1.4.10 (a) Let

\[ G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R}, a \neq 0, c \neq 0 \right\} \]

be the set of upper-triangular invertible 2x2 matrices. Want to check that \( G \) is closed under multiplication. We have

\[ \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix}, \]

which is upper-triangular. Also \( a_1a_2 \neq 0 \) since \( a_1 \neq 0 \) and \( a_2 \neq 0 \) are nonzero, and \( b_1b_2 \neq 0 \) for the same reason. Hence \( G \) is closed under multiplication.

(b) We know from linear algebra that

\[ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \begin{pmatrix} 1/a & -b/(ac) \\ 0 & 1/c \end{pmatrix}. \]

First note that we are not dividing by 0 since \( a \neq 0, c \neq 0, ac \neq 0 \) if the matrix is in \( G \). The inverse is also an element of \( G \) because it is upper-triangular and its diagonal entries are non-zero. Hence \( G \) is closed under inverses.

(c) \( G \) has an identity, namely \( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \). \( G \) is closed under products, and every element of \( G \) has an inverse in \( G \). Hence \( G \) is a group.

2.1.6 Suppose \((G, \cdot)\) is abelian, and let \( H \) denote the set of torsion elements of \( G \). Want to show that \((H, \cdot)\) is a group.

- Since \( 1 \in G \) is a torsion element, \( 1 \in H \).
- \( H \) is closed under multiplication: Suppose \( a, b \in H \), i.e. \( a^m = 1, b^n = 1 \) for some positive integers \( m \) and \( n \). Then

\[ (ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = 1^n1^m = 1 \]

where the first equality used that \( a \) and \( b \) commute.
• $H$ has inverses: Suppose $a \in H$ with $a^m = 1$. Since $H$ is a subset of $G$ which is a group, we know that $a$ has an inverse in $G$. Is $a^{-1} \in H$? Since $a \cdot a^{-1} = 1$, we have that

$$1 = a^m \cdot (a^{-1})^m = 1 \cdot (a^{-1})^m = (a^{-1})^m.$$ 

This shows that $a^{-1}$ is a torsion element, hence in $H$.

To construct a counterexample when $G$ is not abelian, it suffices to do the following: we need a group $G$ and two torsion elements $A, B \in G$ such that $A \cdot B$ has infinite order in $G$. (Then the torsion elements are not closed under multiplication, hence not a subgroup.)

Take $G = GL_2(\mathbb{R})$ and let $A$ and $B$ be reflection matrices with the following properties: $A$ should reflect each vector around the x-axis. $B$ should reflect each vector around the axis which makes an angle of $\sqrt{2} \pi$ with the x-axis. Then $A$ and $B$ both have order 2, but $AB$ is a rotation around the origin by an angle of $2\sqrt{2} \pi$. Since $2\sqrt{2}$ is irrational, $AB$ must have infinite order.

If you want to work out the matrices $A$ and $B$ in explicit co-ordinated, google “Haushoelder reflection.” The subgroup generated by $A$ and $B$ is sometimes called the “infinite dihedral group” and isomorphic to the free product $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ (if you don’t know what a free product is, don’t worry about it).

2.3.6 Soren sent out an email that you only need to list the subgroups of $\mathbb{Z}/48\mathbb{Z}$. Since $\mathbb{Z}/48\mathbb{Z}$ is cyclic (e.g. generated by $\bar{1}$), we know that all of its subgroup will be cyclic as well. Here’s the complete list of subgroups together with all of their generators:

- $\mathbb{Z}/48\mathbb{Z} = \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle = \langle 13 \rangle = \langle 17 \rangle = \langle 19 \rangle = \langle 23 \rangle = \langle 25 \rangle = \langle 29 \rangle = \langle 31 \rangle = \langle 35 \rangle = \langle 37 \rangle = \langle 41 \rangle = \langle 43 \rangle = \langle 47 \rangle$
- $2\mathbb{Z}/48\mathbb{Z} = \langle 2 \rangle = \langle 10 \rangle = \langle 14 \rangle = \langle 22 \rangle = \langle 26 \rangle = \langle 34 \rangle = \langle 38 \rangle = \langle 46 \rangle$
- $4\mathbb{Z}/48\mathbb{Z} = \langle 4 \rangle = \langle 20 \rangle = \langle 28 \rangle = \langle 44 \rangle$
- $8\mathbb{Z}/48\mathbb{Z} = \langle 8 \rangle = \langle 40 \rangle$
- $16\mathbb{Z}/48\mathbb{Z} = \langle 16 \rangle = \langle 32 \rangle$
- $3\mathbb{Z}/48\mathbb{Z} = \langle 3 \rangle = \langle 9 \rangle = \langle 15 \rangle = \langle 21 \rangle = \langle 27 \rangle = \langle 33 \rangle = \langle 39 \rangle = \langle 45 \rangle$
- $6\mathbb{Z}/48\mathbb{Z} = \langle 6 \rangle = \langle 18 \rangle = \langle 30 \rangle = \langle 42 \rangle$
- $12\mathbb{Z}/48\mathbb{Z} = \langle 12 \rangle = \langle 36 \rangle$
• $24\mathbb{Z}/48\mathbb{Z} = \langle 24 \rangle$
• $48\mathbb{Z}/48\mathbb{Z} = \langle 0 \rangle$

