Solutions to Assignment 2

1. Show that the formula for multiplication of matrices over a ring R follows the distributive and associative laws in R.

Solution: The rule for addition is "entry-wise": if $A+B=C$ then $C_{i,j}=A_{i,j}+B_{i,j}$. Since addition in R is commutative and associative, so is the addition of matrices.

If $A\cdot B=D$ then we have $D_{i,j}=\sum_k A_{i,k}\cdot B_{k,j}$. Now, if $D\cdot C=M$ then $M_{i,j}=\sum_k D_{i,k}\cdot C_{k,j}$. Let us put $B\cdot C=E$. We see that

$$\begin{aligned} M_{i,j} &= \sum_k \left(\sum_n A_{i,n}\cdot B_{n,k}\right)\cdot C_{k,j} \\ &= \sum_k \sum_n (A_{i,n}\cdot B_{n,k})\cdot C_{k,j} \\ &= \sum_k \sum_n A_{i,n}\cdot (B_{n,k}\cdot C_{k,j}) \\ &= \sum_n \sum_k A_{i,n}\cdot (B_{n,k}\cdot C_{k,j}) \\ &= \sum_n A_{i,n}\cdot \left(\sum_k B_{n,k}\cdot C_{k,j}\right) \end{aligned}$$

Now $E_{i,j}=\sum_k B_{i,k}\cdot C_{k,j}$, so we see that the right-hand side is $\sum_n A_{i,n}\cdot E_{n,j}$, which is the (i,j)-th entry of $A\cdot E$. This checks the associativity for multiplication. Note that we have used associativity for multiplication in R in the third step of the calculation above.

A similar calculation can be used to check the distributive law for matrices by using the distributive law in R.

2. Using the associative law show that if $x^2=r$ and $y^2=s$ and $x\cdot y=-(y\cdot x)$, then $x\cdot y)^2=-r\cdot s$.

Solution: We check

$$\begin{aligned}(x\cdot y)^2 = (x\cdot y)\cdot(x\cdot y) = x\cdot(y\cdot(x\cdot y)) = x\cdot((y\cdot x)\cdot y)\\ = x\cdot(-(x\cdot y)\cdot y) =\\ = x\cdot(((-1)\cdot(x\cdot y))\cdot y) =\\ = x\cdot((-1)\cdot((x\cdot y)\cdot y)) =\\ = (x\cdot(-1))\cdot(x\cdot(y\cdot y)) =\\ = (-1)\cdot x)\cdot(x\cdot(y\cdot y)) =\\ = (-1)\cdot(x\cdot(x\cdot(y\cdot y)) =\\ = (-1)\cdot((x\cdot x)\cdot(y\cdot y)) =\\ = (-1)\cdot x^2\cdot y^2 = -r\cdot s\end{aligned}$$

We have skipped some steps in the interests of brevity! Secondly, we have used $-x = (-1)\cdot x = x\cdot(-1)$, which is true for any ring R (Check!).

3. Consider the ring $\mathbb{H}$ consisting of pairs $(a,\vec{u})$ where a is a real number and $\vec{u}$ is a vector in 3-dimensional space. Addition is carried out component-wise and multiplication is given by:

$$(a,\vec{u})\cdot(b,\vec{v}) = (ab-\vec{u}\cdot\vec{v}, a\vec{v}+b\vec{u}+\vec{u}\times\vec{v})$$

(**Warning**: There was an error in the exercise as stated in the assignment!) where $\vec{v}\cdot\vec{w}$ is the usual dot-product and $\vec{v}\times\vec{w}$ is the usual cross-product.

Check that $\mathbb{H}$ is a ring under these operations.

Solution: First of all addition is component-wise so it is associative and commutative. Secondly, we know that the following distributive laws hold:

1. $a(\vec{v}+\vec{w}) = a\vec{v}+a\vec{w}$.
2. $(a+b)\vec{v} = a\vec{v}+b\vec{v}$
3. $\vec{v}\cdot(\vec{w}+\vec{u}) = \vec{v}\cdot\vec{w}+\vec{v}\cdot\vec{u}$ and also on the right-hand side.
4. $\vec{v}\times(\vec{w}+\vec{u}) = \vec{v}\times\vec{w}+\vec{v}\times\vec{u}$ and also on the right-hand side.

