1

Let G be a group acting on A. FIx $a \in A$. Show that $G_a = \{g \in G \mid ga = a\}$ is a subgroup of g.

To show that $G_a \leq G$, we need to show that G_a is nonempty and $\forall x, y \in G_a, xy^{-1} \in G_a$.

- nonempty: $e \in G_a$, trivially, since $ea = a$.
- Closure: Let $g, h \in G_a$. Need $gh^{-1} \in G_a, i.e. gh^{-1}a = a$.

$$gh^{-1}a = g(h^{-1}a) = ga = a, \tag{1}$$

where, we used the fact that $h^{-1} \in G_a$ since

$$\begin{aligned} h \in G \Rightarrow h^{-1} \in G \text{ and } ha = a \\ \Rightarrow h^{-1}ha = h^{-1}a \Rightarrow ea = h^{-1}a \Rightarrow a = h^{-1}a. \end{aligned} \tag{2}$$

Thus, $G_a \leq G$.

2.

H is a group acting on A. Show that

$$a \sim b \text{ iff } \exists h \in s.t.\ a = hb \tag{3}$$

is anequivalence relation on A.

- Reflexive : true, since $e \in H, ea = a \Rightarrow a \sim a$.
- Symmetric: Suppose $a \sim b$. Then, $\exists h \in H\ s.t.\ ha = b$. Since $h \in H \Rightarrow h^{-1} \in H$, we have $h^{-1}b = h^{-1}ha = ea = a \Rightarrow b \sim a$.
- Transitive: Suppose $a \sim b, b \sim c$, then

$$\begin{gathered} \exists h_1 \in H, a = h_1 b; \exists h_2 \in H, b = h_2 c \\ \Rightarrow a = h_1 h_2 c \\ \Rightarrow (h_1 h_2) \in H, a = (h_1 h_2) c \Rightarrow a \sim c. \end{gathered} \tag{4}$$

Thus $\sim$ is an equivalence relation on A.

3

Let G be any group. Show that $(g_1, g_2)a := g_1 a g_1^{-1}$ gives an action of $G \times G$ on G. Show thatn the Kernel of this action is $\{(g, g) |\ g \in \mathbb{Z}(G)\}$

1

consider $e_1, e_2 \in G$

$$(e_1, e_2)a = e_1 a e_2^{-1} = eae = a. \tag{5}$$

- consider $(h_1, h_2), (g_1, g_2) \in G \times G$.

$$\begin{aligned}(h_1, h_2)((g_1, g_2)a) &= (h_1, h_2)(g_1 a g_2^{-1}) \\ &= h_1 g_1 a g_2^{-1} h_2^{-1}. \\ ((h_1 g_1), (h_2 g_2))a &= (h_1 g_1) a (h_2 g_2)^{-1} \\ &= h_1 g_1 a g_2^{-1} h_2^{-1} = (h_1, h_2)((g_1, g_2)a).\end{aligned} \tag{6}$$

so this is an action of $G \times G$ on G.

2

Consider the kernel $(g_1, g_2)\ s.t.\ (g_1, g_2)a = a, \forall a \in G$. Then

$$g_1 a g_2^{-1} = a \Leftrightarrow g_1 = a g_2 a^{-1}, \forall a \in G \tag{7}$$

which gives $g_2 = a^{-1} g_1 a\ \forall a \in G$. Let arbitrary $x, y \in G$, then

$$x^{-1} g_1 x = y^{-1} g_1 y \Rightarrow g_1 (x y^{-1}) = (x y^{-1}) g_1. \tag{8}$$

Then $g_1 \in Z(G.)$ Hence $g_2 = a^{-1} g_1 a = g_1 := g$. Thus, the kernel is

$$\{(g, g) \mid g \in Z(G)\}. \tag{9}$$

4

Let G be a group and let G act on itself by left conjugation, s.t. each $g \in G$ maps $G \to G$ by $x \mapsto gxg^{-1}$. For fixed $g \in G$, prove:

1. Conjugation by g is automorphisim of G.
2. x, gxg^{-1} have same order $\forall x \in G$.
3. $\forall A \subseteq G, |A| = |gAg^{-1}|$.