The subgroups include into each other by "reverse divisibility":

\[
\begin{align*}
48\mathbb{Z}/48\mathbb{Z} &\subset 24\mathbb{Z}/48\mathbb{Z} \subset 12\mathbb{Z}/48\mathbb{Z} \subset 6\mathbb{Z}/48\mathbb{Z} \subset 3\mathbb{Z}/48\mathbb{Z} \subset \mathbb{Z}/48\mathbb{Z} \\
48\mathbb{Z}/48\mathbb{Z} &\subset 16\mathbb{Z}/48\mathbb{Z} \subset 8\mathbb{Z}/48\mathbb{Z} \subset 4\mathbb{Z}/48\mathbb{Z} \subset 2\mathbb{Z}/48\mathbb{Z} \subset \mathbb{Z}/48\mathbb{Z} \\
24\mathbb{Z}/48\mathbb{Z} &\subset 8\mathbb{Z}/48\mathbb{Z} \\
12\mathbb{Z}/48\mathbb{Z} &\subset 4\mathbb{Z}/48\mathbb{Z} \\
6\mathbb{Z}/48\mathbb{Z} &\subset 2\mathbb{Z}/48\mathbb{Z}
\end{align*}
\]

2.3.9 Want to show that $\psi_a : \mathbb{Z}/48\mathbb{Z}$ is well-defined if and only if $a$ is a multiple of 3.

Necessary: Note that our proposed homomorphism has the form $\psi_a(\bar{k}) = x^{ak}$ for all $\bar{k} \in \mathbb{Z}/48\mathbb{Z}$. In order to be well-defined, it has to be constant on equivalence classes of $\mathbb{Z}/48\mathbb{Z}$. In particular, $\psi_a(1+48) = x^{49a}$ must equal $\psi_a(1) = x^a$. But $x^a = x^{49a}$ in $\mathbb{Z}_{36}$ if and only if $49a - a = 48a \equiv 0$ mod 36. This happens if and only if $a$ is a multiple of 3.

Sufficient: Suppose $a$ is a multiple of 3, e.g. $a = 3a'$. Then for any $z \in \mathbb{Z}/48\mathbb{Z}$,

\[
\begin{align*}
\psi_a(z + k \cdot 48) &= \psi_a(z + k \cdot 48) \\
&= \psi_a(z) \cdot \psi_a(k \cdot 48) \\
&= \psi_a(z) \cdot x^{a \cdot 48 \cdot k} \\
&= \psi_a(z) \cdot x^{3a' \cdot 48 \cdot k} \\
&= \psi_a(z) \cdot (x^{36})^{4ka'} \\
&= \psi_a(z) \cdot 1^{4ka'} \\
&= \psi_a(z) \cdot 1
\end{align*}
\]

For those values of $a$ for which $\psi_a$ is well-defined, it is automatically a homomorphism because

\[
\psi_a(z + w) = x^{a(z+w)} = x^{az} \cdot x^{aw} = \psi_a(z) \cdot \psi_a(w).
\]

Claim that $\psi_a$ is not onto for any value of $a$ because $x^4$ cannot be in the image of $\psi_a$. By the lemma below, if $\psi(z) = x^4$, then $|z| = k \cdot |x^4| = 9k$ for some integer $k$. However, there’s no element in $\mathbb{Z}/48\mathbb{Z}$ whose order is a multiple of 9.
Lemma: If $f : A \to B$ is a homomorphism of groups, then $|f(a)|$ divides $|a|$ for every $a \in A$.

