Problem Set 4 solutions

Problem 1. Prove that if $f : G \to H$ is a group homomorphism and $K \le H$ then the **preimage** of K, defined as
$$f^{-1}(K) := \{g \in G | f(g) \in K\}$$
is a subgroup of G.

Proof. Since f is a homomorphism, $f(e_G) = e_H \in K$, and thus $e_H \in f^{-1}(K) \neq \emptyset$.

If $x, y \in f^{-1}(K)$, then $f(x) \in K$ and $f(y) \in K$. Since f is a homomorphism and K is closed under multiplication and taking inverses,
$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} \in K,$$
and thus $xy^{-1} \in f^{-1}(K)$. By the One-step subgroup test, we conclude that $f^{-1}(K)$ is a subgroup of G. □

Problem 2. Let G be a group and $a \in G$. Let
$$C_G(a) := \{x \in G \mid xa = ax\}.$$
Prove that $C_G(a)$, called the **centralizer** of a in G, is a subgroup of G.

Proof. First, note that $e \in C_G(a)$, and thus $C_G(a)$ is nonempty. Let $x \in C_G(a)$, so that $xa = ax$. Multiplying on the left and right by x^{-1}, we obtain $ax^{-1} = x^{-1}a$. Thus, $x^{-1} \in C_G(a)$.

Now let $x, y \in C_G(a)$. Then
$$\begin{aligned}(xy)a &= x(ya) && \text{by associativity}\\ &= x(ay) && \text{since } y \in C_G(a)\\ &= (xa)y && \text{by associativity}\\ &= (ax)y && \text{since } x \in C_G(a)\\ &= a(xy) && \text{by associativity.}\end{aligned}$$
By the Two-step test, $C_G(a)$ is a subgroup of G. □

Problem 3. Let G be a group and H and H' subgroups of G. Prove that $H \cup H'$ is a subgroup of G if and only if $H \subseteq H'$ or $H' \subseteq H$.

Proof. ($\Leftarrow$) We either have $H \cup H' = H$ or $H \cup H' = H'$, which are both subgroups.

($\Rightarrow$) Suppose by way of contradiction that $H \cup H'$ is a subgroup but $H \not\subset H'$ and $H' \not\subset H$. Choose $a \in H \setminus H'$ and $b \in H' \setminus H$. Then $a, b \in H \cup H'$, and since $H \cup H'$ must be closed for the multiplication, we conclude that $ab \in H \cup H'$. But if $ab \in H$, then multiplying on the left by a^{-1} gives $b \in H$, a contradiction. A similar contradiction holds if $ab \in H'$. Thus $ab \notin H \cup H'$. □

Problem 4. Suppose H and K are subgroups of G of relatively prime (hence, finite) order. Prove that $H \cap K = \{1\}$.

Proof. Let $x \in H \cap K$. Then the order of x divides the orders of H and K by Lagrange's Theorem. But the orders of H and K are relatively prime, so the order of x must be 1. Therefore, x must be the identity. □

Problem 5. Let G be a group and $x \in G$. Consider the map $\psi_x : G \to G$ that for each $a \in G$ is given by

$$\psi_x(a) = xax^{-1}.$$

(a) Prove that $\psi_x \in \mathrm{Aut}(G)$ for all $x \in G$.

Proof. We first prove ψ_x is a homomorphism. Given $a, b \in G$, we have

$$\psi_x(ab) = x(ab)x^{-1} = (xax^{-1})(xbx^{-1}) = \psi_x(a)\psi_x(b).$$

We have shown in class that $x \cdot a = xax^{-1}$ determines an action of G on G, so let $\rho\colon G \to \mathrm{Perm}(G)$ be the corresponding group homomorphism. Note that $\psi_x = \rho(x)$, and thus ψ_x is a bijection. We conclude that ψ_x is an isomorphism.

Alternatively, we can prove that ψ_x is a bijection by constructing an explicit inverse. First, we claim that $\psi_x \circ \psi_y = \psi_{xy}$ for all $x, y \in G$. Indeed, for all $a \in G$ we have

$$(\psi_x \circ \psi_y)(a) = \psi_x(\psi_y(a)) = \psi_x(yay^{-1}) = x(yay^{-1})x^{-1} = (xy)a(xy)^{-1} = \psi_{xy}(a).$$

Hence, $\psi_x \circ \psi_y = \psi_{xy} \in H$. From this, it follows that

$$\psi_x \circ \psi_{x^{-1}} = \psi_e = \mathrm{id}_G \quad \text{and} \quad \psi_{x^{-1}} \circ \psi_x = \mathrm{id}_G.$$

Hence, $\psi_{x^{-1}}$ is an inverse for ψ_x, so ψ_x is necessarily bijective and thus an isomorphism. □

(b) Prove that $\{\psi_x \mid x \in G\}$ is a subgroup of $\mathrm{Aut}(G)$.

Proof. Let $H = \{\psi_x \mid x \in G\}$. To show H is a subgroup, note first that H is nonempty since $\psi_e \in H$. We showed already above that for all $\psi_x, \psi_y \in H$, $\psi_x \circ \psi_y = \psi_{xy} \in H$, so H is closed for the product. Finally, we also proved already that for all $x \in G$, $(\psi_x)^{-1} = \psi_{x^{-1}} \in H$, so H is closed under inverses. Thus, H is a subgroup of $\mathrm{Aut}(G)$ by the Two-step test. □

Problem 6. Prove Lagrange's Theorem:

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Hint: Let H act on G by left multiplication, that is, define $h \cdot g = hg$ for any $h \in H$ and $g \in G$. You may use without checking that this is a group action. What is the size of each orbit?

Proof. Let H act on G by left multiplication. We show that every orbit of this action has size $|H|$. Indeed, consider $g \in G$ and define a function

$$H \xrightarrow{\ f\ } \mathcal{O}_H(g)$$
$$g \longmapsto f(g) = h \cdot g = hg.$$

I claim this function is bijective. First, note that it is surjective by construction. To see it is injective, assume $f(h) = f(h')$. Then $hg = h'g$, and by the cancellation property we conclude that $h = h'$, which shows f is injective. Now since f is bijective we conclude that $|H| = |\mathcal{O}_H(g)|$.

The orbits for this action form a partition of G. Since G is finite, there are finitely many orbits, so we choose representatives $g_1, \ldots, g_k$ for each distinct orbit, and we have a disjoint union

$$G = \bigcup_{i=1}^{j} \mathcal{O}_H(g_i).$$

Therefore we have

$$|G| = \sum_{i=1}^{k} |\mathcal{O}_H(g_i)| = \sum_{i=1}^{k} |H| = k|H|,$$

and thus $|H|$ divides $|G|$. □