1.1. (a) No: \((a - b) - c = a - b - c, a - (b - c) = a - b + c\). These are different when \(c \neq 0\).
(b) Yes, \((a * b) * c\) and \(a * (b * c)\) are both equal to \(a + b + c + ab + bc + ab + abc\).
(c) No: \((a * (b * c)) = \frac{a^2}{25} + \frac{b}{25} + \frac{c}{5}\) and \((a * b) * c = \frac{a}{25} + \frac{b}{5} + \frac{c}{5}\), which are not equal unless \(a = c\).
(d) Yes. Here’s an interesting way to show that it is associative. For each pair \((a, b)\), consider the matrix
\[M_{(a, b)} = \begin{pmatrix} b & a \\ 0 & b \end{pmatrix}.\]
One can check that the multiplication of pairs (in this problem) is the same as matrix multiplication of the corresponding matrices. Since matrix multiplication is associative, so is the multiplication of pairs.

How does one figure this out? Suppose you are given some binary operation \(*\) on vectors in \(\mathbb{R}^n\), and suppose you notice that \(u * v\) depends on \(v\) in a linear way. Then the linear map \(v \mapsto u * v\) can be expressed by a matrix:
\[u * v = M_u v\]
If \(M_a M_b = M_{a*b}\), then the \(*\) multiplication is the same as matrix multiplication, so it’s associative. In this problem, one works out the 2x2 matrix \(M\) such that
\[M \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ad + bc \\ bd \end{pmatrix}\]
(e) No. \((a * b) * c = ab^{-1}c^{-1}\) and \(a * (b * c) = ab^{-1}c\), so these will be different unless \(c = 1\).

1.6. (a) Yes.
(b) No, it’s not closed under \(+\). For example, \(\frac{1}{6} + \frac{1}{6} = \frac{1}{3}\).
(c) No, not closed under \(+\).
(d) No, not closed under \(+\). For example \(2 + (-3/2) = 1/2\).
(e) Yes.
(f) No, not closed: \(1/2 + (-1/3) = 1/6\).

22. By the associative law (and induction), \((g^{-1}xg)^n = g^{-1}x^n g\). Therefore
\[(g^{-1}xg)^n = 1 \iff g^{-1}x^n g = 1 \iff x^n = g1g^{-1} = 1\]
so \(|x| = |g^{-1}xg|\). If we take \(x = ab\) and \(g = b^{-1}\), then \(g^{-1}xg = b(ab)b^{-1} = ab\), so this shows \(|ab| = |ba|\).

Remark: we can also show directly that \(ab\) and \(ba\) have the same order. Note that \((ab)^n = a(ba)^{n-1}b\). Thus if \((ab)^n = 1\), then multiplying on the left by \(b\) and on the right by \(b^{-1}\) gives
\[(ba)^n = bb^{-1} = 1.\]
So \((ab)^n = 1\) implies \((ba)^n = 1\). Likewise \((ba)^n = 1\) implies \((ab)^n = 1\).
25. Suppose \( x^2 = 1 \) for every \( x \in G \). Thus every element is its own inverse. Now for any group, \((xy)^{-1} = y^{-1}x^{-1}\). Thus in this group, \( xy = yx \).

31. Consider all pairs \( \{a, b\} \) where \( ab = 1 \) and \( a \neq b \). Each element of \( t(G) \) belongs to exactly one such pair, so the number of elements of \( t(G) \) is twice the number of such pairs and is therefore even.

Thus \( G - T(G) \) also has an even number of elements. Since \( G - t(G) \) contains the element 1, it must have at least one other element \( a \neq 1 \). Since \( a \notin t(G) \), \( a = a^{-1} \), which means \( a^2 = 1 \), so \( a \) has order 2.

35. Suppose \( m \) in \( \mathbb{Z} \). By the division algorithm, \( m = nq + r \) with \( 0 \leq r < n \), and then
\[
x^m = x^{nq}x^r = (x^n)^q x^r = x^r \in \{1, x, \ldots, x^{n-1}\}.
\]

1.2.3. If \( g \in D_{2n} \) is not a power of \( r \), then \( g = sr^i \neq 1 \). Recall that \( r^i s = sr^{-i} \) and \( r^2 = 1 \), so
\[
g^2 = sr^i sr^{-i} = s(r^i r)^i = s(s r^{-i}) r^i = s^2 = 1
\]

Thus \( a = s \) and \( b = sr \) each have order 2. We can express \( s \) and \( r \) in terms of \( a \) and \( b \) (namely \( s = a \) and \( r = ab \)), so \( a \) and \( b \) generate the whole group.

1.3: 15. Suppose \( \sigma \in S_n \), and write \( \sigma = \alpha_1 \cdots \alpha_k \) where the \( \alpha_i \) are disjoint cycles. For each \( i \) let \( d_i \) be the length of \( \alpha_i \), so \( d_i \) is also the order of \( \alpha_i \). Since disjoint cycles commute, for every \( n \in \mathbb{Z} \)
\[
\sigma^n = (\alpha_1 \cdots \alpha_k)^n = \alpha_1^n \cdots \alpha_k^n.
\]

Since the \( \alpha_i \) are disjoint, the \( \alpha_i^n \) are disjoint, and so \( \alpha_1^n \cdots \alpha_k^n = 1 \iff \alpha_1^n = \cdots = \alpha_k^n = 1 \). But \( \alpha_i^n = 1 \iff d_i \mid n \), so
\[
\sigma^n = 1 \iff d_i \mid n \text{ for every } i \iff \text{l.c.m.}[d_1, \ldots, d_k] \mid n.
\]

Therefore the order of \( \sigma \) is \( \text{l.c.m.}[d_1, \ldots, d_k] \).

