Problem 1.1 # 6. Determine which of the following sets are groups under addition.

(a) Rational numbers in lowest terms including \(0 = 0/1\) whose denominators are odd.
(b) Rational numbers in lowest terms whose denominators are even, together with \(0\).
(c) The set of rational numbers of absolute value \(< 1\).
(d) The set of rational numbers of absolute value \(\geq 1\) together with \(0\).
(e) The set of rational numbers with denominators equal to \(1\) or \(2\).
(f) The set of rational numbers with denominators equal to \(1\), \(2\) or \(3\).

Solution. Let \(G_{(a)}\) denote the set in (a), and similarly for \(G_{(b)}, \ldots\). Then \(G_{(a)}\) is a group, that is, an additive subgroup of \((\mathbb{Q}, +)\). Let \(G_{(b)}\) be the set of rational numbers in lowest terms including \(0 = 0/1\) whose denominators are odd. If \(x, y \in G_{(a)}\) we need to show that \(x + y, -x\) and \(0\) are in \(G_{(a)}\). Write \(x = a/b, y = c/d\) where \(b, d\) are odd. Then \(x + y = (ad + bc)/bd\). This expression may not be in lowest terms, but if we write \(x + y = r/s\) with \(s\) minimal then \(s\) divides \(bd\) so \(s\) is odd and \(x + y \in G_{(a)}\); also \(-x = (-a)/b\) and \(0 = 0/1\) are in \(G_{(a)}\) so \(G_{(a)}\) is a group.

Also \(G_{(e)}\) is a group; this may be characterized as the set of \(r \in \mathbb{Q}\) such that \(2r \in \mathbb{Z}\) and so if \(r, s \in G_{(e)}\) then \(2(r + s) = 2r + 2s \in \mathbb{Z}\) and similarly \(2(-r) = -2r \in \mathbb{Z}\) so this set is closed under the group operations and contains \(0\), confirming that it is a subgroup of \(\mathbb{Q}\).

\(G_{(b)}, G_{(c)}, G_{(d)}\) and \(G_{(f)}\) are not subgroups of \((\mathbb{Q}, +)\) because they are not closed under \(+\). We give examples to show this. First, \(1/2 \in G_{(b)}\) but \(1/2 + 1/2 = 1/1 \notin G_{(b)}\), so \(G_{(b)}\) is not a subgroup of \((\mathbb{Q}, +)\). Similarly \(3/4 \in G_{(c)}\) but \(3/4 + 3/4 = 3/4 \notin G_{(c)}\); \(2, -3/2 \in G_{(d)}\) but \(2 + (-3/2) \notin G_{(d)}\); and finally, \(1/2, 1/3 \in G_{(f)}\) but \(1/2 + 1/3 = 5/6 \notin G_{(f)}\).
Problem 1.1 # 12. Find the orders of the following elements of \((\mathbb{Z}/12\mathbb{Z})^\times\): \(1, -1, 5, 7, -7\) and \(13\).

Solution. The orders are given by the following table:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>-1</th>
<th>5</th>
<th>-7</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>order of x</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Note that \(13 = 1\).

Problem 1.1 # 15. Prove that \((a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}\) in a group \(G\).

Solution. Let \(x = a_1 \cdots a_n\) and \(y = a_n^{-1} \cdots a_1^{-1}\). We check that \(xy = 1\). When we multiply \(x\) and \(y\) together we may cancel adjacent entries in pairs, thus:

\[
xy = a_1 \cdots a_n a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1} = a_1 \cdots a_n^{-1} \cdot a_{n-1}^{-1} \cdots a_1^{-1} = a_1 \cdots a_{n-1} a_n^{-1} \cdots a_1^{-1} = a_1 \cdots a_{n-2} a_{n-2}^{-1} \cdots a_2^{-1} = \cdots = a_1 a_1^{-1} = 1.
\]

We have shown that \(xy = 1\). Therefore \(x^{-1} = y\), that is, \((a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}\) as required.

Problem 1.1 # 22. If \(x\) and \(g\) are elements of a group \(G\) prove that \(|x| = |g^{-1}xg|\). Deduce that \(|ab| = |ba|\) for \(a, b \in G\).

Solution.

Lemma 1 If \(x, g \in G\) then

\[
(g^{-1}xg)^k = g^{-1}x^k g.
\]

Proof If \(k > 0\) then the left-hand side of (1) equals

\[
(g^{-1}x)(g^{-1}x)(g^{-1}x) \cdots (g^{-1}x),
\]

with \(k\) factors. Cancelling \(gg^{-1}\) gives \(g^{-1}x^k g\). Equation (1) remains true if \(k < 0\) or \(k = 0\), but we leave these cases (which we don’t actually need for this exercise) to the reader.

Now \((g^{-1}xg)^k = 1\) if and only if \(g^{-1}x^k g = 1\) or \(x^k = g \cdot g^{-1} = 1\). This means that \(x\) and \(g^{-1}xg\) have the same order. This proves the first assertion.

Two elements \(x\) and \(y\) are called conjugates if \(y = gxg^{-1}\) for some \(g \in G\). We have proven that two conjugates have the same order. To prove the second assertion, we note that \(ab\) and \(ba\) are conjugates. This follows from the identity \(ba = b(ab)b^{-1}\). Since \(ba\) and \(ab\) are conjugates, they have the same order.
Problem 1.1 # 25. Prove that if $x^2 = 1$ for all $x \in G$ then $G$ is abelian.

