1 Problems

1. 2.8.1

Solution:
(a) This map is an automorphism. It is a homomorphism since \( T(x + y) = -(x + y) = -x - y = T(x) + T(y) \). This function is a one-to-one correspondence since it equals its own inverse. That is, \( T(T(x)) = x \) for every \( x \).

(b) This map is an automorphism. It is a homomorphism since \( T(xy) = (xy)^2 = x^2y^2 = T(x)T(y) \). This function is a one-to-one correspondence since it has an inverse. Let \( S(x) = \sqrt{x} \), then for every positive \( x \) we have \( T(S(x)) = S(T(x)) = x \).

(c) This map is not an automorphism. Let \( G = (a) \). Then \( T \) is definitely a homomorphism since \( T(a^i a^j) = a^{3(i+j)} = a^{3i} a^{3j} = T(a^i)T(a^j) \).

This function is not, however, a correspondence. For example, \( T(a^4) = a^{12} = e = T(e) \) so \( T \) is not one-to-one.

(d) This map is not even a homomorphism. It is one-to-one and onto since \( T(T(g)) = g \) for any \( g \). However, if we represent \( G \) as \( G = \{ e, y, y^2, x, xy, xy^2 \} \) with \( x^2 = y^3 = e \) and \( xy = x y^2 \), then \( T(xy) = (xy)^{-1} = y^2 x = xy \)

but \( T(x)T(y) = xy^2 \neq xy \).

2. 2.8.4

Solution: We’ve already seen that for any group \( G \), if \( Z \) is the center of \( G \) then \( G/Z \cong \text{Inn} G \). Thus all we need to do is prove that in \( S_3 \), the center is trivial. You can explicitly compute that no \( e \neq g \in S_3 \) commutes with every other element. A slicker way to do this problem is to recall that the center is always normal, and we’ve previously seen that the only non-trivial normal subgroup of \( G \) is the subgroup \( H = \{ e, y, y^2 \} \). Of course \( y \notin Z \) since \( y \) does not commute with \( x \). Thus \( Z = \{ e \} \) and the assertion follows.

3. 2.8.5

Solution: Let \( \varphi \in \text{Aut} G \) and \( \tau_g \in \text{Inn} G \). We must prove that \( \varphi \circ \tau_g \circ \varphi^{-1} \in \text{Inn} G \). Recall that \( \tau_g \) is defined by \( \tau_g(x) = gxg^{-1} \). Thus for any \( x \in G \) we have

\[
\varphi \circ \tau_g \circ \varphi^{-1}(x) = \varphi(g \varphi^{-1}(x)g^{-1}) = \varphi(g) \varphi(\varphi^{-1}(x)) \varphi(g)^{-1} = \varphi(g) \varphi(g)^{-1} = \tau_{\varphi(g)}(x).
\]

Thus indeed \( \varphi \circ \tau_g \circ \varphi^{-1} = \tau_{\varphi(g)} \in \text{Inn} G \) and so \( \text{Inn}(G) \) is normal in \( \text{Aut}(G) \).
4. 2.8.6

**Solution:** Any automorphism $\varphi : G \to G$ must satisfy $\varphi(e) = e$. Thus since $\varphi$ permutes the other three elements of $G$, we see that $o(\text{Aut}(G)) \leq 6$. Let $\sigma : G \to G$ be function satisfying

$$\sigma(e) = e, \sigma(a) = b, \sigma(b) = a, \sigma(ab) = ab$$

and let $\tau : G \to G$ be the function satisfying

$$\tau(e) = e, \tau(a) = b, \tau(b) = ab, \tau(ab) = a.$$  

Convince yourselves that $\sigma$ and $\tau$ both define homomorphisms, and since they are correspondences we have $\sigma, \tau \in \text{Aut}(G)$. Check further that $\sigma^2 = \tau^3 = I$ and $\tau\sigma = \sigma\tau^2$, so $H = (\sigma, \tau) \subseteq \text{Aut}(G)$ is a non-abelian group of order 6. Since $o(\text{Aut}(G)) \leq 6$ we get $\text{Aut}(G) \cong S_3$.

