3.1

2. For each binary operation \( * \) defined on a set below, determine whether or not \( * \) gives a group structure on the set. If it is not a group, say which axioms fail to hold.

(b) Define \( * \) on \( \mathbb{Z} \) by \( a * b = \max \{a, b\} \).

This operation fails to define a group on because no element of \( \mathbb{Z} \) will serve as the identity under this operation; such an element would have to be less than or equal to all other integers. That is, if \( e * a = a \) for all \( a \in \mathbb{Z} \), then \( \max \{e, a\} = a \) and thus \( e \leq a \) for all \( a \in \mathbb{Z} \). To see that this is impossible, set \( a = e - 1 \).

Notice that \( \mathbb{Z} \) under \( * \) does satisfy associativity and closure, and it makes no sense to talk of inverses in the absence of an identity.

(d) Define \( * \) on \( \mathbb{Z} \) by \( a * b = |ab| \).

Again, this operation fails to define a group on the set \( \mathbb{Z} \). Note again that there can be no identity element. For contradiction, suppose \( -1 * e = -1 \) for some \( e \in \mathbb{Z} \), then \( |(-1)e| = -1 \), which is clearly impossible.

Again, notice that \( \mathbb{Z} \) under \( * \) does satisfy associativity and closure, and it makes no sense to talk of inverses in the absence of an identity.

(e) Define \( * \) on \( \mathbb{Q} \) by \( a * b = ab \).

This operation does not define a group on \( \mathbb{Q} = \{\frac{m}{n} | m, n \in \mathbb{Z} \text{ and } n \neq 0\} \), where \( \frac{m}{n} \) and \( \frac{p}{q} \) represent the same element if \( nr = mp \). All group axioms are satisfied except for (iv) on page 91, the existence of inverses. We use the notation \( \left[ \frac{m}{n} \right] \) to denote the element of \( \mathbb{Q} \) which may be represented by \( \frac{m}{n} \); notice that \( \left[ \frac{1}{1} \right] = \left[ \frac{1}{2} \right] \). The fact that \( * \) is well-defined is checked on page 90 of the text.

We will show that \( \left[ \frac{0}{1} \right] \) does not have an inverse.

Suppose \( \left[ \frac{m}{n} \right] \in \mathbb{Q} \) is an inverse for \( \left[ \frac{0}{1} \right] \). Then we have that \( \left[ \frac{m}{n} \right] * \left[ \frac{0}{1} \right] = \left[ \frac{(m)(0)}{(n)(1)} \right] = \left[ \frac{0}{n} \right] \) is the identity element of \( \mathbb{Q} \) under \( * \). This is clearly absurd; if this were the case, \( \left[ \frac{1}{1} \right] = \left[ \frac{1}{2} \right] * \left[ \frac{0}{1} \right] = \left[ \frac{(1)(0)}{2(1)} \right] = \left[ \frac{0}{2} \right] \). That is, \((0)(1) = (n)(2)\), which is impossible because \( n \neq 0 \).
3. Let \((G, \cdot)\) be a group. Define a new binary operation \(*\) on \(G\) by the formula \(a * b = b \cdot a\), for all \(a, b \in G\).

(a) Show that \((G, *)\) is a group

The philosophy here is that \((G, *)\) inherits all necessary characteristics from \((G, \cdot)\).

We proceed by checking the four axioms on page 91:

**Closure:** Let \(a, b \in G\). Then \(a * b = b \cdot a\), and \(b \cdot a \in G\) because \((G, \cdot)\) is a group and thus satisfies closure.

**Associativity:** Let \(a, b, c \in G\). Then

\[
a * (b * c) = a * (c \cdot b) = (c \cdot b) \cdot a = c \cdot (b \cdot a) = c \cdot (a \cdot b) = (a * b) \cdot c
\]

The middle equality is, again, due to the fact that \((G, \cdot)\) is a group.

**Identity:** Let \(e\) be the identity for \((G, \cdot)\). Then for \(a \in G\), \(a * e = e \cdot a = a = a \cdot e = e * a\). Thus \(e\) is also an identity for \((G, *)\).

**Inverses:** Let \(a \in G\), and let \(a^{-1}\) be its inverse in \((G, \cdot)\). Then \(a * a^{-1} = a^{-1} \cdot a = e = a \cdot a^{-1} = a^{-1} * a\), so \(a^{-1}\) is also an inverse to \(a\) in \((G, *)\).

(b) Give examples to show that \((G, *)\) may not be the same as \((G, \cdot)\).

An example could be found by setting \((G, \cdot) = GL_n(\mathbb{R})\), the group of \(n \times n\) invertible matrices over \(\mathbb{R}\) with \(\cdot\) as matrix multiplication. For \(n \geq 2\), this group is not abelian.

Notice, however, that if \(\cdot\) is defined as addition we have equality with \((G, *)\).

