Solutions to Homework 1

1. No. The group $\mathbb{R}_{>0}$ is torsion-free, but $\mathbb{R}^2$ has an element of order 2, namely $-1$.

2. (a) Let $n \in \mathbb{Z}$ be non-zero. We have $1 = f(1) = f(1/n + \cdots + 1/n) = n \cdot f(1/n)$, which says that $f(1/n) = 1/n$. If $p/q \in \mathbb{Q}$, then
\[ f(p/q) = f(1/q + \cdots + 1/q) = p \cdot f(1/q) = p/q \]
so $f$ is the identity when restricted to $\mathbb{Q}$. As $\mathbb{Q}$ is dense in $\mathbb{R}$, $f$ must be the identity on all of $\mathbb{R}$ by continuity.

If we don’t assume that $f$ is continuous, the result need not be true. Let $\{r_\alpha\}_{\alpha \in A}$ be a basis for $\mathbb{R}$ as a vector space over $\mathbb{Q}$. We may assume $1 \in \mathbb{Q}$ is a basis element. Then any invertible linear transformation that fixes 1 but permutes any of the other basis elements is a counterexample.

(b) Suppose $f : \mathbb{R} \to \mathbb{R}$ is a function which satisfies $f(x+y) = f(x)+f(y)$ and $f(xy) = f(x)f(y)$, for all $x, y \in \mathbb{R}$. Show that either $f \equiv 0$, or that $f$ is the identity map.

Assume $f$ is not the zero map. Then $f(1) = f(1 \cdot 1) = f(1)^2 = f(1)^3 = \cdots$, so $f(1) = 1$. As in part (a), this implies that $f$ is the identity on $\mathbb{Q}$. Now let $r \in \mathbb{R}_{>0}$. Then $f(r) = f(\sqrt{r})^2 \geq 0$, and if we pick $q \in \mathbb{Q}$ such that $0 < q < r$, then
\[ f(r) = f(r-q) + f(q) = f(r-q) + q > 0 \]
so $f$ preserves positivity. If $r_1 < r_2$ we have
\[ f(r_2) = f(r_2 - r_1) + f(r_1) > f(r_1) \]
hence $f$ preserves the ordering on $\mathbb{R}$. If $f(r) \neq r$, WLOG assume $r < f(r)$. Pick $q \in \mathbb{Q}$ such that $r < q < f(r)$. But $f(r) < f(q) = q$, a contradiction.

3. Let $G$ be a group with proper subgroups $H_1$ and $H_2$, and suppose that $G = H_1 \cup H_2$. If either $H_1$ or $H_2$ is contained in the other, then $G$ would be equal to a proper subgroup, which is a contradiction. So we may assume there exists $h_1 \in H_1, h_1 \notin H_2$, and $h_2 \in H_2, h_2 \notin H_1$. Consider the element $h_1 h_2 \in G$, if $h_1 h_2 \in H_1$, then by closure we would have $h_1^{-1} h_1 h_2 = h_2 \in H_1$, a contradiction. Similarly, $h_1 h_2$ cannot be in $H_2$. But then $h_1 h_2 \notin G$.

4. Let $k = \text{lcm}(m,n)$, so $m | k$ and $n | k$. Then $(xy)^k = x^ky^k = e$, hence $k$ divides the order of $xy$.

We have the following counterexample if $x$ and $y$ do not commute. Let $G = S_3$, and let $x = (12), y = (23)$. Then $|x| = |y| = 2$, and $xy = (132)$, which has order 3.

To see that we can have $k \neq |xy|$, consider $G = \mathbb{Z}/2\mathbb{Z} = \{0,1\}$. Set $x = y = 1$, then $x$ and $y$ have order 2 but their sum is 0, which has order 1.
5. (a) Suppose that \( AB \) is a subgroup of \( G \). Let \( a \in A \) and \( b \in B \), then certainly both \( a \) and \( b \) are in \( AB \). Hence their product \( ba \) is in \( AB \), which proves \( BA \subseteq AB \). To see the opposite inclusion, note that \( ab \mapsto (ab)^{-1} \) is a bijection from \( AB \) to itself (because we’ve assumed that \( AB \) is a subgroup). But \((ab)^{-1} = b^{-1}a^{-1} \in BA \), thus \( AB \subseteq BA \), which proves \( AB = BA \).

Now suppose that \( AB = BA \). Let \( a_1b_1, a_2b_2 \in AB \). Since \( AB = BA \), we can find \( a_3 \in A \) and \( b_3 \in B \) such that \( b_1a_2 = a_3b_3 \). Then \( a_1b_1a_2b_2 = a_1a_3b_3b_2 \in AB \), so \( AB \) is closed under multiplication. If \( a \in A \) and \( b \in B \), then \((ab)^{-1} = b^{-1}a^{-1} \in BA = AB \), so \( AB \) is closed under taking inverses. This proves \( AB \) is a subgroup.

(b) We can write \( AB = \bigcup_{a \in A} aB \), then the problem becomes to count the number of distinct \( aB \). We have that \( aB = a'B \) if and only if \( a^{-1}a' \in B \), which happens if and only if \( a^{-1}a' \in A \cap B \). Thus the number of distinct \( aB \) is \( |A|/|A \cap B| \). Since \( |aB| = |B| \) for any \( a \), we have that \( |AB| = (\text{cardinality of } B) = |A| \cdot |B|/|A \cap B| \).

6. Throughout this problem, let \( X \) and \( Y \) be the same matrices as in Dummit and Foote.

(a) Any \( X \) and \( Y \) where \( af \neq cd \) won’t commute.

(b) It follows from the computation of \( XY \) in (a) that
\[
X^{-1} = \begin{pmatrix}
1 & -a & -b + ac \\
0 & 1 & -c \\
0 & 0 & 1
\end{pmatrix}
\]

(c) Since \( a, b, c \) can be arbitrary elements of \( F \), there is an obvious set bijection \( F^3 \rightarrow H(F) \), which proves \( |H(F)| = |F|^3 \).

(d) If \( F = \mathbb{Z}/2\mathbb{Z} \), then
\[
X^2 = \begin{pmatrix}
1 & 0 & a + c \\
0 & 1 & 0 \\
0 & 0 & 1
\end{pmatrix}
\]
so any \( X \) where \( a + c = 0 \) has order 2 (or 1 if \( X = I \)), otherwise \( X \) has order 4.

(e) Suppose \( X \in H(\mathbb{R}) \) is of finite order. Then
\[
X^n = \begin{pmatrix}
1 & na & * \\
0 & 1 & nc \\
0 & 0 & 1
\end{pmatrix}
\]
for every \( n \), thus \( a = c = 0 \). It follows that
\[
X^n = \begin{pmatrix}
1 & 0 & nb \\
0 & 1 & 0 \\
0 & 0 & 1
\end{pmatrix}
\]
which says that \( b = 0 \) as well, thus \( X = I \).