Math 453

Selected Solutions to Assignment 3

Problem 5: Let S be a set with an associative law of composition and with an identity element. Let G be the subset of S consisting of invertible elements (i.e. those $s \in S$ for which there is an inverse under the given law of composition). Show that G is a group.

Solution: First, note that that G has a binary operation $\phi : G \times G \to S$ inherited from the law of composition on S (define $\phi(a, b) = a * b$, where $*$ is the law of composition on S), but for G to be a group, we need to show that $\phi(G \times G) \subseteq G$. That is, we need to show that for each $x, y \in G$, $\phi(x, y) \in G$, so G is closed under ϕ. Let $x, y \in G$. Then by definition of G, there exist $x^{-1}, y^{-1} \in S$. By Problem 2, we have that $(x * y)^{-1} = y^{-1} * x^{-1}$; since $y^{-1} * x^{-1} \in S$, we have that $x * y$ has an inverse in S. Thus, $\phi(x, y) = x * y \in G$.

Now, ϕ is associative since for each $a, b, c \in G$, we have

$$\phi(\phi(a, b), c) = \phi(a, b) * c = (a * b) * c = a * (b * c) = a * (\phi(b, c)) = \phi(a, \phi(b, c)),$$

with the middle equality by the fact that $a, b, c \in S$ and associativity of $*$ on S, and all others by definition of ϕ. Hence, G has an associative binary operation.

Furthermore, let $e \in S$ denote the identity element; then $e * e = e$, so e has an inverse in S by definition of an inverse element. Hence, $e \in G$. Since for each $g \in G$, $\phi(e, g) = e * g = g = g * e = \phi(g, e)$, we have that g is the identity element on G with respect to the binary operation ϕ.

Finally, let $x \in G$, so there exists an inverse element $x^{-1} \in S$ with respect to $*$. By Problem 2, we have $(x^{-1})^{-1} = x$, so x^{-1} has an inverse element in S with respect to $*$ (namely, x), so $x^{-1} \in G$. Since $*$ acts on G the same way that ϕ does, for each $x \in G$, x has an inverse element with respect to ϕ. Therefore, G is a group under the binary operation ϕ.

Problem 6: Determine all integers n such that 2 has an inverse (under multiplication) modulo n.

Solution: We will show that if we extend our definition of modular arithmetic to be include any integer, 2 has a multiplicative inverse modulo n if and only if n is an odd integer. (Arguably, you could exclude the case where $n = \pm 1$, since the "spirit of the question," and our particular definition of modular arithmetic, excluded this case.) Note that the multiplicative identity modulo n is 1 modulo n, which is also 0 modulo n if $n = \pm 1$.

Let n be odd. Then $n = 2k+1$ for some $k \in \mathbb{Z}$, so $n = 2(k+1) - 1$, so $2(k+1) \equiv 1 \bmod n$ by definition of modular arithmetic. Hence, there exists an inverse under multiplication modulo n.

On the other hand, suppose $n \in \mathbb{Z}$ such that 2 has an inverse under multiplication modulo n. Then by definition of modular arithmetic, there exist $k, l \in \mathbb{Z}$ such that $2k - 1 = nl$, so $2k = nl + 1$. Then by definition of even, $nl + 1$ is even, so nl is odd, so n and l must both be odd. Hence, n is odd.

Problem 7: Let a, b be elements of a group G. Suppose that a has order 5 and that $a^3b = ba^3$. Prove that $ab = ba$.

Solution: We have $a^3b = ba^3$, so by multiplying on the left by b^{-1}, we have $b^{-1}a^3b = (b^{-1})ba^3$, so $b^{-1}a^3b = ea^3 = a^3$. Hence,

$$\begin{aligned} b^{-1}a^6b &= b^{-1}a^3(bb^{-1})a^3b \\ &= (b^{-1}a^3b)(b^{-1}a^3b) \\ &= (a^3)(a^3) \\ &= a^6. \end{aligned}$$

But $a^6 = (a^5)a = ea = a$ since a has order 5. Hence, $b^{-1}ab = a$, so multiplying on the left by b gives $ab = ba$, as desired.