THE UNIVERSITY OF SYDNEY

MATH2022 LINEAR AND ABSTRACT ALGEBRA

Semester 1 **Week 2 Longer Solutions**

1. (a) $2A = \begin{bmatrix} 2 & 4 \\ 0 & 6 \end{bmatrix}$ in each case.

(b) $-B = \begin{bmatrix} 6 & -3 \\ -4 & -1 \end{bmatrix}$ over $\mathbb{R}$, $\begin{bmatrix} 6 & 4 \\ 3 & 6 \end{bmatrix}$ over $\mathbb{Z}_7$, and $\begin{bmatrix} 6 & 10 \\ 9 & 12 \end{bmatrix}$ over $\mathbb{Z}_{13}$.

(c) $A + B = \begin{bmatrix} -5 & 5 \\ 4 & 4 \end{bmatrix}$ over $\mathbb{R}$, $\begin{bmatrix} 2 & 5 \\ 4 & 4 \end{bmatrix}$ over $\mathbb{Z}_7$, and $\begin{bmatrix} 8 & 5 \\ 4 & 4 \end{bmatrix}$ over $\mathbb{Z}_{13}$.

(d) $A - B = \begin{bmatrix} 7 & -1 \\ -4 & 2 \end{bmatrix}$ over $\mathbb{R}$, $\begin{bmatrix} 0 & 6 \\ 3 & 2 \end{bmatrix}$ over $\mathbb{Z}_7$, and $\begin{bmatrix} 7 & 12 \\ 9 & 2 \end{bmatrix}$ over $\mathbb{Z}_{13}$.

(e) $A^2 = \begin{bmatrix} 1 & 8 \\ 0 & 9 \end{bmatrix}$ over $\mathbb{R}$ and $\mathbb{Z}_{13}$, and $\begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}$ over $\mathbb{Z}_7$.

(f) $AB = \begin{bmatrix} 2 & 5 \\ 12 & 3 \end{bmatrix}$ over $\mathbb{R}$ and $\mathbb{Z}_{13}$, and $\begin{bmatrix} 2 & 5 \\ 5 & 3 \end{bmatrix}$ over $\mathbb{Z}_7$.

(g) $BA = \begin{bmatrix} -6 & -3 \\ 4 & 11 \end{bmatrix}$ over $\mathbb{R}$, $\begin{bmatrix} 1 & 4 \\ 4 & 4 \end{bmatrix}$ over $\mathbb{Z}_7$, and $\begin{bmatrix} 7 & 10 \\ 4 & 11 \end{bmatrix}$ over $\mathbb{Z}_{13}$.

(h) $CD = \begin{bmatrix} -3 \end{bmatrix} = -3$ over $\mathbb{R}$, $\begin{bmatrix} 4 \end{bmatrix} = 4$ over $\mathbb{Z}_7$, and $\begin{bmatrix} 10 \end{bmatrix} = 10$ over $\mathbb{Z}_{13}$.

(i) $EF - 3D = \begin{bmatrix} -13 \\ -6 \\ -1 \end{bmatrix}$ over $\mathbb{R}$, $\begin{bmatrix} 1 \\ 1 \\ 6 \end{bmatrix}$ over $\mathbb{Z}_7$, and $\begin{bmatrix} 0 \\ 7 \\ 12 \end{bmatrix}$ over $\mathbb{Z}_{13}$.

(j) $CEF = \begin{bmatrix} -64 \end{bmatrix} = -64$ over $\mathbb{R}$, $\begin{bmatrix} 6 \end{bmatrix} = 6$ over $\mathbb{Z}_7$, and $\begin{bmatrix} 1 \end{bmatrix} = 1$ over $\mathbb{Z}_{13}$.

2. Let A be $p \times q$ and B be $r \times s$ and suppose that $AB = BA = I_n$. Since $AB = I_n$ is $n \times n$ and the product is defined, we have $q = r$ and $p = s = n$. Also, since $BA = I_n$ is $n \times n$, we have $s = p$ and $r = q = n$. Thus $p = q = r = s = n$, so that A and B are both $n \times n$ square matrices.