Proof of Lemma: Certainly the $|f(a)| \leq |a|$ since
$$f(a)^{|a|} = f(a^{|a|}) = f(1) = 1.$$ For brevity, denote $m = |a|$ and $|f(a)| = n$. We know that $n \leq m$. If $n$ divides $m$, then $\text{gcd}(m, n) = n$. Otherwise, $\text{gcd}(m, n) < n$. By the Euclidean Algorithm, there exist integers $r, s$ so that $rm + sn = \text{gcd}(m, n) = k$. Then

$$f(a)^{\text{gcd}(m,n)} = f(a)^{rm+sn} = f(a^m)^r \cdot (f(a)^n)^s = f(1)^r \cdot 1^s = 1$$

Since $\text{gcd}(m, n) \leq n = |f(a)|$ and $f(a)^{\text{gcd}(m,n)} = 1$, we conclude that $\text{gcd}(m, n) = |f(a)|$, which happens if and only if $|a|$ is a multiple of $|f(a)|$. 

2.4.14 (a) If $H$ is a finite group, then $H = \langle H \rangle$ with $H$ a finite set, hence finitely generated.

(b) $\mathbb{Z} = \langle 1 \rangle$ since we know from elementary school that any nonzero integer can be written as $1+1+\ldots+1$ or $-1-1-\ldots-1$. Hence $\mathbb{Z}$ is finitely generated.

(c) Suppose $A = \{ a_{b_1}, \ldots, a_{b_k} \}$. You can check that

$$H := \{ \sum_{i=1}^{k} x_i \frac{a_i}{b_i} : x_i \in \mathbb{Z} \}$$

is a group containing all elements of $A$. In fact, we must have $H = \langle A \rangle$ since any group containing the elements of $A$ must also contain their sums. Notice that all elements of $H$ can be written with denominator $b_1 \cdot \ldots \cdot b_n = b$, hence $H$ is a subgroup of $\langle \frac{1}{b} \rangle$. But subgroups of cyclic groups are cyclic, hence $H = \langle A \rangle$ must be cyclic.

(d) We will argue by contradiction. Suppose $\mathbb{Q}$ were finitely generated. Then by part (c), $\mathbb{Q}$ would have to be cyclic, i.e. there exists a fraction such that $\mathbb{Q} = \langle \frac{a}{b} \rangle$. But

$$\langle \frac{a}{b} \rangle = \{ k \frac{a}{b} : k \in \mathbb{Z} \}$$
so no element of \( \langle \frac{a}{b} \rangle \) has denominator smaller than \( b \) (in lowest terms). In particular, \( \frac{1}{b+1} \in \mathbb{Q} \) but not in \( \langle \frac{a}{b} \rangle \). Hence \( \langle \frac{a}{b} \rangle \neq \mathbb{Q} \), so \( \mathbb{Q} \) cannot be finitely generated.

3.1.37 Suppose \( A \) and \( B \) are groups. Define \( \tilde{A} = \{(a,1) : a \in A\} \subset A \times B \). It is easy to see that \( \tilde{A} \) is a group (and in fact isomorphic to \( A \)). It remains to check that \( \tilde{A} \) is normal in \( A \times B \). For any \((a,b) \in A \times B\), \((\tilde{a},1) \in \tilde{A}\),

\[
(a,b) \cdot (\tilde{a},1) \cdot (a,b)^{-1} = (a,b) \cdot (\tilde{a},1) \cdot (a^{-1},b^{-1}) = (a \cdot \tilde{a} \cdot a^{-1}, b^{-1} \cdot 1) = (a \cdot \tilde{a} \cdot a^{-1}, 1) \in \tilde{A}.
\]

Since \( \tilde{A} \trianglelefteq A \times B \), the quotient \((A \times B)/\tilde{A}\) is a group. In fact, \( A \times B / \tilde{A} \cong B \) via the homomorphism \( \phi \) that sends the equivalence class \((a,b) \mapsto b \). Check that \( \phi \) is well defined on equivalence classes: First we observe that \((a_1,b_1) = (a_2,b_2)\) iff

\[
(a_1,b_1) \cdot (a_2,b_2)^{-1} = (a_1a_2^{-1}, b_1b_2^{-1}) \in \tilde{A},
\]

which is true iff \( b_1 = b_2 \). So if \((a_1,b_1) = (a_2,b_2)\), then \( b_1 = b_2 \), and so \( \phi((a_1,b_1)) = b_1 = b_2 = \phi((a_2,b_2)) \). Hence \( \phi \) is well-defined on equivalence classes. \( \phi \) is a homomorphism because

\[
\phi \left( (a_1,b_1) \cdot (a_2,b_2) \right) = \phi(a_1a_2,b_1b_2) = b_1b_2 = \phi(a_1,b_1) \cdot \phi(a_2,b_2).
\]

\( \phi \) is onto because for any \( b \in B \) I choose, \( \phi(1,b) = b \). To check that \( \phi \) is 1-1, it suffices to check that its kernel is trivial. If \( \phi(a,b) = 1 \), then \( b = 1 \), so \((a,b) = (a,1) \in \tilde{A} \), so \((a,b) = (1,1) \in (A \times B)/\tilde{A}\).