5. Let $\varphi : G \to \overline{G}$ be an isomorphism of $G$ onto $\overline{G}$. For $a \in G$ prove that $a^n = e$ if and only if $\varphi(a)^n = \overline{e}$. Use this to prove that $o(a) = o(\varphi(a))$.

(This shows you that if $\varphi : C_n \to C_n$ is an automorphism, then necessarily $\varphi(a) = a^i$ for some $i$ which is relatively prime to $n$. Check out Example 2.8.1 for the full identification of $\text{Aut}(C_n)$.)

**Solution:** Let $\psi : G \to \overline{G}$ be any homomorphism. We first prove by induction that $\psi(a^n) = \psi(a)^n$ for any $n \in \mathbb{Z}$. This is clear for $n = 0, 1$, so assume it is true for $n = k$ where $k \geq 1$. Then

$$\psi(a^{k+1}) = \psi(a^k a) = \psi(a^k)\psi(a) = \psi(a)^k\psi(a) = \psi(a)^{k+1}. $$

To get this for negative integers, recall that $\psi(a^{-1}) = \psi(a)^{-1}$ so for any $n \geq 1$ we have

$$\psi(a^{-n}) = \psi((a^{-1})^n) = \psi(a^{-1})^n = (\psi(a)^{-1})^n = \psi(a)^{-n}. $$

With this in mind, if $\varphi : G \to \overline{G}$ is an isomorphism and $a^n = e$, then

$$\overline{e} = \overline{\varphi(e)} = \varphi(a^n) = \varphi(a)^n. $$

Conversely, if $\varphi(a)^n = \overline{e}$ then we get

$$e = \varphi^{-1}(\overline{e}) = \varphi^{-1}(\varphi(a)^n) = \varphi^{-1}(\varphi(a^n)) = a^n. $$

It follows immediately that $o(a) = o(\varphi(a))$. We just showed that $\varphi(a)^{o(a)} = \overline{e}$ so $o(\varphi(a)) \mid o(a)$ and conversely $a^{o(\varphi(a))} = e$ so $o(a) \mid o(\varphi(a))$ proving equality.

6. A subgroup $C \subseteq G$ is said to be a characteristic subgroup of $G$ if $\varphi(C) \subseteq C$ for every $\varphi \in \text{Aut}(G)$.

(a) Prove that any characteristic subgroup of $G$ is normal.

**Solution:** We are told that every automorphism $\varphi \in \text{Aut}(G)$ has the property $\varphi(C) \subseteq C$. In particular, for every $g \in G$, the inner automorphism $\tau_g$ has the property $\tau_g(C) \subseteq C$. This says that for every $g$, $gCg^{-1} \subseteq C$ which implies that $C$ is normal.

(b) Let $G'$ be the commutator subgroup of $G$ (see 2.7.5). Prove that $G'$ is a characteristic subgroup of $G$. 

Page 2
Solution: Recall that if \( S = \{ aba^{-1}b^{-1} | a, b \in G \} \) then \( G' = (S) \). If \( \varphi \in \text{Aut}(G) \), then for any \( a, b \in G \) we have
\[
\varphi(aba^{-1}b^{-1}) = \varphi(a)\varphi(b)\varphi(a)^{-1}\varphi(b)^{-1}
\]
which shows that \( \varphi(S) \subseteq S \). Since \( \varphi^{-1} \in \text{Aut}(G) \) as well, the same argument shows that \( \varphi^{-1}(S) \subseteq S \) so in fact \( \varphi(S) = S \). The proof is now easy since \( G' \) consists of products of elements of \( S \) and their inverses. For practice, we give a proof using intersections. We know
\[
G' = \bigcap_{H \subseteq G} H
\]
where the intersection is taken over all subgroups. Thus
\[
\varphi(G') = \bigcap_{H \subseteq G} \varphi(H) = \bigcap_{K \subseteq G} K
\]
since \( S \subseteq H \) if and only \( \varphi(S) \subseteq \varphi(H) \). But we just showed \( \varphi(S) = S \) so
\[
\varphi(G') = \bigcap_{K \subseteq G} K = G'
\]
proving that \( G' \) is characteristic.

