Comments from the grader: a few students misunderstood associativity as commutativity. About half of the students were not careful enough for the fourth part of 1, as they did not check that $\mathbb{Q} - \{1\}$ is closed under the operation (but no points were deducted for this). In problem 6, some students used the division algorithm, and the grader did not understand what they were doing. About 20% did not understand the difference between problems 5 and 6.

1. $\mathbb{Z}$ is not a group under subtraction, because subtraction is not associative:

$$0 - (0 - 1) = 1 \neq -1 = (0 - 0) - 1.$$

Moreover, there is no $n \in \mathbb{Z}$ such that $n - m = m$ for all $m \in \mathbb{Z}$.

$\mathbb{Z}$ is not a group under the operation $a * b := a + b + ab$ either, as -1 has no inverse. In fact multiplication by -1 is not injective: for all $n \in \mathbb{Z}$

$$n * (-1) = n - 1 - n = -1.$$

$\mathbb{N}$ is not a group under addition, because 1 has no inverse ($1 + n \geq 1$ for all $n \in \mathbb{N}$).

$\mathbb{Q} - \{-1\}$ is a group under the given operation, with identity 0 and

$$a^{-1} = -\frac{a}{a+1}$$

for all $a \in \mathbb{Q} - \{-1\}$.

The set of rational numbers with denominator divisible by five (when written in lowest terms) is not closed under addition, because $\frac{2}{5} + \frac{3}{5} = \frac{1}{1}$.

If G has more than one element, then the operation $a * b := a$ has no identity element: given a candidate $e \in G$, pick a different element $a \in G$ and note that $e * a = e \neq a$.

2. Let $a, b \in G$. By assumption $abab = (ab)^2 = e$. Multiplying by a and b gives

$$ba = a^2bab^2 = a(abab)b = aeb = ab.$$

3. From example 10 in the book, we know that $fh = h^{-1}f$. Conjugating both sides by h^{-1} gives $hf = fh^{-1}$. You can show by induction that $h^jf = fh^{-j}$ for all $j \in \mathbb{N}$. Conjugating both sides by h^j extends this to all $j \in \mathbb{Z}$. In a similar way, you can prove that

$$h^jf^s = f^sh^{(-1)^sj}$$

for all $s, j \in \mathbb{Z}$. It follows that

$$(f^ih^j) * (f^sh^t) = f^{i+s}h^{(-1)^sj+t}$$

for all $i, j, s, t \in \mathbb{Z}$. By dividing the exponents by 2 and n respectively, and taking remainders, you can write this as $f^a h^b$ for some $a \in \{0, 1\}$ and $b \in \{0, \ldots, n-1\}$. Therefore D_{2n} is closed under the operation. The operation is associative, because it is just function composition. Moreover, the identity function $f^0 h^0$ belongs to D_{2n}. Finally, each element $f^a h^b \in D_{2n}$ has an inverse, namely $h^{n-b} f^{2-a}$. Therefore D_{2n} is a group.

To see that D_6 has order 6, we need to check that the elements $f^a h^b$ are distinct for $a \in \{0, 1\}$ and $b \in \{0, 1, 2\}$. This can be done, for example, by writing down matrices representing each element. It follows that D_6 is nonabelian, because

$$hf = fh^{-1} = fh^2 \neq fh.$$

4. The identity permutation has order 1.

   Let $a, b, c, d \in \{1, 2, 3, 4\}$ be distinct. You can check directly that the permutation which sends $a \mapsto b \mapsto c \mapsto d \mapsto a$ has order 4. There are $3 \times 2 = 6$ such permutations, because 1 can be sent to 3 possible elements (namely 2, 3 or 4), the latter has 2 places to go, and the others have no choice.

   The permutation which swaps a with b and c with d clearly has order 2. There are only 3 such permutations, because 1 can be sent to 3 possible elements, and the other two must be swapped.

   The permutation which just swaps a with b also has order 2. However, there are $\binom{4}{2} = 6$ such permutations, one for each choice of $\{a, b\} \subset \{1, 2, 3, 4\}$.

   On the other hand, the permutation which sends $a \mapsto b \mapsto c \mapsto a$ and fixes d has order 3. There are $4 \times 2 = 8$ such permutations, because d can be any element of $\{1, 2, 3, 4\}$, and the smallest element of $\{1, 2, 3, 4\} - \{d\}$ has just 2 places to go.

   Since S_4 has $4! = 24$ elements, and $1 + 6 + 3 + 6 + 8 = 24$, every element of S_4 is described above. The elements $x \in S_4$ such that $x^4 = e$ are those appearing in the first four paragraphs (but not the fifth).

5. Suppose that, for some $a \in G$, there is no positive integer n such that $a^n = e$. If $i, j \in \mathbb{Z}$ and $i \neq j$, then $a^i \neq a^j$, since otherwise $i - j$ or $j - i$ would be such a positive integer n. This shows that the function $\mathbb{Z} \to G$ sending $i \mapsto a^i$ is injective, contradicting the fact that G is finite. Thus, for every $a \in G$, there is a positive integer n such that $a^n = e$.

