Debra Griffin
Math 210A
HW #4, 2.5 p. 80 #42, 47, 51, 52, 53, 64

2.42 This exercise gives some invariants of a group. Let $f : G \to H$ be an isomorphism.

(i) Prove that if $a \in G$ has infinite order, then so does $f(a)$, and if a has finite order n, then so does $f(a)$. Conclude that if G has an element of some order n and H does not, then $\sim(G \cong H)$.

Proof:

Let $a \in G$ and suppose that the order of a is infinite. Then $\forall\, n, m \in \mathbb{Z}$, where $n \neq m$, $a^n \neq a^m$ (otherwise $1 = a^n a^{-n} = a^m a^{-n} = a^{m-n}$ where $m - n$ is finite).

Then by injectivity and homomorphism properties of f, $f(a)^n = f(a^n) \neq f(a^m) = f(a)^m$.

$\therefore$ The order of $f(a)$ is infinite.

Now suppose the order of a is $n < \infty$.

Then, $1 = a^n \Rightarrow f(a^n) = f(a)^n = 1$. $\therefore$ The order of $f(a)$ divides n.

$\therefore$ The order of $f(a)$ is finite.

Additionally, we have that, if $\circ[f(a)] = m < \infty$, $1 = f(a)^m = f(a^m) \Rightarrow a^m = 1$, hence $n \mid m$.

And, as previously noted, $\circ[f(a)] \mid n$. $\therefore$ $m = n$.

In conclusion, this gives us that if G has an element of some order n and H does not, then $\sim(G \cong H)$.

(ii) Prove that if $G \cong H$, then, for every divisor d of $|G|$, both G and H have the same number of elements of order d.

Proof:

Since $G \cong H$, then $\exists\, f : G \to H$ that is a bijection.

Let d be a divisor of $|G|$. Let $G_d = \{g \in G \mid \circ(g) = d\}$ and $H_d = \{h \in H \mid \circ(h) = d\}$.

We shall show there is a bijection $\phi : G_d \to H_d$, hence $|G_d| = |H_d|$.

Define $\phi : G_d \to H_d$ by $\phi(g) = f(g)$, and let $a, b \in G_d$ such that $\phi(a) = \phi(b)$.

Then $f(a) = f(b)$. Since f is an isomorphism, then $a = b$. $\therefore$ ϕ is an injection.

Let $y \in H_d$. Then $\circ(y) = d$. Since f is a surjection, then $\exists\, x \in G$ such that $f(x) = y$. And by (i), $\circ(x) = \circ(f(x)) = \circ(y)$. $\therefore$ $\circ(x) = d$, hence $x \in G_d$.

$\therefore$ ϕ is a surjection and we have our desired bijection.

$\therefore$ For every divisor d of $|G|$, both G and H have the same number of elements of order d.

2.47 **(i)** If $f: G \to H$ is a homomorphism and $x \in G$ has order k, prove that $f(x) \in H$ has order m, where $m \mid k$.

Proof:
Let $x \in G$ with $\circ(x) = k$. By homomorphism properties, if $m = \circ(f(x))$, then $1 = f(1) = f(x^k) = f(x)^k$. Hence, $m \mid k$.

(ii) If $f: G \to H$ is a homomorphism and if $(|G|, |H|) = 1$, prove that $f(x) = 1$ for all $x \in G$.

Proof:
Let $|G| = n$ and $|H| = q$. Let $x \in G$, $\circ(x) = k$, and $\circ(f(x)) = m$. By (i), $m \mid k$, and by corollary to Lagrange's Theorem, $k \mid n$ and $m \mid q$.

So now we have $m \mid k \mid n$ which implies $m \mid n$ and $m \mid q$.

But since $(n, q) = 1$, then $m = 1$.

So then $\forall\ x \in G$, $\circ(f(x)) = 1$, but the only element with order one is the identity.

$\therefore f(x) = 1$ for all $x \in G$.

2.51 **(i)** Prove that if $\alpha \in S_n$, then α and α^{-1} are conjugate.

Proof:
Let $\alpha \in S_n$. Then $\alpha = (c_1\ c_2\ ...c_r)$ for some $r \le n$ and $\alpha^{-1} = (c_r\ c_{r-1}\ ...c_2\ c_1)$.

