of $X$, then $g_1 x = g_2 x$ for all $x \in X$. So that $g_2^{-1} g_1 \cdot x = g_2^{-1} g_2 \cdot x = x$ for all $x \in X$, then $g_2^{-1} g_1 = e$, in other words $g_1 = g_2$.

   ($\Leftarrow$) Conversely, if no two elements of $G$ have the same actions on $X$, this implies that the associated homomorphism $\rho : G \to S_X$ satisfies $\rho(g_1) \neq \rho(g_2)$ for $g_1 \neq g_2$, therefore $\rho(g) \neq \rho(e) = \mathrm{id}$ for any $g \neq e$. So $G$ acts faithfully.

2. Let $X$ be a $G$-set and let $Y \subseteq X$. Show that $G_Y := \{g \in G : gy = y \text{ for all } y \in Y\}$ is a subgroup of $G$.

   *Proof.* Let $g, h \in G_Y$, then $gy = hy = y$ for all $y \in Y$, therefore $y = h^{-1}hy = h^{-1}y$ and $ghy = g(hy) = gy = y$. Also note that $e \in G_Y$ so it is nonempty, therefore it forms a subgroup.

3. Let $G$ be the additive group of real numbers. Let the action of $\theta \in G$ on the real plane $\mathbb{R}^2$ be given by rotating the plane counterclockwise about the origin through $\theta$ radians. Let $P$ be a point other than the origin in the plane.

   (a) Show that $\mathbb{R}^2$ is a $G$-set.

   (b) Describe geometrically the orbit containing $P$.

   (c) Find the group $G_P$.

   *Proof.*

   (a) We can describe the action by either using matrices or complex coordinates. Here we use the latter, we identify $\mathbb{R}^2$ and $\mathbb{C}$ by $(x, y) \leftrightarrow x + iy$. Then rotation of $z = x + iy$ about the origin by $\theta$ radian can be written as $\rho : G \times \mathbb{R}^2 \to \mathbb{R}^2$ by $\rho(\theta, x + iy) = e^{i\theta}(x + iy)$.

   Then we can see that $G$ acts on $\mathbb{R}^2$ since $(\theta_1 + \theta_2) \cdot (x + iy) = e^{i\theta_1 + i\theta_2}(x + iy) = e^{i\theta_1} e^{i\theta_2}(x + iy) = \theta_1 \cdot (\theta_2 \cdot (x + iy))$; where we have used $\cdot$ to denote action. And for $\theta = 0$, we have $0 \cdot (x + iy) = e^0(x + iy) = x + iy$ so $0 \in \mathbb{R}$ acts by identity.

   (b) The orbit containing $P$ is the circle centered at origin with radius $|P|$, since $|e^{i\theta} P| = |P|$ for any $\theta \in \mathbb{R}$.

   (c) $e^{i\theta} P = P$ if and only if $e^{i\theta} = 1$, this occus precisely when $\theta \in 2\pi\mathbb{Z}$. So $G_P = 2\pi\mathbb{Z}$.

4. Let $H$ be a subgroup of $G$, and let $L_H$ be the set of all left cosets of $H$ in $G$. Show that there is a well-defined action of $G$ on $L_H$ given by $g(aH) = (ga)H$ for $g \in G$ and $aH \in L_H$. We call $L_H$ a **left coset $G$-set**.

   *Proof.* We will first show that this is well-defined, i.e. we take $\rho : G \times L_H \to L_H$ by $\rho(g, aH) = (ga)H$. Then $\rho$ does not depend on the representative of the coset. Say $aH = bH$, then $b^{-1}a \in H$. Rewriting $b^{-1}a = b^{-1}g^{-1}ga$, we see that $(ga)H = (gb)H$, therefore the function $\rho$ is well-defined. Now consider $\rho(e, aH) = e(aH) = aH$, we see that $e \in G$ acts by identity map. And $\rho(g', \rho(g, aH)) = g'(ga)H = (g'ga)H = (g'g)aH = \rho(g'g, aH)$. So it indeed defines a group action.

