Problem Set 6
solutions

Problem 1. Let H be a subgroup of G.

(1.1) Fix $g \in G$. Prove that $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ is a subgroup of G of the same order as H.

Note: we are not assuming that H is finite, so you must show that there is a bijection between H and gHg^{-1}.

Proof. Since
$$e = geg^{-1} \in gHg^{-1},$$
then $gHg^{-1} \neq \emptyset$. For any $x, y \in H$, we have
$$(gxg^{-1})(gyg^{-1})^{-1} = gxg^{-1}gy^{-1}g^{-1} = g(xy^{-1})g^{-1} \in gHg^{-1}.$$
By the One-Step subgroup test, it follows that gHg^{-1} is a subgroup of G.

The map given by conjugation by g
$$\begin{aligned} H &\xrightarrow{c_g} gHg^{-1} \\ x &\longmapsto gxg^{-1} \end{aligned}$$
is surjective by the definition of the set gHg^{-1}. Furthermore,
$$c_g(x) = c_g(y) \iff gxg^{-1} = gyg^{-1} \iff x = y,$$
where on the last step we multiplied by g on the right and g^{-1} on the left, or their inverses to get $(\Leftarrow)$. thus c_g is injective. Therefore, c_g is a bijection and we conclude that $|H| = |gHg^{-1}|$. □

(1.2) Show that if H is the unique subgroup of G of order $|H|$, then $H \trianglelefteq G$.

Proof. Let $g \in G$. If H is the unique subgroup of G of order $|H|$, then by part (a) we have $gHg^{-1} = H$. Multiplying by g on the right, we conclude that $Hg = gH$. This holds for for all $g \in G$, hence from a criterion for normality proven in class we conclude that $H \trianglelefteq G$. □

Problem 2.

(2.1) Let A and B be groups and let $f : A \to B$ be any homomorphism of groups. Prove that if A is finite, then $|\operatorname{im}(f)|$ divides $|A|$.

Proof. By the First Isomorphism Theorem, $\operatorname{im}(f) \cong A/\ker(f)$, and hence
$$|\operatorname{im}(f)| = |A/\ker(f)| = \frac{|A|}{|\ker(f)|}$$
where the last equality follows from Lagrange's Theorem. Thus $|\operatorname{im}(f)|$ divides $|A|$. □

(2.2) Let G be a finite group, and let H and N be subgroups of G such that $|H|$ and $[G : N]$ are relatively prime. Prove that if $N \trianglelefteq G$ then $H \subseteq N$.

Proof. Let $i : H \to G$ be the inclusion homomorphism and $\pi : G \to G/N$ be the canonical projection. Then

$$f = \pi \circ i \colon H \to G/N$$

is also a homomorphism, as the composition of homomorphisms is a homomorphism. Note that $f(h) = hN$ for any $h \in H$. By part (a), $|\operatorname{im}(f)|$ divides $|H|$. Moreover, $\operatorname{im}(f)$ is a subgroup of G/N, so by Lagrange's Theorem, $|\operatorname{im}(f)|$ also divides $|G/N| = [G : N]$. Thus $|\operatorname{im}(f)|$ divides both $|H|$ and $[G : N]$. Since $|H|$ and $[G : N]$ are relatively prime, we conclude that $|\operatorname{im}(f)| = 1$ and hence f is the trivial map. Therefore, for all $h \in H$ we have $hN = f(h) = N$, which implies that $h \in N$. We conclude that $H \subseteq N$. □

Alternative proof. We can instead apply the Second Isomorphism Theorem to get that

$$H/(H \cap N) \cong HN/N$$

and hence $|H/(H \cap N)| = |HN/N|$. Since HN/N is a subgroup of G/N, its order divides $|G/N| = [G : N]$. On the other hand,

$$|H/(H \cap N)| = [H : H \cap N],$$

which divides $|H|$. Since $[G : N]$ and $|H|$ are relatively prime, we must have $[H : H \cap N] = 1$ and hence $H \cap N = H$. This implies $H \subseteq N$. □

Problem 3. Let G be a finite group. Prove that if the order of G is even, then G must have an element of order 2.

You are NOT allowed to use Cauchy's theorem, in case we prove it before this problem set is due. Hint: Consider the set $S = \{g \in G \mid g \neq g^{-1}\}$, and show that S has an even number of elements.