3. Observe that

$$AB = \frac{1}{ad-bc}\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{ad-bc}\begin{bmatrix} ad-bc & -ab+ba \\ cd-dc & -cb+da \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

and

$$BA = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \frac{1}{ad-bc}\begin{bmatrix} da-bc & db-bd \\ -ca+ac & -cb+ad \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Over $\mathbb{Z}_2$, since $ad - bc = 1$ (the only nonzero element of $\mathbb{Z}_2$) and $1 = -1$, we get

$$A^{-1} = \begin{bmatrix} d & b \\ c & a \end{bmatrix}.$$

4. (a) Using the formula from the previous question,

$$T_\theta^{-1} \;=\; \frac{1}{-\cos^2\theta - \sin^2\theta} \begin{bmatrix} -\cos\theta & -\sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \;=\; \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \;=\; T_\theta\ .$$

(b) Using trig identities, we get

$$\begin{aligned} R_\theta R_\phi \;&=\; \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{bmatrix} \\ &=\; \begin{bmatrix} \cos\theta\cos\phi - \sin\theta\sin\phi & -\cos\theta\sin\phi - \sin\theta\cos\phi \\ \sin\theta\cos\phi + \cos\theta\sin\phi & -\sin\theta\sin\phi + \cos\theta\cos\phi \end{bmatrix} \\ &=\; \begin{bmatrix} \cos(\theta+\phi) & -\sin(\theta+\phi) \\ \sin(\theta+\phi) & \cos(\theta+\phi) \end{bmatrix} \;=\; R_{\theta+\phi}\ . \end{aligned}$$

(c) Observe first that

$$R_{2\pi} \;=\; \begin{bmatrix} \cos 2\pi & -\sin 2\pi \\ \sin 2\pi & \cos 2\pi \end{bmatrix} \;=\; \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \;=\; I\ .$$

Observe next, by iterating the result in (b), for any angle θ and positive integer n,

$$R_\theta^n \;=\; R_\theta R_\theta \ldots R_\theta \;=\; R_{\theta+\theta+\ldots+\theta} \;=\; R_{n\theta}\ .$$

In particular, $R_{2\pi/n}^n = R_{2n\pi/n} = R_{2\pi} = I$.

(d) Using trig identities, we get

$$\begin{aligned} T_\theta T_\phi \;&=\; \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \begin{bmatrix} \cos\phi & \sin\phi \\ \sin\phi & -\cos\phi \end{bmatrix} \\ &=\; \begin{bmatrix} \cos\theta\cos\phi + \sin\theta\sin\phi & \cos\theta\sin\phi - \sin\theta\cos\phi \\ \sin\theta\cos\phi - \cos\theta\sin\phi & \sin\theta\sin\phi + \cos\theta\cos\phi \end{bmatrix} \\ &=\; \begin{bmatrix} \cos(\theta-\phi) & -\sin(\theta-\phi) \\ \sin(\theta-\phi) & \cos(\theta-\phi) \end{bmatrix} \;=\; R_{\theta-\phi}\ . \end{aligned}$$

(e) Using the formula from the previous question, and the facts that cos is an even function and sin is an odd function, we get

$$R_\theta^{-1} \;=\; \frac{1}{\cos^2\theta + \sin^2\theta} \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \;=\; \begin{bmatrix} \cos(-\theta) & -\sin(-\theta) \\ \sin(-\theta) & \cos(-\theta) \end{bmatrix} \;=\; R_{-\theta}\ .$$