It is interesting to consider what it means for two groups to be the “same”. Notice that a group is completely defined by its multiplication table, and that \((G, \cdot)\) and \((G, *)\) will always have very similar multiplication tables— to derive one from the other it is simply necessary to reflect the table about the diagonal. In the case that \((G, \cdot)\) is abelian, the multiplication table will be symmetric about the diagonal, which gives the equality with \((G, *)\).

10. Show that the set \(A = \{f_{m,b} : \mathbb{R} \to \mathbb{R} | m \neq 0 \text{ and } f_{m,b}(x) = mx + b\}\) of affine functions from \(\mathbb{R}\) to \(\mathbb{R}\) forms a group under composition of functions. Note that our composition will occur right to left.

We show that the four relevant axioms are satisfied.

**Closure:** \([f_{m,b} \cdot f_{n,c}](x) = f_{m,b}(f_{n,c}(x)) = m(nx + c) + b = (mn)x + (mc + b)\). Note that because \(m, n \neq 0\), \(mn \neq 0\), and \(f_{m,b} \cdot f_{n,c} \in A\).

**Associativity:** This proof is just a restatement of the fundamental fact that composition of functions is always associative, which is what justifies the second and third equalities. Items in square brackets should be thought of as affine functions (elements of \(A\)) while items in round brackets should be thought of as input variables for the element of \(A\) to their left.

\[
[f_{m,b} \cdot [f_{n,c} \cdot f_{p,d}]](x) = f_{m,b}([f_{n,c} \cdot f_{p,d}](x)) \\
= f_{m,b}(f_{n,c}(f_{p,d}(x))) \\
= [f_{m,b} \cdot f_{n,c}](f_{p,d}(x)) \\
= [[f_{m,b} \cdot f_{n,c}] \cdot f_{p,d}](x)
\]
Identity: We will show that \( f_{1,0} \) serves as the identity.

\[
[f_{1,0} \cdot f_{a,b}](x) = 1(ax + b) + 0 = ax + b = f_{a,b}(x)
\]

and

\[
[f_{a,b} \cdot f_{1,0}](x) = a((1)x + 0) + b = ax + b = f_{a,b}(x)
\]

Inverses: Finally, for \( f_{n,c} \in A \), we will show that \( f_{\frac{1}{n},-\frac{c}{n}} \) serves as an inverse. Note that \( f_{\frac{1}{n},-\frac{c}{n}} \) is well defined as \( n \neq 0 \).

\[
[f_{n,c} \cdot f_{\frac{1}{n},-\frac{c}{n}}](x) = (n)(\frac{1}{n}x - \frac{c}{n}) + c = x + 0 = f_{1,0}(x)
\]

\[
[f_{\frac{1}{n},-\frac{c}{n}} \cdot f_{n,c}](x) = \frac{1}{n}(nx + c) - \frac{c}{n} = x + 0 = f_{1,0}(x)
\]

22. Let \( G \) be a group. Prove that \( G \) is abelian if and only if \((ab)^{-1} = a^{-1}b^{-1}\) for all \( a, b \in G \).

Recall that a group \( G \) is abelian if its operation is commutative; that is, \( ab = ba \) for all \( a, b \in G \). We will break the proof up into two parts. A basic fact we use (proven on page 91 and in discussion) is \((ab)^{-1} = b^{-1}a^{-1}\).

\(\Rightarrow\): Here we will show that if \( G \) is abelian, \((ab)^{-1} = a^{-1}b^{-1}\) for all \( a, b \in G \). Let \( a, b \in G \). Then \((ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}\). The second equality is true because \( G \) is abelian.

\(\Leftarrow\): Here we will show that if \((ab)^{-1} = a^{-1}b^{-1}\) for all \( a, b \in G \), \( G \) is abelian. Let \( a, b \in G \). Because \( G \) is a group, we know there exist \( a^{-1}, b^{-1} \in G \). Then:

\[
ba = (b^{-1})^{-1}(a^{-1})^{-1} = (a^{-1}b^{-1})^{-1} = (a^{-1})^{-1}(b^{-1})^{-1} = ab
\]

The second equality is due to the basic fact noted at the beginning of the proof, while the third equality is due to our hypothesis. Thus we have \( ab = ba \) for all \( a, b \in G \) and \( G \) is abelian.

Note that it is possible to prove this in a string of if and only if statements:

\((ab)^{-1} = a^{-1}b^{-1}\) for all \( a, b \in G \) \(\Leftrightarrow\) \((a^{-1}b^{-1})^{-1} = (a^{-1})^{-1}(b^{-1})^{-1}\) for all \( a, b \in G \) \(\Leftrightarrow\) \((b^{-1})^{-1}(a^{-1})^{-1} = (a^{-1})^{-1}(b^{-1})^{-1}\) for all \( a, b \in G \) \(\Leftrightarrow\) \( ba = ab \) for all \( a, b \in G \).

23. Let \( G \) be a group. Prove that if \( x^2 = e \) for all \( x \in G \), then \( G \) is abelian.

Because \( x^2 = e \), \( x \cdot x = e \) and \( x = x^{-1} \) for all \( x \in G \). Combining this result with an observation from the previous problem, we see that for \( a, b \in G \):

\[
ab = (ab)^{-1} = b^{-1}a^{-1} = ba
\]

24. Show that if \( G \) is a finite group with an even number of elements, then there must exist an element \( a \neq e \in G \) such that \( a^2 = e \).

