Solutions

Problem 1 Indicate whether the following statements are true or false. You do not need to justify your answers and no partial credit will be awarded.

1. Every binary operation is associative.
2. If x, y are elements of a group G, and $x = y^{-1}$, then $y = x^{-1}$.
3. The set of integers $\mathbb{Z}$ form a group under multiplication.
4. Subtraction is an associative binary operation on $\mathbb{Z}$.
5. If x is an element in a group G of order 1, then x is the identity.

Solution: 1) **False**. The binary operation of subtraction on $\mathbb{Z}$ is not associative since $(1-1)-1 \neq 1-(1-1)$.

2) **True**. This follows from the theorem $(x^{-1})^{-1} = x$ proven in the textbook.

3) **False**. The binary operation is not cancellative since $0 \cdot 2 = 0 \cdot 3$ but $2 \neq 3$. We have seen that all groups are cancellative.

4) **False**. Consider $(1-1)-1 \neq 1-(1-1)$.

5) **True**. If x has order 1, then $x^1 = e$. Since $x^1 = x$, we see $x = e$.

Problem 2 Find $\gcd(72, 56)$ and two integers x, y such that $72x + 56y = \gcd(72, 56)$.

Solution: We apply the Euclidean algorithm for 72 and 56:

$$\begin{aligned} 72 &= 1(56) + 16 \\ 56 &= 3(16) + 8 \\ 16 &= 2(8) + 0 \end{aligned}$$

Thus, $\gcd(72, 56) = 8$.

Now we apply the extended Euclidean algorithm to find Bezout coefficients:

$$\begin{aligned} 8 &= (1)(56) + (-3)(16) \\ &= (1)(56) + (-3)[72 + (-1)(56)] \\ &= (-3)(72) + (4)(56) \end{aligned}$$

Thus $x = -3$ and $y = 4$ give a solution to the equation.

Problem 3 Let G be the set of positive integers and consider the binary operation $x * y = 2x + 2y$ on G. Is $*$ associative? Is $*$ commutative? Does $(G, *)$ form a group?

Solution: The operation is *not* associative. Indeed, $(2*1)*1 = 6*1 = 14$ while $2*(1*1) = 2*4 = 12$.

However, $*$ is commutative since $x * y = 2x + 2y = 2y + 2x = y * x$ for all positive integers x and y.

Since $*$ is not associative, $(G, *)$ is not a group.

Comments: Many students showed that $x * (y * z) = 2x + 4y + 4z$ and $(x * y) * z = 4x + 4y + 2z$ and concluded that this meant G was not associative. *Technically*, we need to verify with a specific counterexample that this isn't somehow an equality for everything in G. (I gave full credit anyway, though.)

Problem 4 Let G be a group. Suppose $xyz = yzx$ for all $x, y, z \in G$. Prove that G is abelian.

Solution: Let $a, b \in G$. Since G is a group, it has an identity element e. The formula we are assuming gives $aeb = eba$. Simplifying, this is $ab = ba$, which shows that G is abelian.

Comments: Several students said (something like) every element w of G can be written $w = yz$ for some $y, z \in G$. Thus $x(yz) = (yz)x$ demonstrates $xw = wx$ for all $x, w \in G$. However, you still need to prove that every element of G can be written as a product! To see how this might fail when G is not a group, consider the binary operation of multiplication on the set of even integers E; there is no solution to $yz = 2$ for $y, z \in E$.

Problem 5 Let n and d be positive integers. Let M be a matrix of order n in the general linear group $\mathrm{GL}(d, \mathbb{R})$. Let M^T denote the transpose matrix of M. Show that M^T is in $\mathrm{GL}(d, \mathbb{R})$ and M^T has order n.

Solution: From linear algebra, we know that M is invertible if and only if M^T is invertible. Since M is invertible, so must be M^T. Thus, M^T is also in $\mathrm{GL}(d, \mathbb{R})$.

Another key fact from linear algebra is that for any square matrix A, we have $(A^T)^k = (A^k)^T$ for all positive integers k. If A is a matrix of finite order k, then $A^k = I_d$. Thus $(A^T)^k = (A^k)^T = I_d$ and $o(A^T) \leq o(A)$. Since M has order n, we have $o(M^T) \leq o(M)$. Now $(M^T)^T = M$ and M^T has finite order, so we apply the result again to conclude $o(M) = o((M^T)^T) \leq o(M^T)$. Thus $o(M) = o(M^T)$.

Comments: You can derive the facts we used above using only the definition of the transpose and the fact that $(AB)^T = B^T A^T$. Indeed, even the fact can be proved from the definition without too much trouble. Many students showed that $(M^T)^n = (M^n)^T = I_d$ and then concluded that $o(M^T) = n$ right away. To see why that's not enough, consider the case where you are considering the order of M^2 instead of M^T. It's certainly true that $(M^2)^n = (M^n)^2 = I_d$, but that only tells you that $o(M^2) \leq n$. Indeed, if M has order 2 then it is a strict inequality.