We also have, noting cancellations at the third step,

$$\begin{aligned} T_\phi R_\theta T_\phi \;&=\; \begin{bmatrix} \cos\phi & \sin\phi \\ \sin\phi & -\cos\phi \end{bmatrix} \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} \cos\phi & \sin\phi \\ \sin\phi & -\cos\phi \end{bmatrix} \\ &=\; \begin{bmatrix} \cos\phi\cos\theta + \sin\phi\sin\theta & -\cos\phi\sin\theta + \sin\phi\cos\theta \\ \sin\phi\cos\theta - \cos\phi\sin\theta & -\sin\phi\sin\theta - \cos\phi\cos\theta \end{bmatrix} \begin{bmatrix} \cos\phi & \sin\phi \\ \sin\phi & -\cos\phi \end{bmatrix} \\ &=\; \begin{bmatrix} \cos^2\phi\cos\theta + \sin^2\phi\cos\theta & \sin^2\phi\sin\theta + \cos^2\phi\sin\theta \\ -\cos^2\phi\sin\theta - \sin^2\phi\sin\theta & \sin^2\phi\cos\theta + \cos^2\phi\cos\theta \end{bmatrix} \\ &=\; \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \;=\; R_{-\theta}\ . \end{aligned}$$

5. Working mod 7, we have

$$100^{100} \;=\; 2^{100} \;=\; (2^3)^{33}(2) \;=\; 1^{33}(2) \;=\; 2\ ,$$

so the day will be two days after Monday, which is Wednesday.

6. Working mod 24, first note that $16^2 = (-8)^2 = 64 = -8 = 16$, so that 16 coincides with all of its positive powers, and we therefore have

$$100^{100} \;=\; 4^{100} \;=\; (4^2)^{50} \;=\; 16^{50} \;=\; 16\ ,$$

so the time will be 16 hours after 9 am, that is 1 am the following day. Furthermore, $100^{100} - 16$ hours is a multiple of 24, so the ratio is the number of days, which, working mod 7, and using the result of the previous exercise, gives

$$\frac{100^{100}-16}{24} \;=\; \frac{2-2}{3} \;=\; 0\ .$$

Hence the meteor strike will occur 16 hours after 9 am on some Monday, which will be 1 am on Tuesday.

7. (a) We have

$$M^2 \;=\; \begin{bmatrix} 3 & -1 \\ 4 & -1 \end{bmatrix}\begin{bmatrix} 3 & -1 \\ 4 & -1 \end{bmatrix} \;=\; \begin{bmatrix} 5 & -2 \\ 8 & -3 \end{bmatrix} \;=\; \begin{bmatrix} 6 & -2 \\ 8 & -2 \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \;=\; 2M - I\ .$$

(b) Using part (a), we have

$$M^3 \;=\; M(M^2) \;=\; M(2M-I) \;=\; 2M^2 - M \;=\; 2(2M-I) - M \;=\; 3M - 2I\ .$$

From this pattern, we may conjecture that, for any positive integer n,

$$M^n \;=\; nM - (n-1)I\ .$$

This holds for $n = 2, 3$ by what we have just shown, and it clearly holds also for $n = 1$. Suppose this formula holds for $n = k$, We show that it holds for $n = k+1$:

$$\begin{aligned} M^{k+1} &\;=\; M^k M \;=\; (kM - (k-1)I)M \;=\; kM^2 - (k-1)M \\ &\;=\; k(2M - I) - (k-1)M \;=\; (2k - k + 1)M - kI \\ &\;=\; (k+1)M - kI\ , \end{aligned}$$

which establishes the inductive step, and proves the result for all positive integers n. Note that, by convention,

$$M^0 \;=\; I \;=\; 0M - (0-1)I\ ,$$

so the formula also holds for $n = 0$. Further, for any positive integer n, we have

$$\begin{aligned} M^n &\;=\; nM - (n-1)I \;=\; \begin{bmatrix} 3n & -n \\ 4n & -n \end{bmatrix} + \begin{bmatrix} 1-n & 0 \\ 0 & 1-n \end{bmatrix} \\ &\;=\; \begin{bmatrix} 2n+1 & -n \\ 4n & -2n+1 \end{bmatrix}, \end{aligned}$$

so that, if we put $m = -n$, then

$$\begin{aligned} M^m \;=\; M^{-n} &= \frac{1}{(2n+1)(-2n+1)+4n^2}\begin{bmatrix} -2n+1 & n \\ -4n & 2n+1 \end{bmatrix} \\ &= \begin{bmatrix} -3n & n \\ -4n & n \end{bmatrix} + \begin{bmatrix} n+1 & 0 \\ 0 & n+1 \end{bmatrix} \\ &= (-n)M + (n+1)I \\ &= mM - (m-1)I\,, \end{aligned}$$

which verifies the formula also for negative powers.