Let \( A = \{a \in G|a = a^{-1}\} \), \( B = \{a \in G|a \neq a^{-1}\} \). Recall that for all \( a \in G \), there
exists a unique $a^{-1}$ such that $a^{-1}a = e = aa^{-1}$. Note also that $(a^{-1})^{-1} = a$. Therefore, we may partition $B$ into subsets $C_1, C_2 \ldots C_n$ consisting of pairs of inverses. For example, $C_1 = \{c, c^{-1}\}$ for some $c \in B$. Because $a \neq a^{-1}$ for all $a \in B$, $|C_i| = 2$ for all $1 \leq i \leq n$. Note that $|G| = |B| + |A| = \sum_{i=1}^{n} |C_i| + |A| = 2n + |A|$. As $e \in A$, $|A| \geq 1$. However, $|G|$ is even, so $|A| \geq 2$ and $A$ must contain an element other than the identity. Thus, there exists $a \in G$, $a \neq e$ such that $a^2 = e$.

1.1

17. Let $a, b, n$ be integers with $n > 1$. Suppose that $a = nq_1 + r_1$ with $0 \leq r_1 < n$ and $b = nq_2 + r_2$ with $0 \leq r_2 < n$. Prove that $n|(a - b)$ iff $r_1 = r_2$.

\[ \Rightarrow: \] Suppose without loss of generality that $r_1 \leq r_2$. If $n|(a - b)$ then $a - b = nq_3$ for some integer $q_3$. Adding $b$ to both sides, $a = nq_3 + b = nq_3 + nq_2 + r_2 = n(q_3 + q_2) + r_2$. Thus $nq_1 + r_1 = n(q_3 + q_2) + r_2$ and $n(q_1 - q_2 - q_3) = r_2 - r_1$. Then $|n|(r_2 - r_1)$, and because $0 \leq r_2 - r_1 \leq r_2 < n$, $r_2 - r_1 = 0$. Therefore, $r_2 = r_1$.

\[ \Leftarrow: \] If $r_1 = r_2$, then $a - b = n(q_1 - q_2) + (r_1 - r_2) = n(q_1 - q_2)$ which is clearly divisible by $n$.

18. Show that any nonempty set of integers that is closed under subtraction must also be closed under addition.

Let $S$ be a nonempty set of integers closed under subtraction, $a, b \in S$. Note $0 = a - a \in S$, and thus $-b = 0 - b \in S$. Therefore $a + b = a - (-b) \in S$, and $S$ is closed under addition.

1.2

16. A positive integer $a$ is called a square if $a = n^2$ for some $n \in \mathbb{Z}$. Show that the integer $a > 1$ is a square if and only if every exponent in its prime factorization is even.

The integer $a > 1$ is a square $\iff a = n^2$ for some $n = p_1^{a_1}p_2^{a_2}\ldots p_n^{a_n} \in \mathbb{Z} \iff a = (p_1^{a_1}p_2^{a_2}\ldots p_n^{a_n})^2 = p_1^{2a_1}p_2^{2a_2}\ldots p_n^{2a_n} \iff$ Every exponent in the prime factorization of $a$ is even.

17. Show that if the positive integer $a$ is not a square, then $a \neq \frac{b^2}{c^2}$ for integers $b, c$.

We proceed by contradiction. Let $a$ not be a square, $a = \frac{b^2}{c^2}$ and $p_1, p_2, \ldots p_n$ be the primes occurring in the prime factorization of any of $a, b$ or $c$. Then $a = p_1^{a_1}p_2^{a_2}\ldots p_n^{a_n}$ with $a_i \geq 0$ for all $1 \leq i \leq n$. By the previous problem, at least one $a_i$ is odd. Without loss of generality, suppose $a_1$ is odd. Let $b = p_1^{b_1}p_2^{b_2}\ldots p_n^{b_n}$, $c = p_1^{c_1}p_2^{c_2}\ldots p_n^{c_n}$.

Because $ac^2 = b^2$, we have:
\[ p_1^{a_1+2c_1} p_2^{a_2+2c_2} \cdots p_n^{a_n+2c_n} = (p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n})(p_1^{2c_1} p_2^{2c_2} \cdots p_n^{2c_n}) \]
\[ = (p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n})(p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n})^2 \]
\[ = ac^2 \]
\[ = b^2 \]
\[ = (p_1^{b_1} p_2^{c_2} \cdots p_n^{b_n})^2 \]
\[ = p_1^{2b_1} p_2^{2c_2} \cdots p_n^{2b_n} \]

By the fundamental theorem of arithmetic, \( a_i + 2c_i = 2b_i \) for all \( 1 \leq i \leq n \). In particular, \( a_1 + 2c_1 = b_1 \). This, however, is a contradiction, as \( a_1 \) is odd.