1

Define $c_g : G \to G, c_{g(x)} = gxg^{-1}$. Now, for any $x, g \in G$, consider

$$\begin{gathered} c_{g(xy)} = gxyg^{-1}; \\ c_{g(x)}c_{g(y)} = (gxg^{-1})(gyg^{-1}) = gx(g^{-1}g)yg^{-1} = gxyg^{-1} \\ c_{g(xy)} = c_{g(x)}c_{g(y)}. \end{gathered} \tag{10}$$

So c_g is a homomorphism. Further, recall that a map f is bijective if $\exists g : B \to A \; s.t. \; f \circ g = e_B, g \circ f = e_A$.

We define an "inverse conjugation" as $c_{g^{-1}} : G \to G, c_{g(x)} = g^{-1}xg$. Then,

$$\begin{gathered} c_g \circ c_{g^{-1}}(x) = c_{g(g^{-1}xg)} = g(g^{-1}xg)g^{-1} = exe = x; \\ c_{g^{-1}} \circ c_g(x) = c_{g^{-1}}(gxg^{-1}) = g^{-1}(gxg^{-1})g = exe = x. \end{gathered} \tag{11}$$

Therefore $c_g \circ c_{g^{-1}} = e = c_{g^{-1}} \circ c_g$. Thus, c_g is bijective, and hence an automorphism of G.

2

Since c_g is an automorphism, it is isomorphic, so using proposition from lecture that isomorphic elements have the same order, we have that x and gxg^{-1} have the same order.

3

Since $c_g : G \to G$ is bijective, it is injective, and so a subset $A \subset G$ is injective to $c_{g(A)} = gAg^{-1}$. Further, we can show that c_g is surjective from A to gAg^{-1}. Consider any $y \in gAg^{-1}$. Then, $\exists a \in A \; s.t. \; y = gag^{-1}$. But then, $c_{g(a)} = gag^{-1} = y$. Thus, c_g is surjective from A to gAg^{-1}.

Since c_g is both injective and surjective from A to gAg^{-1}, c_g is bijective from A to gAg^{-1}, and so $|A| = |gAg^{-1}|$.

5

Give an explicit example where G is a group, $H \subset G$, $|H| = \infty$, H is closed under the group opreation, but H is not a subgroup of G.

We can construct such an example by failing the subgroup definition that $\forall x \in H, x^{-1} \in H$.

Consider $G = (\mathbb{R}, +)$, $H = \mathbb{N}$. It is easily verified that $H \subset G$, $|H| = \infty$, and H is closed under addition. However, consider $2 \in H$. Its inverse would be -2, but it is not in H. Thus, H is not a subgroup of G.

6

Prove that

1. If H and K are subgroups of G, then $H \cap K$ is a subgroup of G.
2. The intersection of an arbitrary nonempty collection of subgroups of G is a subgroup of G.

1

Consider arbitrary $x, y \in H \cap K$. Then $x, y^{-1} \in H, x, y^{-1} \in K$ and $xy^{-1} \in H$, $xy^{-1} \in K$ by subgroup definiton. Then $xy^{-1} \in H \cap K$. Further, $e \in H, e \in K \Rightarrow e \in H \cap K$, nonempty. Thus, $H \cap K \leq G$.

2

Denote $H_i \leq G (i = I)$ for some index set I, and denote $S = \cap_i H_i$.

First, it's clear that $e \in S$ as $e \in H_i \forall i$, and so S is nonempty.

Then, consider $x, y \in S$, then $x, y \in H_i \forall i \in I$ by definition of intersection. By subgroup definition, $xy^{-1} \in H_i \forall i \in I$, and so $xy^{-1} \in S$. Thus, $S \leq G$.

7

Prove the following:

1. Assume $H \leq G, K \leq G$, then $H \cup K$ not closed under multiplication unless $H \leq K$ or $K \leq H$.
2. 2. Let $H_n \leq G$ $(n = 1, 2, \ldots)$ $s.t.$ $H_n \leq H_{n+1}$. Prove that $\cup_{n=1}^{\infty} H_n \leq G$.

1

We need to prove : $H \cup K$ closed under multilpication $\Rightarrow H \leq K$ or $K \leq H$. Suppose not: $H \cup K$ but $H \nleq K$ or $K \nleq H$.