Let $\beta \in S_n$ such that $\beta(c_1) = c_r$, $\beta(c_2) = c_{r-1}$, ..., $\beta(c_r) = c_1$.

Then $\beta\alpha\beta^{-1} = \alpha^{-1}$. $\therefore$ α and α^{-1} are conjugate.

(ii) Give an example of a group G containing an element x for which x and x^{-1} are not conjugate.

Proof:
Let $G = \mathbb{Z}_3 = \{[0], [1], [2]\}$. Let $x = [1]$, then $x^{-1} = [2]$.

$\gamma_{[0]}([1]) = [0] + [1] + [0] = [1] \neq [2]$.

$\gamma_{[1]}([1]) = [1] + [1] + [2] = [0] \neq [2]$.

$\gamma_{[2]}([1]) = [2] + [1] + [1] = [0] \neq [2]$.

$\therefore\ \forall\ g \in G, gxg^{-1} \neq x^{-1}$.

2.52 Prove that the intersection of any family of normal subgroups of a group G is itself a normal subgroup of G.

Proof:
Let $\{K_\alpha\}_{\alpha \in G}$ be a family of normal subgroups of G.
Since $e \in K_\alpha$ for each α, then $e \in \bigcap_\alpha K_\alpha$.

Let $j, k \in \bigcap_\alpha K_\alpha$. Then $j, k \in K_\alpha$ for each α.

Since K_α is a group for each α, then $j^{-1} \in \bigcap_\alpha K_\alpha$.

And by closure, $kj^{-1} \in K_\alpha$ for each α, hence $kj^{-1} \in \bigcap_\alpha K_\alpha$.

Let $g \in G$. Then, since $K_\alpha \lhd G$ for each α, $gkg^{-1} \in K_\alpha$ for each α.
$\therefore\ gkg^{-1} \in \bigcap_\alpha K_\alpha$. $\therefore\ \bigcap_\alpha K_\alpha \lhd G$.

2.53 Define $W = \langle (12)(34) \rangle$, the cyclic subgroup of S_4 generated by (12)(34). Show that W is a normal subgroup of $\boldsymbol{V}$, but that W is not a normal subgroup of S_4. Conclude that normality is not transitive: $W \lhd \boldsymbol{V}$ and $\boldsymbol{V} \lhd G$ do not imply $W \lhd G$.
Proof:
$\boldsymbol{V} = \{(1), (12)(34), (23)(41), (13)(42)\}$.

$W = \langle (12)(34) \rangle = \{(1), (12)(34)\}$. If $W \lhd \boldsymbol{V}$, then $\forall\ w \in W, \forall\ v \in \boldsymbol{V}, vwv^{-1} \in W$.

So, we verify $W \lhd \boldsymbol{V}$ by computation:

Since $[(12)(34)]^2 = [(23)(41)]^2 = [(13)(42)]^2 = (1)$, then

$(1)(1)(1) = (12)(34)(1)(12)(34) = (23)(41)(1)(23)(41) = (13)(42)(1)(13)(42) = (1) \in W$.

and

$(1)(12)(34)(1) = (12)(34)(12)(34)(12)(34) = (23)(41)(12)(34)(23)(41) =$

$(13)(42)(12)(34)(13)(42) = (12)(34) \in W$. $\therefore\ W \lhd \boldsymbol{V}$.

To verify $\boldsymbol{V} \lhd S_4$, we will simply note that $\forall\ \alpha \in S_4$, $\alpha(1)\alpha^{-1} = (1)$ and where

$\beta \in \boldsymbol{V}$ and $\beta \neq (1)$, $\alpha\beta\alpha^{-1}$ is of the same cycle structure as β (i.e. (12)(34)). Since there are 3 permutations of the form (12)(34) in $\boldsymbol{V}$ and the same 3, and only 3, occur in S_4, then $\alpha\beta\alpha^{-1}$ is guaranteed to live in $\boldsymbol{V}$. $\therefore\ \boldsymbol{V} \lhd S_4$.

However,
$(123)(12)(34)(321) = (32)(14) \notin W$. $\therefore\ \sim(W \lhd S_4)$.

Thus, we can conclude that normality is not transitive.

2.64 **(i)** For every group G, show that the function $\Gamma : G \to \text{Aut}(G)$, given by $g \mapsto \gamma_g$ (where γ_x is conjugation by g), is a homomorphism.

