# Math 56: Proofs and Modern Mathematics
# Homework 1 Solutions

Naomi Kraushar

October 11, 2021

**Problem 1.** Suppose $X$ is a non-empty set, and let $S$ be the collection of maps $f : X \to X$. Show that $S$ is a monoid, with composition of maps as the operation: $\circ : S \times S \to S$.

**Solution.** Since $X$ is nonempty, there exist maps from $X$ to itself, so $S$ is non-empty. We need to prove that composition is associative, and that there exists an identity element.
Associativity: Let $f, g, h$ be maps from $X$ to itself; we want to show that $(f \circ g) \circ h = f \circ (g \circ h)$. Let $x$ be an arbitrary element in $X$. By definition, we have

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))).$$

Similarly, we have

$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))).$$

Hence $((f \circ g) \circ h)(x) = (f \circ (g \circ h))(x)$ for all $x \in X$, so $(f \circ g) \circ h = f \circ (g \circ h)$, as required.

Identity: Define the identity function $e : X \to X$ by $e(x) = x$ for all $x \in X$. Let $f$ be an arbitrary function in $S$, and $x$ any element in $X$. We then have

$$(e \circ f)(x) = e(f(x)) = f(x), \quad (f \circ e)(x) = f(e(x)) = f(x).$$

Hence $(e \circ f)(x) = (f \circ e)(x)$ for all $f \in S$ and $x \in X$, so $e \circ f = f \circ e$ for all $f \in S$. Hence and as required.

Having proven associativity of composition, and the existence of an identity element, we conclude that $S$ is a monoid.

**Problem 2.** Suppose $(F, +, \cdot)$ is a field. Show that $x, y \in F$ and $x \cdot y = 0$ imply that either $x = 0$ or $y = 0$.

**Solution.** First, we will need the fact that for any $a \in F$, we have $a \cdot 0 = 0$. You have seen this already, but I'll prove it again here to make sure: we have

$$\begin{aligned} a \cdot 0 &= a \cdot (0 + 0) && \text{(since 0 is the additive identity)} \\ &= a \cdot 0 + a \cdot 0 && \text{(by the distributive law)} \\ \implies 0 &= a \cdot 0 && \text{(adding the additive inverse of } a \cdot 0 \text{ to both sides)} \end{aligned}$$

so $a \cdot 0 = 0$ as required.

Now suppose that we have $x, y \in F$ with $x \cdot y = 0$; we want to show that $x = 0$ or $y = 0$. Suppose therefore that $x \neq 0$; we now have to show that this forces $y = 0$. Since $x \neq 0$, $x$ has a multiplicative inverse $x^{-1}$. Multiplying both sides of the equation $x \cdot y = 0$ by $x^{-1}$ on the left, we have

$$\begin{aligned}
& x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0 \\
\implies & (x^{-1} \cdot x) \cdot y = 0 && \text{(associativity of multiplication, also } a \cdot 0 = 0 \text{ for all } a \in F) \\
\implies & 1 \cdot y = 0 && \text{(by definition of the multiplicative inverse } x^{-1}) \\
\implies & y = 0 && \text{(since 1 is the multiplicative identity.)}
\end{aligned}$$

Hence $y = 0$ as required.

**Problem 3.** Let $F$ be the subset of $\mathbb{R}$ given by numbers of the form

$$\{a + b\sqrt{2} : a, b \in \mathbb{Q}\},$$

and define $+$ and $\cdot$ to be the usual operations inherited from $\mathbb{R}$.

(a) Show that for $x, y \in F$, one has $x + y$, $x\dot{y} \in F$.

(b) Show that $(F, +, \cdot)$ is a field.

**Solution.** (a) Let $x, y$ be elements of $F$, so we have $x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$ for some $a, b, c, d \in \mathbb{Q}$. We then compute

$$\begin{aligned}
x + y &= (a + b\sqrt{2}) + (c + d\sqrt{2}) \\
&= (a + c) + (b\sqrt{2} + d\sqrt{2}) \\
&\qquad \text{(using associativity and commutativity of addition in the field } \mathbb{R}) \\
&= (a + c) + (b + d)\sqrt{2} && \text{(using distribution in } \mathbb{R}.)
\end{aligned}$$

Since $\mathbb{Q}$ is a field, we have $a + c \in Q$ and $b + d \in Q$, so this is an element of $F$. Similarly for multiplication, we have

$$\begin{aligned}
x \cdot y &= (a + b\sqrt{2})(c + d\sqrt{2}) \\
&= ac + ad\sqrt{2} + bc\sqrt{2} + bd\sqrt{2}\sqrt{2} && \text{(using distribution in } \mathbb{R}) \\
&= (ac + 2bd) + (ad + bc)\sqrt{2} && \text{(using } \sqrt{2}^2 = 2 \text{, distribution in } \mathbb{R}.)
\end{aligned}$$

Again, since $\mathbb{Q}$ is a field, we have $ac + 2bd \in \mathbb{Q}$ and $ad + bc \in Q$, so this is an element of $F$.