Using these, one can easily (but tediously!) check the distributive law for multiplication from left and right.

Checking the associative law for multiplication is the main task.

$$\begin{aligned}((a,\vec{u})\cdot(b,\vec{v}))\cdot(c,\vec{w}) = (ab-\vec{u}\cdot\vec{v}, a\vec{v}+b\vec{u}+\vec{u}\times\vec{v})\cdot(c,\vec{w})\\ (abc-c\vec{u}\cdot\vec{v}-(a\vec{v}+b\vec{u}+\vec{u}\times\vec{v})\cdot\vec{w},\\ ab\vec{w}+c(a\vec{v}+b\vec{u}+\vec{u}\times\vec{v})+(a\vec{v}+b\vec{u}+\vec{u}\times\vec{v})\times\vec{w})\end{aligned}$$

The first element of the tuple on the right-hand side simplifies to

$$abc - c\vec{u} \cdot \vec{v} - a\vec{v} \cdot \vec{w} - b\vec{u} \cdot \vec{w} - (\vec{u} \times \vec{v}) \cdot \vec{w}$$

We need to note that the dot-product of vectors is commutative and the identity

$$(\vec{u} \times \vec{v}) \cdot \vec{w} = \vec{u} \cdot (\vec{v}) \times \vec{w})$$

This follows from the fact that both of these give the (signed) volume of the parallelopiped with "sides" given by these three vectors. This can be used to show that the first component of the product is associative.

The second component of the product is

$$\begin{aligned} ab\vec{w} + c(a\vec{v} + b\vec{u} + \vec{u} \times \vec{v}) + (a\vec{v} + b\vec{u} + \vec{u} \times \vec{v}) \times \vec{w} = \\ ab\vec{w} + bc\vec{u} + ac\vec{v} + \\ c\vec{u} \times \vec{v} + b\vec{u} \times \vec{w} + a\vec{v} \times \vec{w} + \\ \vec{u} \times \vec{v} \times \vec{w} \end{aligned}$$

Now all the above products are associative so we will get the same answer from the right-hand side of the identity. (Check!)

4. Check that the two ways of constructing $\mathbb{H}$ via matrices and as given above result in the same ring via a natural correspondence.

Solution: Both rings contain the ring of real numbers as a subring; in the case of matrices, these are the scalar 4×4 matrices and in the above case they are elements of the form $(a, \vec{0})$. In both descriptions every quaternion in can be written in a *unique* way as $a + b \cdot \hat{i} + c \cdot \hat{j} + d \cdot \hat{k}$. Addition is component-wise and is the same in both cases. The main question is to check that multiplication is the same.

The key point is, the elements of the subring of real numbers *commute* with every quaternion (Check!). Thus, it is enough to check the rules for multiplication between $\hat{i}$, $\hat{j}$ and $\hat{k}$. These are given by

$$\hat{i}^2 = \hat{j}^2 = \hat{k}^2 = -1 = \hat{i}\hat{j}\hat{k}$$

in both cases.

5. (Starred) We take the set S to consist of n-tuples of elements of R and define the operations on S via the rules:

   - addition is defined component-wise.

- for the tuples $e_i = (0, \ldots, 1, \ldots, 0)$ (where 1 is in the i-th place) we define mutliplications $e_i \cdot e_j$ as linear combinations (using elements $c_{i,j,k}$ in R):

Check that the associative law for multiplication requires some identities to hold in R for the elements $c_{i,j,k}$.

Solution: The associative law will follow if we check

$$(e_i \cdot e_j) \cdot e_k = e_j \cdot (e_j \cdot e_k)$$

In terms of the above description, the left-hand side becomes

$$\sum_p c_{i,j,p} e_p \cdot e_k = \sum_p \sum_q c_{i,j,p} c_{p,k,q} e_q$$

Similarly, the right-hand side becomes

$$\sum_p c_{j,k,p} e_i \cdot e_p = \sum_p \sum_q c_{i,p,q} c_{j,k,p} e_q$$

Here we have assumed that elements of R commute all elements of S. Matching entries, we have

$$\sum_p c_{i,p,q} c_{j,k,p} = \sum_p c_{i,j,p} c_{p,k,q}$$

6. (Starred) Why do we define matrix multiplication the way we do?