3.1.41 Let \( G \) be a group and define \( N = \langle x^{-1}y^{-1}xy : x,y \in G \rangle \) its commutator subgroup. Check that \( N \) is normal in \( G \): for \( z \in N \leq G, g \in G \), \( gzg^{-1}z^{-1} \) is a commutator in \( G \), hence \( gzg^{-1}z^{-1} \in N \). But that means that \( gzg^{-1} \in Nz = N \) (because \( z \in N \)). Hence \( N \) is normal in \( G \).

Now consider the quotient group \( G/N \). Is it abelian?

\[
\overline{g_1} \cdot \overline{g_2} = \overline{g_1g_2} = \overline{g_1 \cdot g_2 \cdot (g_2^{-1}g_1^{-1}g_2g_1)} = \overline{g_2} \cdot \overline{g_1} = \overline{g_2} \cdot \overline{g_1}
\]

since \( (g_2^{-1}g_1^{-1}g_2g_1) \in N \).

3.2.11 Let \( H \leq K \leq G \). I will let \( G : K \) denote the collection of left cosets of \( K \) in \( G \). We want to establish a bijection \( \phi : G : K \times K : H \to G : H \). Assuming that the index of \( K \) in \( G \) and the index of \( H \) in \( K \) are finite,
fix a choice of representatives \(g_1K, \ldots, g_iK\) of \(G : K\) and representatives \(k_1H, \ldots, k_jH\) of \(K : H\). Define

\[
\phi(g_aK, k_bH) = g_ahk_bH \in G : H
\]

Need to check that \(\phi\) is 1-1 and onto.

\(\phi\) is 1-1: Suppose \(\phi(g_aK, k_bH) = \phi(g_cK, k_dH)\), i.e. \(g_ahk_b = g_cdk_h\) for some \(h \in H\). Then \(g_c^{-1}g_a = k_dhk_b^{-1} \in H\). But the \(g\)'s were chosen to represent the cosets in \(G : K\); in other words, if there exists a \(\tilde{k} \in K\) such that \(g_c^{-1}g_a = \tilde{k}\), we must have \(g_c = g_a\) because they define the same coset \(g_cK = g_aK\). Now we know that \(g_a = g_c\) and that \(g_ahk_b = k_dh\). Hence \(k_b = k_dh\). But notice that \(k_dH = k_dhH = k_dH\), so \(k_b = k_d\) because we chose exactly one representative from each coset.

In summary: we showed that if \(\phi(g_aK, k_bH) = \phi(g_cK, k_dH)\), then \(g_a = g_c\) and \(h = d\), hence \(\phi\) is 1-1.

\(\phi\) is onto: Pick a coset \(gH\) in \(H : G\). Choose an element \(g_a \in G\) such that \(gK = g_aK\), i.e. \(g = g_ahk\) for some \(k \in K\). Then choose a coset representative \(k_b\) such that \(kH = k_bH\). We get that

\[
\phi(g_aK, k_bH) = g_ahk_bH = g_ahkH = gH
\]

by our choice of \(g_a\) and \(k_b\), hence \(\phi\) is onto.

Since we have a bijection between \(G : K \times K : H\) and \(G : H\), we know that

\[
\]

Finally notice that our argument did not require the indexes of the cosets to be finite. \(\phi\) would still be defined and still be a bijection if we had chosen infinitely many coset representatives at the beginning. So the equality also holds for all \(H \leq K \leq G\), not just finite-index subgroups.

Handout #1  (a) Let \(G\) be the group of invertible upper-triangular 2x2 matrices over \(\mathbb{R}\), as defined in Problem 1.4.10. Consider the subgroup

\[
K = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda > 0 \right\}
\]

together with the homomorphism \(\phi : (H, \cdot) \to (\mathbb{R}, +)\) with

\[
\phi \left( \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \right) = \log(\lambda).
\]
You can convince yourself that $K$ is a subgroup of $G$. $K$ is normal in $G$ because multiples of the identity matrix commute with all matrices. $\phi$ is a homomorphism because

$$
\phi \left[ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} \mu & 0 \\ 0 & \mu \end{pmatrix} \right] = \phi \begin{pmatrix} \lambda \mu & 0 \\ 0 & \lambda \mu \end{pmatrix} = \log(\lambda \mu)
$$

$$
= \log(\lambda) + \log(\mu) = \phi \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} + \phi \begin{pmatrix} \mu & 0 \\ 0 & \mu \end{pmatrix}
$$

Finally $\phi$ is 1-1 and onto because $\log : \mathbb{R}^+ \to \mathbb{R}$ is 1-1 and onto.

