Exam #1 Solutions

Monday, October 16 2017

Problem 1.

In order to show that $(U_n, \times)$ is a monoid, we need to show that:

- $\times$ is a binary operation on the set U_n.
- The binary operation $\times$ on the set U_n is associative.
- The binary operation $\times$ on the set U_n admits an identity element.

First of all, we can observe that $\times$ is well-defined as a binary operationon U_n: it is the induced binary operation from the multiplication in $\mathbb{C}$, and U_n is closed under complex multiplication. Indeed, for any z_1 and z_2 in U_n, the product $z_1 z_2$ still belongs to U_n, since $(z_1 z_2)^n = (z_1)^n (z_2)^n = 1$. In other words, $(U_n, \times)$ is a submagma of $(\mathbb{C}, \times)$.

The fact that $\times$ is associative as a binary operation on U_n is an immediate consequence of the fact that $\times$ is associative as a binary operation on $\mathbb{C}$: The identity $z_1 \times (z_2 \times z_3) = (z_1 \times z_2) \times z_3$ holds for any z_1, z_2 and z_3 in U_n, since it holds for any z_1, z_2 and z_3 in $\mathbb{C}$.

The fact that $\times$ admits an identity element as a binary operation on U_n is a consequence of the fact that $\times$ admits an identity element as a binary operation on $\mathbb{C}$, namely $1 \in \mathbb{C}$, and the fact that this identity element is in U_n ($1 \in U_n$ since $1^n = 1$). Indeed, the identity $1 \times z = z \times 1 = z$ holds for any $z \in U_n$, since it holds for any $z \in \mathbb{C}$.

Thus we have indeed proved that $(U_n, \times)$ is a monoid. Note that the proof that we wrote can easily be adapted to prove the following more general fact: Any submagma of a monoid is a monoid if it contains the identity element.

It remains to discuss whether every element of $(U_n, \times)$ has an inverse. We know that every element of $z \in U_n$ has an inverse in $\mathbb{C}$, namely $\frac{1}{z}$ (note that z cannot be zero, because 0 is not an element of U_n). If we can show that $\frac{1}{z} \in U_n$, we win: it will be the inverse of z in $(U_n, \times)$, since $z \times \frac{1}{z} = \frac{1}{z} \times z = 1$. But it is easy to argue that $\frac{1}{z} \in U_n$, indeed: $\left(\frac{1}{z}\right)^n = \frac{1}{z^n} = \frac{1}{1} = 1$, therefore $\frac{1}{z} \in U_n$. Note that we have showed (very carefully) in this problem that $(U_n, \times)$ is a group.

Problem 2.

Let us prove that K is closed in $(M, \otimes)$. By definition, we want to show that for every $(x, y) \in M^2$, if $x \in K$ and $y \in K$ then $x \otimes y \in K$.

So, let x and y be any two elements of K. We want to show that $x \otimes y \in K$, that is, we want to show that $f(x \otimes y) = e_N$.

Since f is a homomorphism from $(M, \otimes)$ to $(N, \diamond)$, we know that $f(x \otimes y) = f(x) \diamond f(y)$.

Furthermore, since $x \in K$ and $y \in K$, $f(x) = e_N$ and $f(y) = e_N$ (by definition of K).

Therefore, $f(x \otimes y) = e_N \diamond e_N$.

Now, since e_N is the identity element of N, $e_N \diamond e_N = e_N$.

Conclusion: $f(x \otimes y) = e_N$, as we wanted.

Problem 3.

(1) If x is idempotent and invertible, then $x * x = x$, and there exists $y \in M$ such that $x * y = y * x = e$. In order to show that $x = e$, let us compute $(y * x) * x$. On the one hand, this is $(y * x) * x = e * x = x$. On the other hand, by associativity (we are in a monoid), $(y * x) * x = y * (x * x) = y * x = e$. Therefore, identifying the two results, we can conclude that $x = e$.

Conversely, it is quick to check that if $x = e$, then x is idempotent (because $e * e = e$) and x is invertible (e is invertible: its inverse is e).

(2) In the monoid $(\mathcal{M}_n(\mathbb{R}), \times)$, saying that $M^2 = M$ and $\det(M) \neq 0$ amounts to saying, respectively, that M is idempotent and M is invertible. Therefore, we can derive from the previous question that M must be the identity element of $(\mathcal{M}_n(\mathbb{R}), \times)$, that is to say:

$$M = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{bmatrix} .$$

(3) Let $M = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$. Let us compute M^2:

$$\begin{aligned} M^2 &= M \times M \\ &= \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} \times \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} \\ &= \begin{bmatrix} 1/4 + 1/4 & 1/4 + 1/4 \\ 1/4 + 1/4 & 1/4 + 1/4 \end{bmatrix} \\ &= \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} \end{aligned}$$

Thus we find $M^2 = M$. As for the determinant:

$$\begin{aligned} \det(M) &= 1/2 \times 1/2 - 1/2 \times 1/2 \\ &= 0 . \end{aligned}$$

What we just computed shows that M is idempotent and not invertible. This is consistent with our previous answers: if M was invertible, it would have to be equal to the identity matrix according to the previous answer, however that is not the case.