Solution: First of all, it has all the right properties: associativity, distributivity and identity.

Secondly, we can show that any other way of defining mutliplication for tuples of elements of R (such as the previous exercise) is the same as defining a suitable subring of matrices. (In fact, for each p the collection $c_{p,i,j}$ can be seen as the (i,j)-th entry of a matrix and the ring we get is the subring generated by these matrices.)

7. Given a commutative ring R and an element r of R show that matrices of the form:

$$\begin{pmatrix} a & b \cdot r \\ b & a \end{pmatrix}$$

are closed under addition and mutliplication; here a and b denote elements of R.

Solution: The sum is given by

$$\begin{pmatrix} a & b\cdot r \\ b & a \end{pmatrix} + \begin{pmatrix} c & d\cdot r \\ d & c \end{pmatrix} = \begin{pmatrix} a+c & (b+d)\cdot r \\ b+d & a+c \end{pmatrix}$$

The product is given by

$$\begin{pmatrix} a & b\cdot r \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c & d\cdot r \\ d & c \end{pmatrix} = \begin{pmatrix} a\cdot c + b\cdot d\cdot r & (a\cdot d + b\cdot c)\cdot r \\ (b\cdot c + a\cdot d) & (b\cdot d\cdot r + a\cdot c) \end{pmatrix}$$

8. Show that the the ring of complex numbers is the same as the collection of matrices of the form $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ where a and b are real numbers.

Solution: The complex number $a + b\imath$ is identified with the above matrix. We then check that the sum and product are exactly as they should be.

9. Check that 2×2 matrices of the type $\begin{pmatrix} u & -\overline{v} \\ v & \overline{u} \end{pmatrix}$ with u and v in the field of complex numbers is closed under addition and multiplication.

Solution: Since addition is component-wise, and the conjugate of a sum of complex numbers is the sum of their conjugates, the result for addition is easy.

For multiplication, we have

$$\begin{pmatrix} u & -\overline{v} \\ v & \overline{u} \end{pmatrix} \cdot \begin{pmatrix} x & -\overline{y} \\ y & \overline{x} \end{pmatrix} = \begin{pmatrix} ux - \overline{v}y & -u\overline{y} - \overline{vx} \\ vx + \overline{u}y & -v\overline{y} + \overline{ux} \end{pmatrix}$$

This is a matrix of the same type with entries corresponding to $ux - \overline{v}y$ and $vx + \overline{u}y$.

10. Check that $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ is a nilpotent matrix.

Solution: If N is the matrix as above, then we have

$$N^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

It follows by multiplication the $N^3 = 0$.

11. What are the nilpotent elements in the ring $\mathbb{Z}/24$?

Solution: To get a nilpotent element we need an integer k some that some power k^n is divisible by 24. Thus, k^n is divisible is divisible by 2 and 3. It follows that k is divisible by 2 and 3; so k is of the form $6m$ for some integer m. In that case $(6m)^3 = 24(9m^3)$ is divisible by 24. In $\mathbb{Z}/24$ the distinct elements are 6, 12 and 18.

12. Check that a *strictly* upper triangular matrix is nilpotent.

Solution: If N is a $p \times p$ matrix, then its entries are determined by the result of multiplication $N \cdot e_i$ for $i = 1, \ldots, p$ where e_i is the column vector containing 1 in the i-th place and 0 elsehwere.

Now, if N is strictly upper triangular, we see that $N \cdot e_i$ is a combination of e_j for $j \geq i + 1$. Applying this iteratively, we see that $N^k \cdot e_j$ is a combination of e_j for $j \geq i + k$. Since the there are no e_j for j greater than p, we see that N^p is the 0 matrix.

13. (Starred) Give an example of a matrix which is *not* upper or lower triangular and yet is nilpotent.

Solution: All we need is a $p \times p$ matrix that sends v_i to v_{i+1} or 0 if $i = p$. where v_i is a bases of the p dimensional vector space. For example,

$$\begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}$$

14. Check that $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ is an idempotent matrix.

Solution: An easy exercise in matrix multiplication!