(b) Part (a) shows us that $F$ is closed under addition and multiplication; in addition, 0 and 1 are elements of $F$, since we can take $a = 0, b = 0$ for the former and $a = 1, b = 0$ for the latter in the definition of $F$. Since $F$ is a subset of $\mathbb{R}$ with the same addition and multiplication, $F$ inherits the associativity, commutativity, and identity axioms for both addition and multiplication, as well as the distribution axioms. It remains to prove the inverse axioms in $F$.

Let $x = a + b\sqrt{2}$ be any element of $F$. Since $a, b \in \mathbb{Q}$ and $\mathbb{Q}$ is a field, we also have $-a, -b \in \mathbb{Q}$, so $y = -a - b\sqrt{2} \in F$. We also have

$$x + y = (a + b\sqrt{2}) + (-a - b\sqrt{2}) = (a - a) + (b - b)\sqrt{2} = 0,$$

using axioms from $\mathbb{R}$. Hence every element $x \in F$ has an additive inverse.

Now suppose that $x \neq 0$, so $x = a + b\sqrt{2}$ where $a$ and $b$ are not both 0. As many of you may have seen, for the inverse $x^{-1} = \frac{1}{a+b\sqrt{2}}$ that we want, we can rationalize the denominator to get the expression

$$\frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}.$$

We need to show that this is an element of $F$, i.e. that the expressions $\frac{a}{a^2-2b^2}$ and $\frac{-b}{a^2-2b^2}$ are rational. Both numerators and denominators are rational, so these are rational numbers so long as the denominator is nonzero, so we'll need to prove that $a^2 - 2b^2 \neq 0$.

We can show that in two different ways. First method: if $x = a + b\sqrt{2}$ is nonzero, then $a, b$ are nonzero, so $a - b\sqrt{2}$ is also nonzero. We have two nonzero elements in the field $\mathbb{R}$, and we know from problem 2 that the product of two nonzero elements in a field is nonzero, so $a^2 - 2b^2 \neq 0$. Alternatively, suppose $a^2 - 2b^2 = 0$. If $b = 0$, we then have $a^2 = 0$, so $a = 0$ by Problem 2, but this gives $x = 0$, which is false. If $b \neq 0$, we can divide by $b$ to get $2 = a^2/b^2$, but 2 is not the square of a rational number, by Problem 1, so this is also impossible. Hence $a^2 - 2b^2 \neq 0$ for all $a, b \in \mathbb{Q}$ not both 0. Either way, we find that $\frac{a}{a^2-2b^2} \in \mathbb{Q}$ and $\frac{-b}{a^2-2b^2} \in \mathbb{Q}$. Multiplying this by $x$ gives

$$(a + b\sqrt{2})\left(\frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}\right) = \frac{(a + b\sqrt{2})(a - b\sqrt{2})}{a^2 - 2b^2} = \frac{a^2 - 2b^2}{a^2 - 2b^2} = 1,$$

as required. Hence if $x \neq 0$, it has a multiplicative inverse in $F$, and this completes the proof.

**Problem 4.** Show that if $n \geq 2$ is an integer then $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with a unit. (You may use that $(\mathbb{Z}/n\mathbb{Z}, +)$ is a commutative group, as shown in class.)

**Solution.** We already know that $(\mathbb{Z}/n\mathbb{Z}, +)$ is a commutative group, so it remains to show that $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ is a commutative monoid, and that distributivity holds. First, we define multiplication (as you might expect) by $[a][b] = [ab]$; we need to show that this is well-defined, that it obeys associativity and commutativity, that there is an identity element, and that it is distributive.

- Well-defined: suppose we have integers $a$, $a'$, $b$, and $b'$ such that $[a] = [a']$ and $[b] = [b']$; we need to show that $[a][b] = [a'][b']$, so that it does not matter which integer we choose in a particular equivalence class. By definition, since $[a] = [a']$, we have $a - a' = pn$ for some integer $p$, and similarly $b - b' = qn$ for some integer $q$. Using the distribution law in $\mathbb{Z}$, we have

  $$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b' = aqn + pnb' = n(aq + pb'),$$

  so that $[a][b] = [a'][b']$, by definition. Hence multiplication is well defined.

- Associativity: let $[a], [b], [c]$ be elements of $\mathbb{Z}/n\mathbb{Z}$. We have

  $$\begin{aligned} ([a][b])\,[c] &= [ab][c] && \text{(by definition of multiplication in } \mathbb{Z}/n\mathbb{Z}) \\ &= [(ab)c] && \text{(definition of multiplication in } \mathbb{Z}/n\mathbb{Z}) \\ &= [a(bc)] && \text{(associativity of multiplication in } \mathbb{Z}) \\ &= [a][bc] && \text{(definition of multiplication in } \mathbb{Z}/n\mathbb{Z}) \\ &= [a]\,([b][c]) && \text{(definition of multiplication in } \mathbb{Z}/n\mathbb{Z}.) \end{aligned}$$

  So multiplication is associative.