Solution. Let $x, y \in G$. Then $(xy)^2 = 1$. Multiply this identity on the left by $x$ and on the right by $y$. Then $x(xy)(xy)y = xy$ and since $x^2 = y^2 = 1$, this implies $yx = xy$. Therefore $G$ is abelian.

Problem 1.2 # 1. Compute the order of each of the elements in the following groups:
(a) $D_6$; (b) $D_8$; (c) $D_{10}$.

Solution. We will denote by $\gcd(a, b)$ the greatest common divisor of two integers $a, b$.

Lemma 2 Let $r$ be an element of order $n$ in some group. Then the order of $r^i$ is $n/\gcd(n, i)$.

Proof Let $d = \gcd(a, b)$. Then $(r^i)^k = 1$ if and only if $n$ divides $ik$. Note that $\frac{n}{d}$ and $\frac{i}{d}$ are coprime integers. So $(r^i)^k = 1$ if and only if $\frac{ik}{n} = \frac{(i/d)k}{(n/d)}$ is an integer. Since $(i/d)$ and $(n/d)$ are coprime, this means $(r^i)^k = 1$ if and only if $n/d$ divides $k$, and hence $n/d$ is the order of $r^i$. \qed

It will be shown in Problem 1.2 #3 that $sr^i$ has order 2 for any $i$. From this and the Lemma we now have the orders of the elements of $D_6$, $D_8$ and $D_{10}$.

<table>
<thead>
<tr>
<th></th>
<th>$x$</th>
<th>$r^2$</th>
<th>$r^4$</th>
<th>$s$</th>
<th>$sr$</th>
<th>$sr^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>order of $x$</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

$D_8$:

<table>
<thead>
<tr>
<th></th>
<th>$x$</th>
<th>$r^2$</th>
<th>$r^4$</th>
<th>$s$</th>
<th>$sr$</th>
<th>$sr^2$</th>
<th>$sr^3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>order of $x$</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

$D_{10}$:

<table>
<thead>
<tr>
<th></th>
<th>$x$</th>
<th>$r^2$</th>
<th>$r^4$</th>
<th>$s$</th>
<th>$sr$</th>
<th>$sr^2$</th>
<th>$sr^3$</th>
<th>$sr^4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>order of $x$</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Problem 1.2 # 2. Use the generators and relations above to show that if $x$ is any element of $D_{2n}$ which is not a power of $r$ then $rx = xr^{-1}$.

Solution. If $x \in D_{2n}$ is not a power of $r$, then using (4) on page 25, we can write $x = sr^i$ for some $i$. Now $rx = rsr^i = s \cdot sr^{-1} \cdot ri = sr^{-1+i} = sr^i \cdot r^{-1} = xr^{-1}$.

Problem 1.2 # 3 Use the generators and relations above to show that every element of $D_{2n}$ which is not a power of $r$ has order 2. Deduce that $D_{2n}$ is generated by the two elements $s$ and $sr$, both of which have order 2.
Solution. If \( x \in D_{2n} \) is not a power of \( r \), then using (4) on page 25, we can write \( x = sr^i \) for some \( i \). Now \( x^2 = sr^i sr^i = (sr^i s^{-1}) r^i = (sr s^{-1}) r^i = (r^{-1}) r^i = 1 \). Since \( x \neq 1 \) this proves \( x \) has order 2.

Now we claim that \( s, sr \) (both of which have order 2) generate \( D_{2n} \). Indeed, let \( G \) be the subgroup of \( D_{2n} \) generated by \( s \) and \( sr \). Then \( r = s^{-1}(sr) \in G \), so \( G \) contains both \( r \) and \( s \). These generate \( D_{2n} \) so \( G = D_{2n} \), proving that \( D_{2n} \) is generated by two elements of order 2.

Problem 7.1 # 3. Let \( R \) be a ring with 1. Let \( S \) be a subring of \( R \) containing 1. Prove that if \( u \) is a unit in \( S \) then \( u \) is a unit in \( R \). Give an example to show that the converse is not true.

Solution. If \( u \) is a unit in \( S \) then there is an element \( u^{-1} \in S \) such that \( uu^{-1} = u^{-1}u = 1 \). Since \( S \subseteq R \), \( u^{-1} \in R \) proving that \( u \) is a unit in \( R \). This proves the first assertion.

For the counterexample, let \( S = \mathbb{Z} \), \( R = \mathbb{Q} \). Then 2 is a unit in \( \mathbb{Q} \), but not in \( \mathbb{Z} \).

Problem 7.1 # 5. Decide which of the following (a)–(f) are subrings of \( \mathbb{Q} \):

(a) The set of rational numbers with odd denominators (written in lowest terms);
(b) The set of rational numbers with even denominators (when written in lowest terms);
(c) The set of nonnegative rational numbers.
(d) The set of squares of rational numbers.
(e) The set of rational numbers with odd numerators (when written in lowest terms).
(f) The set of rational numbers with even numerators (when written in lowest term).

Solution. Only (a) and (f) are rings. The ring (a) is the only ring with an identity in this list.