Then choose $h \in H \setminus K, k \in K \setminus H$. Since $H \cup K$ closed under multiplictation, $hk \in H \cup K$.

If $hk \in H$, then since $h \in H$, by subgroup definition, $h^{-1} \in H$ and so $k = h^{-1}(hk) \in H$, a contradiction. If $hk \in K$, then since $k \in K$, by subgroup definition, $k^{-1} \in K$ and so $h = (hk)k^{-1} \in K$, a contradiction.

So, $H \cup K$ not closed under multiplication unless $H \leq K$ or $K \leq H$.

2

Denote $H = \cup_{n=1}^{\infty} H_n$. Choose $x, y \in H$. Then $x \in H_m, y \in H_n$ for some $m, n \in \mathbb{N}$. Take $k = \max(m, n)$, then $x, y \in H_k$ since $H_m \leq H_k, H_n \leq H_k$. By subgroup definition, $xy^{-1} \in H_k$, and so $xy^{-1} \in H$. Further, $e \in H_1 \leq H$, so H is nonempty. Thus, $H \leq G$.

8

Let $H \leq G$ for G a group. Prove:
1. $H \subseteq N_G(H)$
2. Find an example where $G$is a group, $A \subseteq G$, but $A \not\subset N_G(A)$
3. $H \subseteq C_G(H)$ iff H is abelian.

1.

Recall $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$. To show $H \subseteq N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ is to show $\forall h \in H, hHh^{-1} = H$.

Fix $h \in H, h^{-1} \in H$. Then $\forall x \in H, hxh^{-1} \in H \Rightarrow hHh^{-1} \subseteq H$.

Simliarly, fix $h^{-1} \in H$. Then $\forall y \in H, h^{-1}yh \in H \Rightarrow y \in hHh^{-1}$. But since $y \in H, H \subseteq hHh^{-1}$.

Collectively, $hHh^{-1} = H$, and so $h \in N_G(H)$. Since $h \in H$ was arbitrary, $H \subseteq N_G(H)$.

2.

Consider $G = S_3 = \{(123), (12), (13), (132), e\}$. Consider $A = \{(12), (13)\} \subset G$.

Further, consider $(12) \in G$. Notice that it is in A, but not in $N_G(A)$, since:

$$\begin{aligned} (12)(12)(12) &= (12) \in A. \\ (12)(13)(12) &= (23) \notin A. \end{aligned} \tag{12}$$

So $(12) \notin N_G(A)$ while $(12) \in A$, so $A \not\subset N_G(A)$.

3.

- Assume $H \subseteq C_G(H) \Leftrightarrow h \in C_G(H)\ \forall h \in H$, which implies for all $a \in A, ha = ah$ by the definition of centralizer. Thus, H is abelian.
- Assume H is abelian. Then, $\forall h \in H, \forall a \in H, ha = ah \Rightarrow hah^{-1} = ahh^{-1} = a \Rightarrow hHh^{-1} = H \Rightarrow h \in C_G(H)$. Since $h \in H$ was arbitrary, $H \subseteq C_G(H)$. Thus completes the proof.

9.

$\boxed{G = Q_8, A = \{i, -i\}, \text{ find } Z(G), C_G(A), N_G(A).}$

$G = \{\pm 1, \pm i, \pm j, \pm k\}$.

1. $Z(G) = Z(Q_8) = \{g \in Q_8 \mid gx = xg, \forall x \in Q_8\} = \{1, -1\}$, since i, j, k do not commute with each other.
2. $C_G(A) = \{g \in Q_8 \mid ga = ag, \forall a \in A\} = \{1, -1, i, -i\} = \langle i \rangle$, as $Z(G) \subseteq C_G(A)$, and j, k do not commute with i.
3. $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$. Since $C_G(A) \subseteq N_G(A)$, examine only $g = j, k$.
   - for $g = j$, notice that $jAj^{-1} = \{-i, i\} = A$;
   - for $g = k$, notice that $kAk^{-1} = \{i, -i\} = A$.
   - for cases $g = -j, -k$, the same results hold in the exact same way.

- Thus, $N_G(A) = \{1, -1, i, -i, j, -j, k, -k\} = Q_8$.