(c) Using our formula, we have

$$M^5 \;=\; 5M - 4I \;=\; \begin{bmatrix} 11 & -5 \\ 20 & -9 \end{bmatrix}, \qquad M^{10} \;=\; 10M - 9I \;=\; \begin{bmatrix} 21 & -10 \\ 40 & -19 \end{bmatrix},$$

$$M^{100} \;=\; 100M - 99I \;=\; \begin{bmatrix} 201 & -100 \\ 400 & -199 \end{bmatrix}, \quad M^{-100} = \left(M^{100}\right)^{-1} = \begin{bmatrix} -199 & 100 \\ -400 & 201 \end{bmatrix}.$$

8. Observe that in $\mathbb{Z}_7$ we have $2(4) = 3(5) = 4(2) = 1$, $5(2) = 3$ and $6(2) = 5$, so that

$$\frac{1}{2} = 4\,, \quad \frac{1}{3} = 5\,, \quad \frac{1}{4} = 2\,, \quad \frac{3}{5} = 2\,, \quad \frac{5}{6} = 2\,.$$

In $\mathbb{Z}_8$ we have $3(3) = 1$ and $5(7) = 3$, so that

$$\frac{1}{3} = 3\,, \quad \frac{3}{5} = 7\,.$$

However, in $\mathbb{Z}_8$, none of the other fractions can exist because the denominators are divisible by 2, so multiplying them by any element of $\mathbb{Z}_8$ will always produce another element divisible by 2, so can never produce a numerator 1, 3 or 5.

In $\mathbb{Z}_9$ we have $2(5) = 4(7) = 1$ and $5(6) = 3$, so that

$$\frac{1}{2} = 5\,, \quad \frac{1}{4} = 7\,, \quad \frac{3}{5} = 6\,.$$

However, in $\mathbb{Z}_9$, the other two fractions cannot exist because the denominators are divisible by 3, so multiplying them by any element of $\mathbb{Z}_9$ will always produce another element divisible by 3, so can never produce a numerator 1 or 5.

In $\mathbb{Z}_{24}$ we have $5(15) = 3$, so $\frac{3}{5} = 15$. None of the other fractions can exist, because their denominators are divisible by 2 or 3, so multiplying by any element of $\mathbb{Z}_{24}$ will produce another element divisible by 2 or 3, so can never produce a numerator 1 or 5.

9. If M is a square matrix then $M(M^2) = M(MM) = (MM)M = (M^2)M$, by associativity, so that M commutes with its square.

10. Put $M = \begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix}$. All of the entries of M are nonzero, since $\pm 1 \neq 0$ in any field, yet

$$M^2 \;=\; \begin{bmatrix} 1-1 & 1-1 \\ -1+1 & -1+1 \end{bmatrix} \;=\; \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},$$

the zero matrix.

11. Let A be a matrix with a row or column of zeros. Suppose to the contrary that A is invertible, so there exists a matrix B such that $AB = BA = I$. If A has a row of zeros then so does AB. If A has a column of zeros then so does BA. This means that I must have a row or column of zeros, which is false. Hence A is not invertible.

12. Both inversion and transposition reverse the order of multiplication. Hence, applying them in succession, we have

$$\left((AB)^{-1}\right)^T \;=\; \left(B^{-1}A^{-1}\right)^T \;=\; \left(A^{-1}\right)^T\left(B^{-1}\right)^T$$

and

$$\left((AB)^T\right)^{-1} \;=\; \left(B^TA^T\right)^{-1} \;=\; \left(A^T\right)^{-1}\left(B^T\right)^{-1} .$$

13. (a) Let $a, b \in G$. Then, by associativity and properties of e, we have

$$(ab)(b^{-1}a^{-1}) \;=\; a(bb^{-1})a^{-1} \;=\; aea^{-1} \;=\; aa^{-1} \;=\; e ,$$

and

$$(b^{-1}a^{-1})(ab) \;=\; b^{-1}(a^{-1}a)b \;=\; b^{-1}eb \;=\; b^{-1}b \;=\; e ,$$

which proves that $(ab)^{-1} = b^{-1}a^{-1}$, by uniqueness of the inverse.