15. Are there any idempotent elements in $\mathbb{Z}/6$ other than 1 and 0?

Solution: We need integers n so that 6 divides $n^2 - n$; this means 2 and 2 divide $n^2 - n = n(n-1)$. Now if 2 divides n then 2 does not divide $n-1$. Now if 3 also divides n, then 6 divides n, so $n = 0$ in $\mathbb{Z}/6$. Thus we need 3 to divide $n-1$. This happens for $n = 4$. Similarly, interchanging the role of n and $n-1$ we see that $n = 3$ is another answer.

16. If p is an idempotent element, then check that $1 - p$ is also an idempotent element.

Solution: We have $(1-p)^2 = 1 - p - p + p^2 = 1 - p$ since $-p + p^2 = 0$.

17. If p is an idempotent element of a ring R, then check that the set $pRp = \{pap | a \in R\}$ is closed under addition and multiplication and that p acts as multiplicative identity on pRp.

Solution: We check that $pap + pbp = p(a+b)p$ by the distributive law in R. We also check that $(pap)(pbp) = p(ap^2b)p$ is also in pRp. (Note that this did not need that p is idempotent. To check that p acts as identity, we have $p(pap) = p^2ap = pap$ where we have used $p^2 = p$.

18. Check that $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ is a zero divisor.

Solution: The product of the above matrix with the matrix $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ is the 0 matrix.

19. What are the zero divisors in the ring $\mathbb{Z}/42$?

Solution: We need to find integers a and b so that ab is divisible by 42 but a is not. Since $42 = 2 \cdot 3 \cdot 7$. We can take a to be of the form $2m$ or $3m$ or $7m$ for some integer m.

20. Give an example of a 2×2 matrix which is not nilpotent and not idempotent and yet is a zero divisor.

Solution: The matrices

$$A = \begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 0 \\ -2 & 0 \end{pmatrix}$$

Have the property that $A \cdot B$ is 0. However,

$$A^k = \begin{pmatrix} 2^k & 2^{k-1} \\ 0 & 0 \end{pmatrix}$$

is different from A and different from 0.

21. Find a condition under which an element k of $\mathbb{Z}/n$ is a zero divisor.

Solution: The conditions is that there is an integer m so that km is divisible by n but m is not divisible by n. In other words, k should have a common factor with n.

22. (Starred) Find the condition under which a 2×2 matrix over rational numbers is a zero divisor in this ring.

Solution: A $p \times p$ matrix A is a zero divisor if (and only if) there is a non-zero vector v so that $A \cdot v = 0$.

We can then take B to be the $p \times p$ matrix all of whose columns are v; we check that $A \cdot B = 0$. Conversely, if there is a non-zero matrix B so that $A \cdot B = 0$, then we can take v to be any non-zero column of v.

Note that, in the above situation, there is also a non-zero row vector so that $w \cdot A = 0$ (since row-rank equals column rank!). Hence there is also a matrix C so that $C \cdot A = 0$.

23. Check that the matrix $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ is a unit in the ring of 2×2 matrices.

Solution: The matrix $B = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}$ has the property that $A \cdot B$ and $B \cdot A$ are the identity matrix.

24. Check that 5 is a unit in the ring $\mathbb{Z}/42$.

Solution: We note that $5 \cdot 17 = 85 = 1 \pmod{42}$.

25. Check that the product of units is also a unit.

Solution: Suppose that $u \cdot v = 1 = v \cdot u$, and $a \cdot b = 1 = b \cdot a$. Then

$$(u \cdot a) \cdot (b \cdot v) = 1 \text{ and } (b \cdot v) \cdot (u \cdot a) = 1$$

Hence $u \cdot a$ is also a unit.

26. Give a condition on an element k of $\mathbb{Z}/n$ so that it is a unit in this ring.

Solution: As seen earlier, if k and n have no common factor then there are integers A and B so that $kA + nB = 1$. It follows that $a = A\%n$ is an element of $\mathbb{Z}/n$ so that $ka = 1$ in this ring. Conversely, it there is such an element a then treating a as an integer we have the identity $ka - 1 = nb$ for a suitable integer b. So k and n have no common factor.

27. (Starred) Give a condition on 2×2 matrices over integers so that it is a unit in this ring.