(b) Now let

$$H = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix} : \lambda \in \mathbb{R}^+ \right\}$$

and define $\phi : (H, \cdot) \to (\mathbb{R}, +)$ as

$$\phi \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix} = \log(\lambda).$$

We have again that $H$ is a subgroup of $G$ and that $\phi$ is an isomorphism. It remains to show that $H$ is not normal in $G$. Just consider

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 3 & -3 \\ 1 & 3 \end{pmatrix} \notin H$$

Handout #2 Let $G, H_1, H_2$ be groups, and $\phi_1 : G \to H_1$, $\phi_2 : G \to H_2$ onto homomorphisms with $\ker(\phi_1) = \ker(\phi_2)$.

(a) Want to define a $\psi : H_1 \to H_2$ such that $\psi(\phi_1(g)) = \phi_2(g)$ for all $g \in G$. Try to define $\psi$ as follows. Given an $h_1 \in H_1$, find a $g \in G$ with $\phi(g) = h_1$. (This exists because $\phi_1$ is onto.) Define $\psi(h_1) = \phi_2(g)$. Need to check that $\psi$ is well-defined because we made a choice of $g$ in the pre-image of $h_1$. Suppose that $\phi_1(g_1) = h_1 = \phi_1(g_2)$, i.e. $1 = \phi_1(g_1)^{-1}\phi_1(g_2) = \phi(g_1^{-1} g_2)$. Then $g_1^{-1} g_2 \in \ker(\phi_1)$. Since $\ker(\phi_1) = \ker(\phi_2)$, $g_1^{-1} g_2 \in \ker(\phi_2)$. So

$$\phi_2(g_1) = \phi_2(g_1) \phi_2(g_1^{-1} g_2) = \phi_2(g_2)$$

i.e. our definition of $\psi(h_1)$ is independent of choice of $g$ as long as $\phi_1(g) = h_1$. Next check that $\psi$ is a homomorphism. Given
$h_1, h_2 \in H_1$, pick $g_1, g_2 \in G$ with $\phi_1(g_1) = h_1$ and $\phi_1(g_2) = h_2$.

Since $\phi_1$ is a homomorphism, $\phi_1(g_1 + g_2) = h_1 + h_2$. So

$$\psi(h_1 + h_2) = \phi_2(g_1 + g_2) = \phi_2(g_1) + \phi_2(g_2) = \psi(h_1) + \psi(h_2).$$

Now we need to check that $\psi$ is in fact an isomorphism. First check that $\psi$ is onto. Given an $h \in H_2$, there exists an $g \in G$ with $\phi_2(g) = h$ because $\phi_2$ is onto by hypothesis. Then

$$\psi(\phi_1(g)) = \phi_2(g) = h$$

so $\psi$ is onto. Finally check that $\psi$ is 1-1. Since $\psi$ is a homomorphism, it suffices to check that its kernel is trivial. So suppose $\psi(h) = 1$ for some $h \in H_1$, and pick a $g \in G$ with $\phi_1(g) = h$. Since $\psi(h) = \phi_2(g)$ by definition, we see that $g \in \ker(\phi_2)$. But $\ker(\phi_1) = \ker(\phi_2)$, so $1 = \phi_1(g) = h$. This shows that $\ker(\psi)$ is trivial, hence $\psi$ is an isomorphism.

(b) Suppose we have another isomorphism $\omega : H_1 \to H_2$ that satisfies $\omega(\phi_1(g)) = \phi_2(g)$ for all $g \in G$. Want to show that $\omega = \psi$. Well, since $\phi_1$ is onto, there’s really no space for $\omega$ to be different from $\psi$. Take an $h_1 \in H_1$, and a $g \in G$ with $\psi_1(g) = h_1$. Then

$$\omega(h_1) = \omega(\phi_1(g)) = \phi_2(g) = \psi(\phi_1(g)) = \psi(h_1)$$

so $\omega(h) = \psi(h)$ for all $h \in H_1$. 

8