Proof. Consider the set $S = \{g \in G \mid g \neq g^{-1}\}$. Define an equivalence relation on G by $a \sim b$ if and only if $a = b$ or $a = b^{-1}$. It is easily checked that this relation is an equivalence relation. Thus, the equivalence classes partition G. For each $a \in G$, the equivalence class of a has 1 or 2 elements, and has 2 elements if and only if $a \in S$. Thus, each equivalence class of an element in S has size 2, and the class is contained in S, so $|S|$ is even. We have $|G| = |S| + n$ where n is the number of elements a having an equivalence class of size 1; those are precisely the elements a satifying $a = a^{-1}$. Since $|G|$ is even and $|S|$ is even, we must have n is even also. Since $e = e^{-1}$, there must exist at least one other element a such that $a = a^{-1}$. Then $a^2 = aa^{-1} = e$ and $a \neq e$, so a has order 2. □

Problem 4. Let G be a group of order 6. Prove that either G is cyclic or $G \cong S_3$.
Hint: By the previous problem, G has a subgroup H of order 2. Consider the action of G on the left cosets of H.

Proof. Let G be any group of order 6. Since G has even order, then there exists an element $h \in G$ of order 2. Let $H := \langle h \rangle$, which is then a subgroup of G of order 2.

Consider the action of G on the set G/H of left cosets of H given by left multiplication:

$$x \cdot (yH) := (xy)H.$$

Since

$$|G/H| = [G : H] = \frac{|G|}{|H|} = \frac{6}{2} = 3,$$

the corresponding permutation representation is a homomorphism $\rho\colon G \to S_3$.

Given $x \in G$, if $x \in \ker \rho$ then in particular

$$\rho(x) = \mathrm{id}_{G/H} \implies x \cdot eH = eH \iff xH = eH \iff x \in H.$$

Thus $\ker \rho \subseteq H$. But $|H| = 2$, so either $\ker \rho = H$ or ρ is injective.

If ρ is injective, then ρ must be an isomorphism since $|G| = 6 = |S_3|$, which forces ρ to be a bijection. In that case, we conclude that $G \cong S_3$.

Now suppose that $\ker \rho = H$. Kernels are normal subgroups, so $H \trianglelefteq G$. Moreover, $|G/H| = 3$. By a problem on the midterm, every group of order 3 is cyclic, since 3 is prime, and thus G/H is cyclic. Thus there exists some $a \in G$ such that $G = \langle aH \rangle$, and aH has order 3 in G/H. Now $n := |a|$ satisfies

$$(aH)^n = a^n H = H.$$

Therefore, $|aH| = 3$ divides $|a|$. On the other hand, by Lagrange's Theorem $|a|$ must divide $|G| = 6$, so we conclude that $|a| = 3$ or $|a| = 6$. If $|a| = 6$, then $G = \langle a \rangle$, as G has order 6, so G is indeed cyclic.

Suppose $|a| = 3$. We claim that $m := |ah| = 6$. First, note that $|ab| \leqslant |G| = 6$. On the other hand, note that since H is a normal subgroup,

$$aha^{-1} \in H \implies aha^{-1} = h \text{ or } aha^{-1} = e.$$

But

$$aha^{-1} = e \implies h = a^{-1}a = e,$$

so $aha^{-1} = h$, and thus

$$ah = ha.$$

Thus a and h commute, so

$$a^m h^m = (ah)^m = e \implies a^m = h^{-m} \in \langle a \rangle \cap \langle b \rangle.$$

By Lagrange's Theorem, the order of $\langle a \rangle \cap \langle b \rangle$ must divide $|\langle a \rangle| = |a| = 3$ and $|\langle h \rangle| = |h| = 2$. Therefore, $\langle a \rangle \cap \langle b \rangle$ has order 1, so $\langle a \rangle \cap \langle b \rangle = \{e\}$. Hence, $a^m = h^m = e$. Thus, $|a| = 3$ and $|h| = 3$ both divide m, so we must have $m \geqslant 6$. But G has order 6, so $m = |ah| = 6$. We conclude that $G = \langle ah \rangle$ is cyclic. □

Problem 5. Suppose that G is an abelian group acting transitively and faithfully on a set X. Prove that $|G| = |X|$.

Proof. By the Orbit-Stabilizer Theorem, for any $x \in X$ we have

$$|G| = |\operatorname{Orb}_G(x)| \cdot |\operatorname{Stab}_G(x)|.$$

Let $h \in \operatorname{Stab}_G(x)$ and $y \in X$. Since the action is transitive, then there exists $g \in G$ such that $g \cdot x = y$. Then

$$\begin{aligned} h \cdot y &= h \cdot (g \cdot x) && \text{since } g \cdot x = y \\ &= (hg) \cdot x && \text{by definition of group action} \\ &= (gh) \cdot x && \text{since } G \text{ is abelian} \\ &= g \cdot (hx) && \text{by definition of group action} \\ &= g \cdot x && \text{since } h \in \operatorname{Stab}_G(x) \\ &= y. \end{aligned}$$

Thus $h \cdot y = y$ for all $y \in X$, but the action is faithful, so $h = e$. We conclude that $\operatorname{Stab}_G(x)$ is trivial, and thus $|\operatorname{Stab}_G(x)| = 1$. Therefore,

$$|G| = |\operatorname{Orb}_G(x)|. \quad \square$$