Proof:
Let $a, b, x \in G$.
Then $\gamma_{ab}(x) = (ab)x(ab)^{-1} = abxb^{-1}a^{-1} = a\gamma_b a^{-1}(x) = \gamma_a\gamma_b(x)$.
Thus $= \Gamma(ab) = \gamma_{ab} = \Gamma(a)\,\Gamma(b)$.
$\therefore$ Γ is a homomorphism.

(ii) Prove that $\ker \Gamma = Z(G)$ and $\text{im}\,\Gamma = \text{Inn}(G)$; conclude that $\text{Inn}(G)$ is a subgroup of $\text{Aut}(G)$.

Proof:
We first show $\ker \Gamma = Z(G)$.
Note that the identity of Aut (G) is the identity map i: $G \to G$ where $\forall\ g \in G$, $i(g) = g$.
Then $\ker \Gamma = \{g \in G \mid \Gamma(g) = i\}$.
To show $\ker \Gamma \subseteq Z(G)$ we let $a \in \ker \Gamma$ and note that $\forall\ x \in G$, $\gamma_a(x) = axa^{-1} = x$.
$\therefore$ $\forall\ x \in G$, $xa = ax$.
$\therefore$ $a \in Z(G)$.
To show $\ker \Gamma \supseteq Z(G)$, let $b \in Z(G)$, let $g \in G$, and note that $bgb^{-1} = g$.
Thus, $\gamma_b(g) = bgb^{-1} = g$, hence $b \in \ker \Gamma$.
$\therefore$ $\ker \Gamma = Z(G)$.

And now we will show $\text{im}\,\Gamma = \text{Inn}(G)$.
We have $\text{im}\,\Gamma \subseteq \text{Inn}(G)$ by definition of Γ.
To show $\text{im}\,\Gamma \supseteq \text{Inn}(G)$, let $b \in \text{Inn}(G)$. Then $b = \gamma_x = \Gamma(x)$ for some $x \in G$.
$\therefore$ $\text{im}\,\Gamma = \text{Inn}(G)$.
We now show, in conclusion, that $\text{Inn}(G) \leq \text{Aut}(G)$.
We know $\text{Inn}(G) \subseteq \text{Aut}(G)$ by definition.
Since $\gamma_e \in \text{Inn}\,(G)$, $\text{Inn}\,(G) \neq \varnothing$.
Let $a, b, x \in G$ and let $\gamma_a, \gamma_b \in \text{Inn}\,(G)$.
Since $b^{-1} \in G$, then $b^{-1}xb \in G$ and $\gamma_b(b^{-1}xb) = bb^{-1}xbb^{-1} = x = \gamma_b\gamma_{b^{-1}}(x)$.
So $\forall\ x \in G$, $\gamma_a\,\gamma_{b^{-1}}(x) = \gamma_a\,(b^{-1}xb) = a(b^{-1}xb)a^{-1} = (ab^{-1})\,x(ba^{-1}) = (ab^{-1})\,x(ab^{-1})^{-1} = \gamma_{ab^{-1}}(x)$.
And $\gamma_{ab^{-1}}(x) \in \text{Inn}\,(G)$ (since $ab^{-1} \in G$).
$\therefore$ $\text{Inn}(G) \leq \text{Aut}(G)$.

(iii) Prove that $\text{Inn}(G) \lhd \text{Aut}(G)$.

Proof:
By (ii) we know $\text{Inn}(G) \leq \text{Aut}(G)$.
Let $\phi \in \text{Aut}\,(G)$, $\gamma_g \in \text{Inn}\,(G)$, where $g \in G$.
Then by homomorphic and surjective properties of ϕ,
$\forall\ x \in G$, $\phi\gamma_g\phi^{-1}(x) = \phi(g\phi^{-1}(x)g^{-1}) = \phi(g)\phi(\phi^{-1}(x))\phi(g^{-1}) = \phi(g)\ x\ \phi(g^{-1}) = \gamma_{\phi(g)}(x)$.
Since $\phi(g) \in G$, then $\gamma_{\phi(g)} \in \text{Inn}\,(G)$, as desired.
$\therefore$ $\text{Inn}(G) \lhd \text{Aut}(G)$.