- Commutativity: let $[a], [b]$ be elements of $\mathbb{Z}/n\mathbb{Z}$. We have

  $$\begin{aligned} [a][b] &= [ab] && \text{(multiplication in } \mathbb{Z}/n\mathbb{Z}) \\ &= [ba] && \text{(commutative of multiplication in } \mathbb{Z}/n\mathbb{Z}) \\ &= [b][a] && \text{(multiplication in } \mathbb{Z}/n\mathbb{Z}.) \end{aligned}$$

  So multiplication is associative.

- Identity: let $[a]$ be an element of $\mathbb{Z}/n\mathbb{Z}$. We have

  $$\begin{aligned} [1][a] &= [1a] && \text{(multiplication in } \mathbb{Z}/n\mathbb{Z}) \\ &= [a] && \text{(identity in } \mathbb{Z}.) \end{aligned}$$

  By commutativity, we also have $[a][1] = [a]$. Hence multiplication has an identity (or unit), $[1]$.

- Distributivity: let $[a], [b], [c]$ be elements of $\mathbb{Z}/n\mathbb{Z}$. We have

  $$\begin{aligned} [a]\,([b] + [c]) &= [a][b + c] && \text{(addition in } \mathbb{Z}/n\mathbb{Z}) \\ &= [a(b + c)] && \text{(multiplication in } \mathbb{Z}/n\mathbb{Z}) \\ &= [ab + ac] && \text{(distribution in } \mathbb{Z}) \\ &= [ab] + [ac] && \text{(addition in } \mathbb{Z}/n\mathbb{Z}) \\ &= [a][b] + [a][c] && \text{(multiplication in } \mathbb{Z}/n\mathbb{Z}.) \end{aligned}$$

  By commutativity, we also have $([b] + [c])[a] = [b][a] + [c][a]$. Hence the distributive properties hold.

Hence $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a commutative ring with unit.

**Problem 5.** Assuming all properties but that non-zero elements have multiplicative inverses (i.e. assuming that $\mathbb{Z}/p\mathbb{Z}$ is a commutative ring with a unit), as you may by Problem 4, show that $\mathbb{Z}/p\mathbb{Z}$ is a field when $p$ is a prime.

(Hint:Let $a \in \{1, \dots, p-1\}$. Show that it suffices to find $b \in \mathbb{Z}$ such that $ab - 1 \in p\mathbb{Z}$. On the other hand, to prove this, consider the $p-1$ integers, $1 \cdot a, 2 \cdot a, \dots, (p-1)a$. Note that none of these is a multiple of $p$ (since $p$ is a prime, and $1 \leq a \leq p-1$), so none of these lies in $[0]$, the equivalence class of 0 modulo $p$ (a.k.a. none of them is a multiple of $p$). Since there are exactly $p-1$ non-zero equivalence classes modulo $p$, there are two cases: either no two of these $p-1$ numbers lies in the same class (i.e. they all lie in different classes), or two lie in the same class, i.e. for some $b, c \in \{1, \dots, p-1\}$, $b \neq c$, $ba - ca$ is a multiple of $p$. Show that the latter cannot happen.)

**Solution.** As noted in the question, problem 4 already tells us that $\mathbb{Z}/p\mathbb{Z}$ is a commutative ring with unit, so the only property of a field that remains to be proven is the existence of multiplicative inverses for all nonzero elements. Let $[a]$ be a nonzero element of $\mathbb{Z}/p\mathbb{Z}$; we can assume without loss of generality that $a \in \{1, \dots, p-1\}$ since every equivalence class has an integer between 0 and $p-1$, and $[a] \neq [0]$. We want to find $[b]$ such that $[a][b] = 1$; again we may assume that $b \in \{1, \dots, p-1\}$ since the inverse of $[a]$ cannot of $[0]$. By definition, $[a][b] = [1]$ if and only if $ab - 1$ is divisible by $p$, so we have reduced the problem to finding $b \in \{1, \dots, p-1\}$ such that $ab - 1 \in p\mathbb{Z}$. If we consider all possible values of $ab$ for $b \in \{1, \dots, p-1\}$, we have the list of integers $a, 2a, \dots, (p-1)a$. Since each of these is the product of two integers less than $p$, and $p$ is prime, none of these are divisible by $p$, and so must be in one of the equivalence classes $[1], [2], \dots, [p-1]$. We have a list of $p-1$ integers that must all be in one of $p-1$ equivalence classes, so either each is in a different equivalence class, or two distinct integers in the list are in the same equivalence class. Suppose we have two elements in the list, $ab$ and $ac$, that are in the same equivalence class. By definition, this means that $ab - ac \in p\mathbb{Z}$, so that $a(b-c)$ is divisible by $p$. But $a, b, c \in \{1, \dots, p-1\}$, so $a(b-c)$ is not divisible by $p$ unless $b - c = 0$. Hence $ab = ac$, which means that distinct integers in the list must be in different equivalence classes. Since there are $p-1$ integers and $p-1$ equivalence classes, there must be some $b \in \{1, \dots, p-1\}$ such that $ab$ is in $[1]$, i.e. $ab - 1 \in p\mathbb{Z}$, which is what we needed to prove. Hence $[a]$ has an inverse and $\mathbb{Z}/p\mathbb{Z}$ is a field, as required.