(c) Prove that the center \( Z \subseteq G \) is a characteristic subgroup.

Solution: Let \( \varphi \in \text{Aut}(G) \) and \( z \in Z \). We must prove that \( \varphi(z) \in Z \) as well. To this end, let \( y \in G \). Since \( \varphi \) is an automorphism, there exists \( x \in G \) so that \( \varphi(x) = y \). Then
\[
y\varphi(z)y^{-1} = \varphi(x)\varphi(z)\varphi(x)^{-1} = \varphi(xzx^{-1}) = \varphi(z)
\]
since \( z \in Z \). This show that \( \varphi(z) \) commutes with \( y \), and since \( y \) is arbitrary, we indeed have \( \varphi(z) \in Z \).

7. Let \( G \) be a group and \( \varphi \in \text{Aut}(G) \), a non-inner automorphism. We define a new group as follows. If \( o(\varphi) = r \), then introduce a new symbol \( x \) and let
\[
S = \{ x^i g | 0 \leq i < r \text{ and } g \in G \}.
\]
Thus if \( G \) is finite then \( o(S) = r \cdot o(G) \). Define multiplication on \( S \) via the rules \( x^r = e \) and \( gx = x\varphi(g) \).

Solution: Before presenting a solution, I’d like to make a quick point about this problem. Hidden in this problem is a uniqueness and existence statement. We’d like to define a product on \( S \) in such a way that \( S \) is a group and that \( x^r = e \) and \( gx = x\varphi(g) \). This is the existence part of the problem. On the other hand, the rules \( x^r = e \) and \( gx = x\varphi(g) \) tell us how we should define the multiplication law on \( S \). This means that if there is a group law on \( S \) then it is unique. What we are doing in this problem is finding the unique group law on \( S \) for which \( S \) is a group and \( x^r = e \) and \( gx = x\varphi(g) \) under this law.

(a) Find the form of the product \( (x^ig)(x^{i'}g') \) as \( x^a\tilde{g} \).
(b) Using your formula from part a), prove that \( S \) forms a non-abelian group.

**Solution:** For completeness, we will show that our multiplication law satisfies all the group laws.

- **Closure:** Since \( 0 \leq [i+i'] < r \) and \( \varphi^{i'}(g)g' \in G \), our set \( S \) is closed under our multiplication law.

- **Associativity:** Let \( i, j, k \in \{0, 1, \ldots, r-1\} \) and \( g_1, g_2, g_3 \in G \). Then
  \[
  (x^i g_1)(x^j g_2)(x^k g_3) = (x^{i+j+k} \varphi(g_1) g_2) g_3 = x^{i+j+k} \varphi(g_1) g_2 g_3
  \]
  whereas
  \[
  ((x^i g_1)(x^j g_2))(x^k g_3) = (x^{i+j} \varphi(g_1) g_2) x^k g_3 = x^{i+j+k} \varphi(g_1) g_2 g_3.
  \]
  Equality now follows since addition modulo \( r \) is associative and since \( \varphi \) is a homomorphism of order \( r \), we get
  \[
  \varphi^k(\varphi^j(g_1) g_2) g_3 = \varphi^k(\varphi^j(g_1)) \varphi^k(g_2) g_3 = \varphi^{j+k}(g_1) \varphi^k(g_2) g_3 = \varphi^{j+k}(g_1) \varphi^k(g_2) g_3.
  \]

- **Identity:** The element \( x^0 e \) will be the identity element of \( S \). This follows since
  \[
  (x^0 e)(x^i g) = x^i \varphi^0(e) g = x^i g
  \]
  and
  \[
  (x^i g)(x^0 e) = x^i \varphi^0(g) e = x^i g.
  \]

- **Inverses:** The inverse of \( x^i g \) will be \( x^{-i} \varphi^{-i}(g^{-1}) \). This is because
  \[
  (x^i g)(x^{-i} \varphi^{-i}(g^{-1})) = x^i \varphi^{-i}(g^{-1}) \varphi^{-i}(g^{-1}) = x^0 e
  \]
  and
  \[
  (x^{r-i} \varphi^{-i}(g^{-1}))(x^i g) = x^{r-i} \varphi^{-i}(g^{-1}) g = x^0 \varphi^{-i}(g^{-1}) g = x^0 e
  \]
  since \( o(\varphi) = r \).