Problem 4.

(1) We need to check that for every $(z_1, z_2) \in \mathbb{C}$, $f(z_1 + z_2) = f(z_1) + f(z_2)$. Let's go: denoting $z_1 = a_1 + ib_1$ and $z_2 = a_2 + ib_2$, we have:

$$\begin{aligned} f(z_1 + z_2) &= f((a_1 + ib_1) + (a_2 + ib_2)) \\ &= f((a_1 + a_2) + i(b_1 + b_2)) \\ &= \begin{bmatrix} a_1 + a_2 & -(b_1 + b_2) \\ b_1 + b_2 & a_1 + a_2 \end{bmatrix}. \end{aligned}$$

On the other hand,

$$\begin{aligned} f(z_1) + f(z_2) &= f(a_1 + ib_1) + f(a_2 + ib_2) \\ &= \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} + \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix} \\ &= \begin{bmatrix} a_1 + a_2 & -b_1 + (-b_2) \\ b_1 + b_2 & a_1 + a_2 \end{bmatrix} \\ &= \begin{bmatrix} a_1 + a_2 & -(b_1 + b_2) \\ b_1 + b_2 & a_1 + a_2 \end{bmatrix} \end{aligned}$$

Thus we indeed find that $f(z_1 + z_2) = f(z_1) + f(z_2)$.

(2) We need to check that for every $(z_1, z_2) \in \mathbb{C}$, $f(z_1 \times z_2) = f(z_1) \times f(z_2)$. Let's go: denoting $z_1 = a_1 + ib_1$ and $z_2 = a_2 + ib_2$, we have:

$$\begin{aligned} f(z_1 \times z_2) &= f((a_1 + ib_1) \times (a_2 + ib_2)) \\ &= f((a_1a_2 - b_1b_2) + i(a_1b_2 + a_2b_1)) \\ &= \begin{bmatrix} a_1a_2 - b_1b_2 & -(a_1b_2 + a_2b_1) \\ a_1b_2 + a_2b_1 & a_1a_2 - b_1b_2 \end{bmatrix}. \end{aligned}$$

On the other hand,

$$\begin{aligned} f(z_1) \times f(z_2) &= f(a_1 + ib_1) \times f(a_2 + ib_2) \\ &= \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} \times \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix} \\ &= \begin{bmatrix} a_1a_2 - b_1b_2 & -a_1b_2 - b_1a_2 \\ b_1 + b_2 & a_1 + a_2 \end{bmatrix} \\ &= \begin{bmatrix} a_1 + a_2 & -(b_1 + b_2) \\ a_2b_1 + a_1b_2 & -b_1b_2 + a_1a_2 \end{bmatrix} \\ &= \begin{bmatrix} a_1a_2 - b_1b_2 & -(a_1b_2 + a_2b_1) \\ a_1b_2 + a_2b_1 & a_1a_2 - b_1b_2 \end{bmatrix}. \end{aligned}$$

Thus we indeed find that $f(z_1 \times z_2) = f(z_1) \times f(z_2)$.

(3) In order to show that f is injective, we show that for any $(z_1, z_2) \in \mathbb{C}^2$, if $f(z_1) = f(z_2)$ then $z_1 = z_2$. So let z_1 and z_2 be any two complex numbers, assume that $f(z_1) = f(z_2)$. Let us write $z_1 = a_1 + ib_1$ and $z_2 = a_2 + ib_2$ (algebraic form). Then the identity $f(z_1) = f(z_2)$ is rewritten:

$$\begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} = \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix}.$$

Now, we know that two matrices are equal when they have the same coefficients in the same places. Therefore, we derive from the equality of the two matrices above that $a_1 = a_2$ and $b_1 = b_2$. This implies that $z_1 = z_2$, which is what we wanted.

(4) We see from the definition of f that, if a matrix $M = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ is in the image of f, then $a_1 1 = a_2 2$ and $a_{21} = -a_{12}$. Not all matrices satisfy this: for instance, the matrix $M = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ is not in the image of f. This shows that f is not sujective.

(5) *Note: there was a typo in the exam: it should have read "[. . .] is an isomorphism from* $(\mathbb{C}, +)$ *to* $(C, +)$ *and from* $(\mathbb{C}, \times)$ *to* $(C, \times)$.

Note that the map $\tilde{f}$ is the same map as f, with the difference that its codomain has been adjusted to match its range. Therefore, the exact same computations as in the previous answers show that $\tilde{f}$ is still a homomorphism from $(\mathbb{C}, +)$ to $(C, +)$ and from $(\mathbb{C}, \times)$ to $(C, \times)$. Furthermore, the same computations show that $\tilde{f}$ is still injective. But $\tilde{f}$ is now surjective as well, since its codomain is equal to its range. Therefore, $\tilde{f}$ is a bijective homomorphism, which shows that it is a isomorphism, both from $(\mathbb{C}, +)$ to $(C, +)$ and from $(\mathbb{C}, \times)$ to $(C, \times)$.