19. By 15, \( n \) is the order of some \( \sigma \in S_7 \) if and only if \( n \) is the least common multiple of a sequence of integers \( d_1, \ldots, d_k \) where \( d_1 + \cdots + d_k \leq 7 \). We may also assume that each \( d_i > 1 \) (unless all \( d_i \) are equal to 1), and that the \( d_i \) are relatively prime. This gives the following possibilities:
\[
d_1, \ldots, d_k : 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 2, 3 \quad 2, 5 \quad 3, 4
\]
\[
n : 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 6 \quad 10 \quad 12
\]

Therefore the set of possible orders is \( \{1, 2, 3, 4, 5, 6, 7, 10, 12\} \).

1.6: 4. The groups cannot be isomorphic since \( \mathbb{C} \setminus \{0\} \) has an element of order 4 (namely \( i = \sqrt{-1} \)) whereas \( \mathbb{R} \setminus \{0\} \) does not.
(A slightly different way to see they are not isomorphic: \( \mathbb{C} \setminus \{0\} \) has 4 elements \( x \) such that \( x^4 = 1 \), namely 1, \(-1\), \( i \), and \(-i \), whereas \( \mathbb{R} \setminus \{0\} \) has only 2.)

17. Let \( f(x) = x^{-1} \). Then \( f(xy) = (xy)^{-1} = y^{-1}x^{-1} \). (This is true for any group.)

Thus

\[
\begin{align*}
f(xy) &= y^{-1}x^{-1} \\
f(x)f(y) &= x^{-1}y^{-1}
\end{align*}
\]

If \( G \) is abelian, then the right hand sides of these two equations are equal (for all \( x \) and \( y \)), so the left hand sides are equal, which means \( f \) is a homomorphism.

Conversely, if \( f \) is a homomorphism, then the left hand sides are equal (for all \( x \) and \( y \)), so the right hand sides are equal, which means \( x^{-1} \) and \( y^{-1} \) commute. In particular, given any elements \( a \) and \( b \), this must be true when \( x = a^{-1} \) and \( y = b^{-1} \). Thus \( a \) and \( b \) commute.

22. Let \( \phi: A \rightarrow A \) be the map \( \phi(a) = a^k \). Since \( A \) is commutative, \( \phi(ab) = (ab)^k = a^kb^k = \phi(a)\phi(b) \) (exercise 24, §1.1) so \( \phi \) is a homomorphism. If \( k = -1 \) then \( (\phi \circ \phi)(a) = \phi(a^{-1}) = (a^{-1})^{-1} = a \), i.e., \( \phi \circ \phi \) is the identity map, so the map \( \phi \) has a left-inverse and a right-inverse, and so \( \phi \) is a bijection and hence an isomorphism.

Additional Problems

I. Since every permutation is a product of cycles, it suffices to show that every cycle is a product of 2-cycles. A little experimentation shows that \( (a_1a_2\ldots a_k) = (a_1a_2)(a_2a_3)\ldots(a_{k-1}a_k) \).

II. By problem 15 of 1.3, the elements of order \( p \) are precisely the \( p \)-cycles \( (a_1a_2\ldots a_p) \). If (as customary) we choose \( a_1 = 1 \), then we have \( p - 1 \) choices for \( a_2 \). Having chosen \( a_2 \), we then have \( p - 2 \) choices for \( a_3 \), and so on. Thus there are \( (p - 1)! \) different \( p \)-cycles.

III. As in problem 1.3.19, we look for relatively prime numbers \( d_1, \ldots, d_k \) whose sum is \( \leq 10 \): we wish the product to be as large as possible.

Suppose we have a collection \( d_1, \ldots, d_k \) of such numbers and that one of them is 6. Note if we replace 6 by 2 and 3, the sum will still be \( \leq 10 \) and the LCM is the same. Likewise 10 can be replaced by 2 and 5. (In general, we may require that each \( d_i \) be a prime number raised to some power.)

Thus we are to choose at most one number from each row of

\[
\begin{array}{ccc}
2 & 4 & 8 \\
3 & 9 & \\
5 & \\
7 & \\
\end{array}
\]

in such a way that the sum is \( \leq 10 \) and the product is a maximum.

If we include 7, the choices are \((7), (7, 3), (7, 2), (7, 4)\). Of these \((7, 4) \mapsto 28\) is clearly the best.

If we include 5 but not 7, the choices are \((5), (5, 3), (5, 2), (5, 4), (5, 3, 2)\). Clearly \((5, 4) \mapsto 20\) beats the preceding 3 choices, but it is beaten by \((5, 3, 2) = 30\).

If we don’t include 5 or 7, but do include a power of 3, the choices are \((3), (3, 2), (3, 4), \) and \((9)\), the best of which is \((3, 4) \mapsto 12\).

Finally, if we only include a power of 2, the best choice is 8.

Thus the best overall is \((5, 3, 2) \mapsto 30\).