The fact that \( S \) is non-abelian follows from \( \varphi \) being non-inner. Since \( \varphi \) is non-inner, there must exist \( g \in G \) so that \( g \neq \varphi(g) \). Then
\[
 gx = x \varphi(g) \neq xg
\]
(c) Prove that $G \subseteq S$ is normal and that $S/G \cong C_r$ the cyclic group of $r$ elements. (Hint: you can prove both of these at once by finding an onto homomorphism $S \to C_r$ which has kernel $G$.)

Solution: Let $C_r = (a)$ and define a function $\psi: S \to C_r$ by $\psi(x^i g) = a^i$. It is easy to check that $\psi$ is a homomorphism. We have

$$\psi((x^i g)(x^{i'} g')) = \psi(x^{i+i'} g' g') = a^{i+i'}$$

whereas

$$\psi(x^i g)\psi(x^{i'} g') = a^i a^{i'} = a^{i+i'}$$

and equality follows since $o(a) = r$ so $a^{i+i'} = a^{i+i'}$. The map $\psi$ is trivially onto, and $x^i g \in \ker(\psi)$ if and only if $a^i$ is the identity element of $C_r$, proving that $\ker(\psi) = \{x^0 g | g \in G\}$ which is just $G$. Thus the isomorphism theorems tell us that $G$ is normal in $S$ and

$$S/G \cong C_r.$$
Next we show that \( \psi \) of \( G \) is well-defined. If \( Na = Nb \), then \( ab^{-1} \in N \). Thus \( \varphi(ab^{-1}) = \varphi(a) \varphi(b)^{-1} \in \varphi(N) = N \) as well. So \( N \varphi(a) = N \varphi(b) \) proving that \( \psi(Na) = \psi(Nb) \).

Solution: First, we must prove that \( \psi \) is well-defined. If \( Na = Nb \), then \( ab^{-1} \in N \). Thus \( \varphi(ab^{-1}) = \varphi(a) \varphi(b)^{-1} \in \varphi(N) = N \) as well. So \( N \varphi(a) = N \varphi(b) \) proving that \( \psi(Na) = \psi(Nb) \).

Next we show that \( \psi \) is a homomorphism. If \( a, b \in G \) then

\[
\psi(NaNb) = \psi(Nab) = N \varphi(ab) = N \varphi(a)N \varphi(b) = \psi(a)\psi(b).
\]

To compute the kernel of \( \psi \), note that \( \psi(Nx) = N \) if and only if \( \varphi(x) \in N \). The map \( \varphi \) is an automorphism so its inverse function \( \varphi^{-1} \) is well-defined, and \( N = \varphi^{-1}(\varphi(N)) = \varphi^{-1}(N) \). Thus \( \varphi(x) \in N \) if and only if \( x \in N \) which proves that only the coset \( N \) is an element of \( \ker(\psi) \). This proves that \( \psi \) is one-to-one.

To see that \( \psi \) is onto, let \( X \) be any coset in \( G/N \). Then there exists \( c \in G \) with \( X = Nc \). Since \( \psi \) is onto, there is \( b \in G \) with \( \varphi(b) = c \). Then \( \psi(Nb) = N \varphi(n) = Nc = X \) and so we see that \( \psi \) is onto.

### 2 For Fun

1. 2.8.12

Solution: This is a fun question, it essentially boils down to cleverly using Lagrange’s Theorem repeatedly. Let \( n = o(G) \) and \( H = \{ g \in G | T(g) = g^{-1} \} \). We do not know that \( H \) is a subgroup of \( G \), only that \( \#H > .75n \). Let \( h \in H \) and consider the set \( S = H \cap Hh \). Since \( \#H > .75n \) and \( \#Hh > .75n \) we have that \( \#S > .5n \). If \( x \in S \) then there exists \( h_1, h_2 \in H \) so that \( x = h_1 = h_2h \).