Solution: Given a matrix A with integer entries for which there is a matrix B with integer entries such that $A \cdot B = 1$. In that case $\det(A)\det(B) = 1$. Since both of the latter are integers, it follows that $\det(A) = \pm 1$. Conversely, suppose

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Then we take

$$C = \begin{pmatrix} d & -b \\ -c & d \end{pmatrix}$$

We get $A \cdot C$ as the diagonal matrix with entries $ad - bc$. Now if $\det(A) = ad - bc = \pm 1$, we put $B = (ad - bc) \cdot C$; then $A \cdot B$ is the identity matrix.

28. If u is a unit *and* is idempotent, then check that $u = 1$.

Solution: We are given that there is a v so that $u \cdot v = 1 = v \cdot u$; moreover, we are given $u^2 = u$. So we get

$$u = u \cdot 1 = u \cdot (u \cdot v) = u^2 \cdot v = u \cdot v = 1$$

29. Can there be a unit which is also a zero divisor?

Solution: If $u \cdot v = 1 = v \cdot u$ and $u \cdot w = 0$, then

$$w = 1 \cdot w = (v \cdot u) \cdot w = v \cdot (u \cdot w) = v \cdot 0 = 0$$

So u is *not* a zero-divisor.

30. Is it possible for the sum of nilpotent elements to be a unit?

Solution: The matrices

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

are nilpotent. On the other hand we check that $(A + B)^2 = 1$. Hence, it *is* possible for the sum of nilpotent elements to be a unit.

31. Is it possible for the sum of units to be nilpotent?

Solution: If u is a unit, then so is $-u$. One the other hand $u + (-u) = 0$ which is certainly nilpotent!

32. (Starred) Ask yourself other questions about other combinations of properties and come up with their answers!

33. Note that the only idempotents in $\mathbb{Z}$ are 0 and 1.

Solution: For an idempotent element n we must have $n^2 - n = 0$. This means that $n \cdot (n - 1) = 0$. Now, in the ring of integers if $a \cdot b = 0$ then either a is 0 or b is 0. Hence, the only solutions are $n = 0$ or $n = 1$.

34. Show that the map that sends an element a or R to the $p \times p$ matrix $f(a)$ which has a on the diagonal and 0 everywhere else gives a ring homomorphism $f : R \to M_p(R)$.

Solution: This is a simple exercise in matrix operations of addition and multiplication.

35. Check that A given by

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_0 & -a_1 & -a_2 & \dots & \end{pmatrix}$$

satisfies the equation

$$X^n + a_{n-1}X^{n-1} + \cdots + a_0 = 0$$

Solution: Let e_i denote the row vector which has 1 in the i-th place and 0 everywhere else. We note that the matrix A can also be described as follows $e_i \cdot A = e_{i+1}$ for $i < n$ and

$$e_n \cdot A = -a_0 e_1 - a_1 e_2 - \cdots - a_{n-1} e_n$$

Note that $e_1 \cdot A^n = (e_1 \cdot A^{n-1}) \cdot A = e_n \cdot A$. Hence,

$$e_1 \cdot (A^n + a_{n-1}A^{n-1} + \dots a_0) = 0$$

Now, it follows that

$$\begin{aligned} e_i \cdot (A^n + a_{n-1}A^{n-1} + \dots a_0) = \\ (e_1 \cdot A^{i-1}) \cdot (A^n + a_{n-1}A^{n-1} + \dots a_0) = \\ e_1 \cdot (A^{n+i-1} + a_{n-1}A^{n-1+i-1} + \dots a_0 A^{i-1}) = \\ (e_i \cdot (A^n + a_{n-1}A^{n-1} + \dots a_0)) \cdot A^{i-1} = 0 \end{aligned}$$

Thus, the matrix $B = (A^n + a_{n-1}A^{n-1} + \dots a_0)$ satisfies $e_i \cdot B = 0$ for all i. In other words left-mutliplication of B by the identity matrix gives 0. So B is the 0 matrix.

36. Check that $2 \cdot 2 + 1 = 0$ in the ring $\mathbb{Z}/5$.

Solution: Simple arithmetic.

37. Check that $2 \cdot 2 \cdot 2 - 1 = 0$ in the ring $\mathbb{Z}/7$.

Solution: Simple arithmetic.