5. Let $H < G$. The **centralizer** of $H$ is the set

$$Z_G(H) := \{g \in G : ghg^{-1} = h \text{ for all } h \in H\},$$

   and the **normalizer** of $H$ is the set

$$N_G(H) := \{g \in G : gHg^{-1} = H\}.$$

   (a) Show that $N_G(H)$ is the largest subgroup of $G$ in which $H$ is normal.

   (b) Show that $Z_G(H)$ is a normal subgroup of $N_G(H)$.

   (c) Show that the quotient group $N_G(H)/Z_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

   *Proof.*

   (a) Let $K$ be any subgroup of $G$ so that $K$ contains $H$ and $H$ is normal in $K$. Let $g \in K$, by assumption $gHg^{-1} = H$, therefore $g \in N_G(H)$. Therefore $K \leq N_G(H)$.

   (b) Let $g \in N_G(H)$, and $z \in Z_G(H)$, then for any $h \in H$, note that $gzg^{-1}h = gzg^{-1}hgg^{-1}$. But $g^{-1} \in N_G(H)$ implies that $g^{-1}hg \in H$, so that $z$ commutes with this element. So we have $gzg^{-1}hgg^{-1} = gg^{-1}hgzg^{-1} = h(gzg^{-1})$. This shows that $gzg^{-1}$ commutes with all $h \in H$, so that it lies in $Z_G(H)$.

   (c) We will define a homomorphism $\varphi$ from $N_G(H)$ to $\mathrm{Aut}(H)$ as follows. $\varphi_g(h) = ghg^{-1}$. This is well-defined by definition of noramlizer, and $\ker\varphi = \{g \in G : ghg^{-1} = h \text{ for all } h \in H\} = Z_G(H)$. Therefore by first isomorphism theorem $N_G(H)/Z_G(H) \cong \mathrm{im}(\varphi) \leq \mathrm{Aut}(H)$.

6. Show that $S_3$ can never act transitively on a set with $5$ elements.

   *Proof.* Suppose $S_3$ acts transitively on a set $X$ with 5 elements, then by orbit stabilizer theorem, the orbit of any element is simply $X$ and has cardinality $5$, and stabilizer of any element is a subgroup of $S_3$, so it has order $1, 2, 3$ or $6$. Therefore we have $|G| = 6 = 5|G_x|$, this is clearly impossible.

7. Let $G$ be a group which contains an element $a$ whose order is at least 3. Show that $|\mathrm{Aut}(G)| \geq 2$.

   *Proof.* If $G$ is nonabelian, then there exists some $g, h$ so that $gh \neq hg$, in that case $h \mapsto ghg^{-1}$ defines a nontrivial automorphism of $G$, so that $|\mathrm{Aut}(G)| \geq 2$.

   Otherwise suppose that $G$ is abelian, and contains an element $a$ of order at least $3$. Then $g \mapsto g^{-1}$ is a well-defined automorphism of $G$ since it is abelian, and it is nontrivial because $a^{-1} \neq a$.

8. Let $G$ be a group whose order is a prime power (i.e. a $p$-**group** for some prime $p$). Let $N$ be a nontrivial normal subgroup of $G$. Show that $N \cap Z(G) \neq \{e\}$.

   *Proof.* Let $N$ be any nontrivial normal subgroup of $G$, then $G$ acts on $N$ by conjugation. The fixed point sets under this action $N_G$ consists of those elements in $N$ so that $gng^{-1} = n$ for all $g \in G$, i.e. $N_G = N \cap Z(G)$. Then the class equation gives

   $$|N| = |N_G| + \sum_{i=1}^{k} [G : G_{x_i}].$$

   Here the sum is taken over representatives $x_i$ of each orbit of size greater than 1. By assumption, the stabilizers $G_{x_i}$ are proper subgroups of $G$, so the index is a positive power of $p$. Since both $|N|$ and the sum on the RHS of the equation are powers of $p$, it follows that $|N_G| = |N \cap Z(G)| \neq 1$.