As \( S \subseteq H \) we know that \( T(x) = x^{-1} \). Of course

\[
x^{-1} = h_1^{-1} = (h_2h)^{-1} = h^{-1}h_2^{-1}.
\]

We also know that \( T \) is a homomorphism so \( T(x) = T(h_2h) = T(h_2)T(h) \). Since \( h_2, h \in H \) we get

\[
x^{-1} = T(x) = T(h_2)T(h) = h_2^{-1}h^{-1}.
\]

This shows that \( h^{-1}h_2^{-1} = h_2^{-1}h^{-1} \) or equivalently \( hh_2 = h_2h \). Since \( x = h_2h = hh_2 \) we have that \( x \) and \( h \) commute. If we define the normalizer

\[
N(h) = \{ g \in G | ghg^{-1} = h \}
\]

then we have just proved that \( S \subseteq N(h) \). The normalizer \( N(h) \) is a subgroup of \( G \), and since \( S \subseteq N(h) \) we have \( o(N(h)) > .5n \). By Lagrange’s theorem, we must in fact have \( N(h) = G \) since \( o(N(h)) | o(G) \). Thus any \( h \in H \) commutes with every \( g \in G \). This proves that \( H \subseteq Z \) the center of \( G \), but then \( o(Z) > .75n \) implies that \( Z = G \) again by Lagrange. This proves that \( G \) must be abelian. If \( x, y \in H \), then \( T(x) = x^{-1} \) and \( T(y) = y^{-1} \). Thus

\[
T(x^{-1}) = T(x)^{-1} = (x^{-1})^{-1} = x
\]

proving that \( H \) is closed under inverses. Now that we know \( G \) is abelian we can also say that

\[
T(xy) = T(x)T(y) = x^{-1}y^{-1} = y^{-1}x^{-1} = (xy)^{-1}
\]

proving that \( H \) is closed under multiplication. Thus \( H \) is actually a subgroup of \( G \), and since \( o(H) > .75n \) we must in fact have \( H = G \), proving that every \( x \in G \) satisfies \( T(x) = x^{-1} \).

It’s worth remarking that you can find non-abelian examples which have exactly three quarters of the...
elements map to their inverse. In homework 6 we introduced the quaternions

\[ Q = \{ \pm 1, \pm i, \pm j, \pm k \} \]

which is a non-abelian group of order 8 where \( ij = k \) and \( i^2 = j^2 = k^2 = -1 \). There is an automorphism \( \varphi: Q \to Q \) mapping

\[ \varphi(\pm 1) = \pm 1, \quad \varphi(\pm i) = \mp i, \quad \varphi(\pm j) = \mp j, \quad \varphi(\pm k) = \pm k. \]

This automorphism maps three quarters of the elements of \( Q \) to their inverses.

2. 2.8.14

**Solution:** We’ve already seen that any non-abelian group \( G \) has a non-trivial inner automorphism. Thus we suppose that \( G \) is abelian. If there exists \( x \in G \) with \( x \neq x^{-1} \) then certainly the map \( \varphi: G \to G \) taking \( \varphi(g) = g^{-1} \) is a non-trivial automorphism. Thus the only case to consider is what happens if every element in \( G \) has the property \( g^2 = e \).

Since \( G \) is finite there must exist a smallest positive integer \( k \) such that \( G = \langle a_1, a_2, \ldots, a_k \rangle \) where \( a_i \in G \). Certainly \( k \geq 2 \) since we are told that \( o(G) \geq 3 \). I claim that in this case \( o(G) = 2^k \). To prove this, define for any subset \( S \subseteq \{ 1, 2, \ldots, k \} \) the element of \( G \)

\[ x_S = \prod_{i \in S} a_i \]

where \( x_\emptyset \) is the identity element. Notice that every element of \( G \) is equal to \( x_S \) for some subset \( S \). This shows that \( o(G) \leq 2^k \). To prove the other inequality we must show that if \( S \neq T \) then \( x_S \neq x_T \). This follows from minimality of \( k \). If \( S \neq T \) then there exists an \( i \) which is in one set but not the other. Assume without loss of generality that \( i \in S \) and \( i \notin T \). Assume for the sake of contradiction that \( x_S = x_T \). Then if \( P = (T \cup (S - \{i\})) - (T \cap (S - \{i\})) \) then we can rearrange the equation \( x_S = x_T \) to get

\[ a_i = x_P. \]

Since \( i \notin P \), we see that \( G = \langle a_1, a_2, \ldots, a_{i-1}, a_{i+1}, \ldots, a_k \rangle \) which contradicts the minimality of \( k \). Thus each \( x_S \) is distinct and hence \( o(G) \geq 2^k \) proving equality.

