Problem Set 5
Due Thursday, October 2

Instructions: You are encouraged to work together on these problems, but each student should hand in their own final draft, written in a way that indicates their individual understanding of the solutions. Never submit something for grading that you do not completely understand. You cannot use any resources besides me, your classmates, and our course notes.

I will post the .tex code for these problems for you to use if you wish to type your homework. If you prefer not to type, please *write neatly.* As a matter of good proof writing style, please use complete sentences and correct grammar. You may use any result stated or proven in class or in a homework problem, provided you reference it appropriately by either stating the result or stating its name (e.g. the definition of ring or Lagrange's Theorem). Please do not refer to theorems by their number in the course notes, as that can change.

Problem 1. Let G be a group and H be a subgroup. For $g \in G$, let $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$.

(1.1) Show that for each $g \in G$, the set gHg^{-1} is a subgroup of G, and that $gHg^{-1} \cong H$.

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

$$H \xrightarrow{\;c_g\;} gHg^{-1}$$
$$x \longmapsto gxg^{-1}$$

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 $|H| = |gHg^{-1}|$. $\qquad \square$

(1.2) Show that if $|H| = n$ and H is the only subgroup of G of order n, 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 $H \trianglelefteq G$. $\quad \square$

Problem 2. Let G be the group of all 2×2 matrices with entries from $\mathbb{Z}$ having determinant 1. Let p be a prime number and take K to be the subset of G consisting of all matrices that are congruent to I_2 modulo p; that is, K consists of all matrices of the form $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with

$$a \equiv d \equiv 1 \pmod{p} \qquad b \equiv c \equiv 0 \pmod{p}.$$

Prove that K is a normal subgroup of G.

Proof. Consider the map $f : G \to \mathrm{SL}_2(\mathbb{Z}/p)$ given by the rule

$$f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{bmatrix},$$

where $\bar{n}$ denotes the congruence class of n modulo p. This is a group homomorphism since

$$f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}\right) = f\left(\begin{bmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{bmatrix}\right) = \begin{bmatrix} \overline{aa' + bc'} & \overline{ab' + bd'} \\ \overline{ca' + dc'} & \overline{cb' + dd'} \end{bmatrix} = f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) f\left(\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}\right),$$

and has the correct target since

$$\det f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \det \begin{bmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{bmatrix} = \overline{ad - bc} = \bar{1}.$$

The identity of the target is $\begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix}$, so $K = \ker(f)$. Since K is the kernel of a group homomorphism, it is a normal subgroup. $\qquad \square$

Problem 3. A subgroup H of a group G is a **characteristic subgroup** if for every $\sigma \in \mathrm{Aut}(G)$, we have $\sigma(H) = H$.

(3.1) Show that a characteristic subgroup is normal.

> *Proof.* For any $g \in G$, the map $c_g : G \to G$ is an automorphism of G, as we have checked in an earlier assignment. If H is characteristic, then $c_g(H) \subseteq H$ for all $g \in G$. In other terms, $gHg^{-1} \subseteq H$, so H is normal. $\qquad \square$

(3.2) Show that if G is a group, H is a normal subgroup of G, and K is a characteristic subgroup of H, then K is a normal subgroup of G.

> *Proof.* Let K, H, G be as above. We claim that for any $g \in G$, the map $c_g : G \to G$ restricts to an automorphism of H. Indeed, since H is normal, $c_g(H) = gHg^{-1} \subseteq H$. Moreover, it is a homomorphism from H to H since it is a restriction of a homomorphism on G, and is an automorphism since $c^{g^{-1}}$ also maps H to H by normality and is its inverse. Since K is characteristic in H, $c_g(K) \subseteq K$, so $gKg^{-1} \subseteq K$. This shows that K is normal in G. $\qquad \square$

Problem 4. Let G be a group. Show that if $G/Z(G)$ is cyclic, then G is abelian.

Proof. Let $Z := \mathbb{Z}(G)$ and suppose $G/Z = \langle xZ \rangle$ for some $x \in G$. Let $a, b \in G$. Then $aZ = x^i Z$ and $bZ = x^j Z$ for some i, j. Hence, $a = x^i z_1$ and $b = x^j z_2$ for some $z_1, z_2 \in G$. Then

$$ba = (x^j z_2)(x^i z_1) = x^{j+i} z_1 z_2 = (x^i z_1)(x^j z_2) = ab.$$

Therefore, G is abelian.   □

Problem 5. Let G be a finite group of order $2n$ for some integer n.

(5.1) Show[1] that G has an element of order 2.

Proof. 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. Note for $a \in G$, 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 equvalence class size 1, i.e.. $a = a^{-1}$. Since $|G|$ is even and $|S|$ is even, we must have n is even also. Since $1 = 1^{-1}$, there must exist at least one other element a such that $a = a^{-1}$. This element clearly has order 2.   □

(5.2) Let G acts on itself by left multiplication, and let $\rho : G \to \operatorname{Perm}(G)$ be the associated permutation representation. Show that for g of order 2, $\rho(g)$ is a product of n disjoint transpositions[2].

Proof. Since g has order 2 and we know that the order of a permutation is the lcm of cycle lengths in its cycle type, it must be a product of disjoint 2 cycles. To show that it consists of n disjoint 2 cycles, it suffices to show that no element is fixed, but if $h \in G$ is fixed, $gh = h$ implies $g = e$ a contradiction.   □

(5.3) Suppose that $n > 1$ is odd. Show that G has a nontrivial normal subgroup.

Proof. Consider the permutation representation corresponding to the left multiplication action, $\rho : G \to S_{2n}$, and consider $H = \rho^{-1}(A_{2n})$. Note that this is a normal subgroup; we need to check that it is nontrivial. We know that $H \neq G$, since any element of order 2 is not in H using part (b). On the other hand, $H \neq \{e\}$: since $|G| \geq 4$ we can take a, b with $a, b \neq e$ and $b \neq a^{-1}$; if $a, b \notin H$, then ab maps to an even permutation in S_{2n}, so $ab \in H$. Thus H is nontrivial.   □

---

[1]You are not allowed to use Cauchy's Theorem for this problem. Instead, you might want to consider $\{g \in G \mid g \neq g^{-1}\}$.

[2]While we have discussed cycle notation just for the symmetric groups $S_{2n} = \operatorname{Perm}([2n])$, as in the proof of Cayley's Theorem, we can identify $\operatorname{Perm}(G)$ with S_{2n} by numbering the elements of G.