(b) Suppose that $a^2 = e$ for all $a \in G$, so that $a = a^{-1}$. Let $a, b \in G$. Then

$$ab \;=\; (ab)^{-1} \;=\; b^{-1}a^{-1} \;=\; ba ,$$

which verifies that G is abelian.

(c) Suppose first that G is abelian. Let $a, b \in G$, so $ab = ba$. Hence, by associativity,

$$(ab)^2 \;=\; (ab)(ab) \;=\; a(ba)b \;=\; a(ab)b \;=\; a^2b^2 .$$

Conversely, suppose that $(ab)^2 = a^2b^2$ for all $a, b \in G$. Then, by associativity and properties of e and inverses,

$$\begin{aligned} ab \;&=\; e(ab)e \;=\; (a^{-1}a)(ab)(bb^{-1}) \;=\; a^{-1}(a^2b^2)b^{-1} \;=\; a^{-1}(ab)^2b^{-1} \\ &=\; a^{-1}(abab)b^{-1} \;=\; (a^{-1}a)(ba)(bb^{-1}) \;=\; e(ba)e \;=\; ba , \end{aligned}$$

which verifies that G is abelian.

14. Denote the identity element of G by E and, to distinguish group inversion in G from matrix inversion, denote the inverse of $A \in G$ by A', so that $AA' = A'A = E$. Suppose that at least one matrix M in G is invertible as a matrix, so the matrix inverse M^{-1} exists. It suffices to show that all matrices in G are invertible. Let $A \in G$. Then

$$I \;=\; M^{-1}M \;=\; M^{-1}(ME) \;=\; (M^{-1}M)E \;=\; IE \;=\; E \;=\; A'A ,$$

and, further,

$$I \;=\; E \;=\; AA' .$$

Hence, in fact, the matrix inverse A^{-1} exists and coincides with the group inverse A'. This completes the proof that every element of G is invertible.

15. (a) We have $0 = 0 + 0$, since 0 is an additive identity element of F. If $0'$ is any other additive identity element then

$$0 \;=\; 0 + 0' \;=\; 0' \,.$$

Similarly, the multiplicative identity element is unique, for if 1 and $1'$ are multiplicative identity elements then

$$1 \;=\; (1)(1') \;=\; 1' \,.$$

(b) Let $a \in F$. Suppose $b, c \in F$ both act as negatives of a, that is,

$$a + b \;=\; b + a \;=\; 0 \;=\; a + c \;=\; c + a \,.$$

Then, by associativity and properties of zero,

$$b \;=\; b + 0 \;=\; b + (a + c) \;=\; (b + a) + c \;=\; 0 + c \;=\; c \,.$$

This proves the negative of a is unique. Suppose now that $a \neq 0$ and both $b, c \in F$ act as multiplicative inverses of a, that is,

$$ab \;=\; ba \;=\; 1 \;=\; ac \;=\; ca \,.$$

Then, by associativity and properties of 1,

$$b \;=\; b(1) \;=\; b(ac) \;=\; (ba)c \;=\; (1)c \;=\; c \,.$$

This proves the multiplicative inverse of a is unique.

(c) Let $a \in F$. Then, by part (a) and distributivity, we have

$$0a \;=\; (0 + 0)a \;=\; 0a + 0a \,,$$

so that, by properties of zero and associativity,

$$0 \;=\; -(0a) + 0a \;=\; -(0a) + (0a + 0a) \;=\; \big(-(0a) + 0a\big) + 0a \;=\; 0 + 0a \;=\; 0a \,.$$

Note that also $0 = a0$ (immediately by commutativity of multiplication).