**Optional Part**

1. Let $\{X_i : i \in I\}$ be a disjoint collection of sets, meaning that $X_i \cap X_j = \emptyset$ for $i \neq j$. Suppose that each $X_i$ is a $G$-set for the same group $G$.

   (a) Show that $\bigcup_{i \in I} X_i$ can naturally be viewed as a $G$-set; we called it the **union** of the $G$-sets $X_i$.

   (b) Show that every $G$-set $X$ is the union of its orbits.

   *Proof.*

   (a) Denote $\rho_i : G \times X_i \to X_i$ be the $G$-actions on $X_i$, then for $X = \bigsqcup_{i \in I} X_i$, we can define $\rho : G \times X \to X$ by $\rho(g, x) = \rho_i(g, x)$ for $x \in X_i$. This is a $G$-action because for $x \in X_i$, $\rho_i(g, x) \in X_i$ and hence $\rho(g_1, \rho(g_2, x)) = \rho_i(g_1, \rho_i(g_2, x)) = \rho_i(g_1 g_2, x) = \rho(g_1 g_2, x)$. And $\rho(e, x) = \rho_i(e, x) = x$.

   (b) Clearly every element $x \in X$ falls into a unqiue orbit $G \cdot x$, and different orbits are disjoint from each other. So we can pick a representative $x_i$ in each orbit and it will give a partition of $X$ as a set. That is, $X = \bigsqcup_{i \in I} G \cdot x_i$. The restriction of the $G$-action on each orbit turns the orbits into $G$-sets since they are closed under the action of $G$. It is clear that the $G$-actions on both sides are the same.

2. Let $X$ and $Y$ be $G$-sets with the *same* group $G$. An **isomorphism** between the $G$-sets $X$ and $Y$ is a bijection $\phi : X \to Y$ which is **equivariant**, i.e. such that $g\phi(x) = \phi(gx)$ for all $x \in X$ and $g \in G$. Two $G$-sets are **isomorphic** if there exists an equivariant bijection between them.

   Let $X$ be a transitive $G$-set, and let $x_0 \in X$. Show that $X$ is isomorphic to the $G$-set $L$ of all left cosets of $G_{x_0}$. [*Hint:* For $x \in X$, suppose $x = gx_0$, and define $\phi : X \to L$ by $\phi(x) = gG_{x_0}$. Be sure to show that $\phi$ is well-defined!]

   *Proof.* Fix $x_0 \in X$, define $\phi : X \to L$ by $\phi(x) = gG_{x_0}$, where $x = g \cdot x_0$. For $x = g_1 x_0 = g_2 x_0$, we have $g_2^{-1} g_1 x_0 = x_0$, hence $g_2^{-1} g_1 \in G_{x_0}$. Therefore $\phi(x) = g_1 G_{x_0} = g_2 G_{x_0}$ is well-defined independent of the choice of $g$. This map is equivariant because $\phi(hx) = hgG_{x_0}$ for $hx = hgx_0$. This map is surjective because given any coset $gG_{x_0}$, we have $\phi(gx_0) = gG_{x_0}$. And it is injective because $gG_{x_0} = g'G_{x_0}$ if and only if $g = g'h$ for some stabilizer $h \in G_{x_0}$, this is equivalent to $gx_0 = g'x_0$.

3. Let $X_i$ for $i \in I$ be $G$-sets for the same group $G$, and suppose that the sets $X_i$ are not necessarily disjoint. Let $X_i' = \{(x, i) : x \in X_i\}$ for each $i \in I$. Then the sets $X_i'$ are disjoint, and each can still be regarded as a $G$-set in an obvious way. (The elements of $X_i$ have simply been tagged by $i$ to distinguish them from the elements of $X_j$ for $i \neq j$.) The $G$-set $\bigcup_{i \in I} X_i'$ is called the **disjoint union** of the $G$-sets $X_i$. Show that every $G$-set is isomorphic to a disjoint union of left coset $G$-sets. (Therefore, left coset $G$-sets are *building blocks* of $G$-sets.)