Now define a function \( f: \{ 1, 2, \ldots, k \} \to \{ 1, 2, \ldots, k \} \) such that \( f(1) = 2, f(2) = 1, \) and \( f(r) = r \) for \( r \neq 1, 2 \). We use \( f \) to define a map \( \varphi: G \to G \) by \( \varphi(x_S) = x_{f(S)} \). Since \( f \) is a one-to-one correspondence, it has an inverse function \( f^{-1} \). Then the function \( \psi: G \to G \) defined by \( \psi(x_S) = x_{f^{-1}(S)} \) has the property that \( \varphi(\psi(x_S)) = \psi(\varphi(x_S)) = x_S \) proving that \( \varphi \) is a correspondence. All that remains is to check that \( \varphi \) is a homomorphism. To do so, notice that for sets \( S \) and \( T \) we have the formula

\[ x_S x_T = x_{S \cup T - (S \cap T)}. \]

Thus

\[
\varphi(x_S x_T) = \varphi(x_{S \cup T - (S \cap T)}) \\
= x_{f(S \cup T - (S \cap T))} \\
= x_{f(S) \cup f(T) - (f(S) \cap f(T))} \\
= x_{f(S)} x_{f(T)} \\
= \varphi(x_S) \varphi(x_T). 
\]

This proves that \( \varphi \) is an automorphism, and it is non-trivial since \( \varphi(a_1) \neq a_1 \).

3. 2.8.15
Solution: Let \( K = \{ x \in G | o(x) = 2 \} \). We are told that \( G \) is a disjoint union \( H = H \cup K \) where \( H \) is a subgroup of \( G \). Thus \( H \) has index 2 in \( G \) so surely it is a normal subgroup. Hence for any \( k \in K \) we get \( kHk^{-1} = H \). Thus if \( h \in H \), there exists \( \bar{h} \in H \) with \( h = \bar{h}k \). Notice that \( \bar{h} = h^{-1} \) which shows that \( h \in K \). This proves that any \( h \in H \) is of the form \( h = k\bar{h}k^{-1} \). Thus if \( h_1, h_2 \in H \) then

\[
h_1h_2 = (kh_1^{-1}k^{-1})(kh_2^{-1}k^{-1}) = k(h_1^{-1}h_2^{-1})k^{-1} = h_2h_1.
\]

This proves that \( H \) is abelian. To show that \( H \) has odd order, recall that in Herstein 2.3.11 we proved that any group of even order has an element of order 2. Since \( K \) consists of exactly those elements in \( G \) of order 2, the subgroup \( H \) must have odd order.

4. 2.8.16

Solution: Let \( m = a^n - 1 \) and let \( U_m = \{ [x] \in J_m | \gcd(x, m) = 1 \} \). Then we have seen that \( U_m \) is a group under multiplication, and by definition \( o(U_m) = \phi(m) \). Let’s compute \( o([a]) \) in \( U_m \). We know that \( a^n - 1 = m \) so \( a^n - 1 \equiv 0 \mod m \) or equivalently \( a^n \equiv 1 \mod m \). This shows that in \( U_m \), \( [a]^n = [1] \) so that \( o([a]) \leq n \). Conversely, we know that \( a^{o([a])} = 1 \mod m \) so \( m \mid a^{o([a])} - 1 \) and \( m \leq a^{o([a])} - 1 \). Thus \( a^n \leq a^{o([a])} \) which shows that \( n \leq o([a]) \). Thus \( o([a]) = n \) and so Lagrange’s theorem tells us that \( n \mid o(U_m) = \phi(a^n - 1) \).