(d) Suppose that $a, b \in F$ and $ab = 0$. It suffices to suppose that $a \neq 0$ and show that $b = 0$. But then the multiplicative inverse a^{-1} exists, and so, by the previous exercise and properties of 1 and associativity, we have

$$0 \;=\; a^{-1}0 \;=\; a^{-1}(ab) \;=\; (a^{-1}a)b \;=\; 1b \;=\; b \,,$$

that is, $b = 0$, and we are done. In particular, $\mathbb{Z}_n$ cannot be a field if n is composite positive integer, for then $n = ab$ for some smaller positive integers a and b, so that $ab = 0$ in $\mathbb{Z}_n$, yet a and b are nonzero, which would be impossible if $\mathbb{Z}_n$ were a field.

(e) Let $a, b \in F$. Observe that, by distributivity,

$$ab + (-a)b = (a + (-a))b = 0b = 0 \qquad \text{and} \qquad ab + a(-b) = a(b + (-b)) = a0 = 0 \,,$$

so, by uniqueness of the negative, we have

$$-(ab) \;=\; (-a)b \;=\; a(-b) \,.$$

In particular,

$$(-a)(-b) = -(a(-b)) = -(-(ab)) \;=\; ab \,,$$

at the last step, again by the uniqueness of the negative.

16. Let $a, b, c \in \mathbb{Z}_n$. Denote addition in $\mathbb{Z}_n$ by $\oplus$ and multiplication by $\otimes$. We use usual symbols for addition and multiplication in $\mathbb{Z}$. We have to show

$$(a \oplus b) \oplus c \;=\; a \oplus (b \oplus c) \qquad \text{and} \qquad (a \otimes b) \otimes c \;=\; a \otimes (b \otimes c)\ .$$

We have $a \oplus b = (a+b) + kn$ for some $k \in \mathbb{Z}$ and then, for some $\ell \in \mathbb{Z}$,

$$\begin{aligned}(a \oplus b) \oplus c &= ((a \oplus b) + c) + \ell n \\ &= ((a+b) + kn) + c) + \ell n \\ &= (a+b+c) + (k+\ell)n\ .\end{aligned}$$

Similarly we have $b \oplus c = (b+c) + k'n$ for some $k' \in \mathbb{Z}$ and then, for some $\ell' \in \mathbb{Z}$,

$$\begin{aligned}a \oplus (b \oplus c) &= (a + (b \oplus c)) + \ell' n \\ &= (a + ((b+c) + k'n) + \ell' n \\ &= (a+b+c) + (k'+\ell')n\ .\end{aligned}$$

But these both lie in the set $\{0, \ldots, n-1\}$, so the difference, as an integer, cannot be a nontrivial multiple of n. Thus

$$(k+\ell)n - (k'+\ell')n \;=\; 0n \;=\; 0\ ,$$

so that $(k+\ell)n = (k'+\ell')n$. This proves $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

Similarly, we have $a \otimes b = (ab) + kn$ for some $k \in \mathbb{Z}$ and then, for some $\ell \in \mathbb{Z}$,

$$\begin{aligned}(a \otimes b) \otimes c &= ((a \otimes b)c) + \ell n \\ &= ((ab) + kn)c) + \ell n \\ &= (abc) + (kc+\ell)n\ .\end{aligned}$$

Similarly we have $b \otimes c = (bc) + k'n$ for some $k' \in \mathbb{Z}$ and then, for some $\ell' \in \mathbb{Z}$,

$$\begin{aligned}a \otimes (b \otimes c) &= (a(b \otimes c)) + \ell' n \\ &= (a((bc) + k'n) + \ell' n \\ &= (abc) + (ak'+\ell')n\end{aligned}$$

for some $\ell \in \mathbb{Z}$. But these both lie in the set $\{0, \ldots, n-1\}$, so the difference, as an integer, cannot be a nontrivial multiple of n. Thus

$$(kc+\ell)n - (ak'+\ell')n \;=\; 0n \;=\; 0\ ,$$

so that $(kc+\ell)n = (ak'+\ell')n$. This proves $(a \otimes b) \otimes c = a \otimes (b \otimes c)$.