   *Proof.* This statement follows from Q1b and Q2. By Q1b, every $G$-set can be decomposed into disjoint union of its orbits. Clearly $G$ acts transitively when restricted to each orbit, therefore by Q2, it is isomorphic to a left cosets. Putting these together, any $G$-set is isomorphic to a disjoint union of $G$-sets which are isomorphic to left cosets.

4. Let $G$ be a group. Show that $G/Z(G)$ is isomorphic to $\mathrm{Inn}(G)$, the set of all inner automorphisms of $G$. Use this to give another proof of the fact that if $G/Z(G)$ is cyclic, then $G$ is abelian.

   *Proof.* Define $G \mapsto \mathrm{Inn}(G)$ to be the obvious homomorphism $I : g \mapsto (i_g : x \mapsto gxg^{-1})$. Then by definition it is surjective, with kernel given by those $g \in G$ so that $i_g = \mathrm{id}_G$. In other words $g \in \ker(I)$ if and only if $gxg^{-1} = x$ for all $x \in G$, therefore $\ker(I) = Z(G)$. By first isomorphism theorem, it follows that $G/Z(G) \cong \mathrm{Inn}(G)$. Suppose $\mathrm{Inn}(G)$ is cyclic, say $i_g$ is a generator, then for each $h \in G$, $hxh^{-1} = g^k x g^{-k}$ for all $x \in G$. In particular, taking $x = g$, we get $hgh^{-1} = g$. Since $h \in G$ is arbitrary, this implies $g \in Z(G)$. This means that $G/Z(G) \cong \mathrm{Inn}(G) \cong 1$, i.e. $G = Z(G)$ is abelian.

5. Let $G$ be a finite group, and let $H \leq G$ be a subgroup of index $p$, where $p$ is the smallest prime which divides $|G|$.

   (a) Write the action of $G$ on the set $G/H$ of left cosets by left multiplication as a homomorphism $\rho : G \to S_p$, where $S_p$ denotes the $p$-th symmetric group.

   (b) Show that $\ker \rho \leq H$.

   (c) Further show, by using the hypothesis, that $H = \ker \rho$. Hence, conclude that $H$ is normal in $G$.

   *Proof.*

   (a) $G$ acts on the left coset space $G/H$ by left multiplication, i.e. $\rho_g : G/H \to G/H$ is defined by $\rho_g(aH) = gaH$. Since $[G : H] = |G/H| = p$, we may regard $\rho_g$ as a permutation of $\{1, ..., p\}$ by picking any bijection between $\{1, ..., p\}$ and $G/H$, thus $\rho : g \mapsto \rho_g$ defines a homomorphism from $G$ to $S_p$.

   (b) Let $g \in \ker \rho$, then $\rho_g = \mathrm{id} : G/H \to G/H$, in particular $\rho_g(H) = gH = H$, thus $g \in H$.

   (c) Assume further that $H = \ker \rho$, then then $h \in H$ acts trivially on $G/H$, i.e. $\rho_h(aH) = haH = aH$ for any $aH \in G/H$. Therefore $a^{-1}ha \in H$ for any $a \in G$ and $h \in H$, i.e. $H$ is normal.

6. Let $G$ be a finite group, and let $H \leq G$ be a subgroup of index $n$. Prove that $H$ contains a subgroup $K$ which is normal in $G$ and such that $[G : K]$ divides the gcd of $|G|$ and $n!$. [*Hint:* Use the strategy of the preceding exercise.]

*Proof.* As in Q5, the left multiplication action on $G/H$ coset space defines a homomorphism $\rho : G \to S_n$. Therefore, $G/\ker\rho \cong \mathrm{im}(\rho) \leq S_n$. Take $K = \ker\rho$, then $K$ is a normal subgroup of $G$, with $[G : K] = |\mathrm{im}(\rho)|$ dividing $|S_n| = n!$, so it divides the $\gcd$ of $|G|$ and $n!$.

*Remark:* In particular, if a group $G$ has a subgroup of index $n$, and $|G| > n!$, then $G$ necessarily have a proper nontrivial normal subgroup, then it must not be a simple group.