6. Since G is finite, we can list its elements: $G = \{a_1, \ldots, a_{|G|}\}$. For each i there is a positive integer n_i such that $a_i^{n_i} = e$. Let m be the product of the n_i, i.e. $m \coloneqq n_1 \cdots n_{|G|}$. If $a \in G$,

then $a = a_i$ for some i, in which case $a^{n_i} = e$ and hence $a^{kn_i} = e$ for all $k \in \mathbb{Z}$. In particular $a^m = e$.

7. Let A and B be subgroups of G. As proven in the book, it suffices to show that $A \cap B$ is closed under the operation and under taking inverses. To this end, let $x, y \in A \cap B$. Since $x, y \in A$, and A is a subgroup, $xy \in A$ and $x^{-1} \in A$. Similarly $xy \in B$ and $x^{-1} \in B$. Therefore $xy \in A \cap B$ and $x^{-1} \in A \cap B$, which completes the proof.

8. For each $a \in \{1, 2, 3\}$ let s_a be the permutation which fixes a but swaps the other two elements. Also let t be the permutation which sends $1 \mapsto 2 \mapsto 3 \mapsto 1$. You can check (as in problem 4) that $S_3 = \{e, s_1, s_2, s_3, t, t^{-1}\}$. Clearly $C(e) = S_3$.

   You can check directly that s_1 does not commute with s_2. A similar argument shows that none of the s_i commute with each other. Therefore $C(s_1) \subseteq \{e, s_1, t, t^{-1}\}$. Since $C(s_1)$ is a subgroup of S_3, it either contains t and t^{-1}, or neither of them. Moreover, the order of $C(s_1)$ divides 6 (by Lagrange's theorem). Since $\{e, s_1\} \subseteq C(s_1)$, the only possibility is that $C(s_1) = \{e, s_1\}$. Similarly $C(s_2) = \{e, s_2\}$ and $C(s_3) = \{e, s_3\}$.

   Since t does not belong to any $C(s_i)$, it does not commute with any s_i. This implies that $C(t) \subseteq \{e, t, t^{-1}\}$. We already know that $\{e, t\} \subseteq C(t)$, so $t^{-1} \in C(t)$ because $C(t)$ is a subgroup of S_3. Therefore $C(t) = \{e, t, t^{-1}\}$. The same argument applies to $C(t^{-1})$.

9. Let H be a subgroup of a cyclic group G. If $H = \{1\}$, then $H = (1)$ is cyclic. Otherwise, there is a smallest positive integer n such that $a^n \in H$. We aim to show that $H = (a^n)$. Since H is a subgroup of G, $(a^n) \subseteq H$. To prove the reverse inclusion, let $h \in H$. Since $h \in G$, we can write $h = a^k$ for some $k \in \mathbb{Z}$. Dividing by n gives $q, r \in \mathbb{Z}$ such that $k = qn + r$ and $0 \leq r < n$. In fact $r = 0$, since

$$a^r = a^{k-qn} = a^k (a^n)^{-q} \in H$$

   (otherwise $r < n$ is a positive integer such that $a^r \in H$). Therefore $h = a^k = (a^n)^q \in (a^n)$.

10. We might as well just do the challenge problem. Given indices $i \neq j$, let E_{ij} denote the $n \times n$ matrix which has a 1 in the ith row of the jth column, and zeros everywhere else. Also let I be the $n \times n$ identity matrix. Note that $I + E_{ij} \in G$, because $\det(I + E_{ij}) = 1$ (as a triangular matrix, its determinant is just the product of the diagonal entries).

    Let $A \in Z(G)$, and denote the ith entry of the jth column of A by a_{ij}. You can check that

$$AE_{ij} = \begin{pmatrix} 0 & \dots & 0 & a_{1i} & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & a_{ni} & 0 & \dots & 0 \end{pmatrix}$$

has zeros in all but the jth column, which is a copy of the ith column of A. Similarly

$$E_{ij}A = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \\ a_{j1} & \dots & a_{jn} \\ 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}$$

has the jth row of A as its ith row. Since A is central, $A(I + E_{ij}) = (I + E_{ij})A$. Cancelling A from both sides gives $AE_{ij} = E_{ij}A$. Since AE_{ij} is zero outside the jth column, and $E_{ij}A$ is zero outside the ith row, $a_{ki} = 0$ for all $k \neq i$ and $a_{jk} = 0$ for all $k \neq j$. The remaining nonzero entry of AE_{ij} is a_{ii}, which matches up with a_{jj} inside $E_{ij}A$. By varying i and j, we see that $a_{ij} = 0$ whenever $i \neq j$, but $a_{ii} = a_{jj}$. In other words $A = a_{11}I$.

Conversely, if $A = aI$ for some $a \in \mathbb{R}$, then $AB = aIB = aB = aBI = B(aI) = BA$ for any $n \times n$ matrix B, so in particular $A \in Z(G)$. Therefore

$$Z(G) = \{aI \mid a \in \mathbb{R}\}.$$