# MATB24 Assignment1 Solutions:

1.

2. 1.2.1 from textbook:

3. (a) We consider  $+_R$  and  $\times_R$  to be standard operation.

To show that real  $n \times n$  matrices form a ring, we need to verify that they satisfy the following axioms of a ring:

1. Addition is closed: For any two  $n \times n$  matrices A and B with real entries, their sum A + B is also an  $n \times n$  matrix with real entries.

Proof: Let  $A_{ij}=(a_{i,j})$  and  $B_{ij}=(b_{i,j})$ , where  $a_{i,j},b_{i,j}\in\mathbb{R}$  for all  $1\leqslant i,j\leqslant n$ 

$$(A+B)_{ij} = (a_{i,j} + b_{i,j}) \in \mathbb{R}$$

2. Multiplication is closed: For any two  $n \times n$  matrices A and B with real entries, their product AB is also an  $n \times n$  matrix with real entries.

Proof: Let  $A_{ij} = (a_{i,j})$  and  $B_{ij} = (b_{i,j})$ , where  $a_{i,j}, b_{i,j} \in \mathbb{R}$  for all  $1 \leq I, j \leq n$ 

$$(A * B)_{ij} = \sum_{k=1}^{n} a_{i,k} b_{k,j}$$

3. The additive identity exists.

There exists an  $n \times n$  matrix 0 with real entries such that A + 0 = A for any  $n \times n$  matrix A with real entries. Which is the zero matrix.

Proof: Let  $A_{ij} = (a_{i,j})$ , where  $a_{i,j} \in \mathbb{R}$  for all  $1 \leq i, j \leq n$ 

$$A_{ij} + 0_{i,j} = a_{ij} + 0 = A_{ij}$$

4. The additive inverse exists.

For any  $n \times n$  matrix A with real entries, there exists an  $n \times n$  matrix -A with real entries such that A + (-A) = 0.

Proof. Let  $A_{ij} = (a_{i,j})$  and  $-A_{ij} = (-a_{i,j})$ , where  $a_{i,j} \in \mathbb{R}$  for all  $1 \leq I, j \leq n$ . Then

$$(A + (-A))_{ij} = a_{i,j} + (-a_{i,j} = 0.$$

5. Associative with addition.

For any three  $n \times n$  matrices A, B, and C with real entries, we have (A+B)+C=A+(B+C).

Let  $A_{ij} = (a_{i,j})$ ,  $B_{ij} = (b_{i,j})$  and  $C_{ij} = (c_{i,j})$ , where  $a_{i,j}, b_{i,j}, c_{i,j} \in \mathbb{R}$  for all  $1 \leq i \leq n$ 

$$[A + (B + C)]_{ij} = a_{i,j} + (b_{i,j} + c_{i,j})$$
$$= (a_{i,j} + b_{i,j}) + c_{i,j}$$
$$= [(A + B) + C]_{ij}$$

6. Commutative with addition.

For any two  $n \times n$  matrices A and B with real entries, we have A + B = B + A.

Let  $A_{ij} = (a_{i,j})$  and  $B_{ij} = (b_{i,j})$ , where  $a_{i,j}, b_{i,j} \in \mathbb{R}$  for all  $1 \leq i, j \leq n$ . Then

$$(A+B)_{ij} = a_{i,j} + b_{i,j}$$
$$= b_{i,j} + a_{i,j}$$
$$= (B+A)_{ij}$$

7. The multiplication identity exist.

There exists an  $n \times n$  matrix I with real entries such that AI = IA = A for any  $n \times n$  matrix A with real entries.

Let  $A_{ij}=(a_{i,j})$  and  $I_{ij}=(I_{i,j})$ , where  $a_{i,j},b_{i,j}\in\mathbb{R}$  for all  $1\leqslant i,j\leqslant n$ .  $I_{i,j}=0$  if  $i\neq j$ . Otherwhise,  $I_{i,i}=0$ .

$$(AI)_{ij} = \sum_{k=1}^{n} a_{i,k} I_{k,j} = a_{i,j} = A_{ij}$$

8. Associative with multiplication.

For any three  $n \times n$  matrices A, B, and C with real entries, we have (AB)C = A(BC).

(This one is hard) Let  $A_{ij}=(a_{i,j}),\ B_{ij}=(b_{i,j})$  and  $C_{ij}=(c_{i,j}),$  where  $a_{i,j},b_{i,j},c_{i,j}\in\mathbb{R}$  for all  $1\leqslant I,j\leqslant n$ 

$$(AB)C = \sum_{l=1}^{n} \left(\sum_{k=1}^{n} a_{i,k} b_{k,l}\right) c_{l,j}$$

$$= \sum_{l=1}^{n} \sum_{k=1}^{n} (a_{i,k} b_{k,l} c_{l,j})$$

$$= \sum_{k=1}^{n} \sum_{l=1}^{n} (a_{i,k} b_{k,l} c_{l,j})$$

$$= \sum_{k=1}^{n} a_{i,k} \left(\sum_{l=1}^{n} b_{k,l} c_{l,j}\right)$$

$$= A(BC)$$

9. Multiplication distributes over addition.

For any three  $n \times n$  matrices A, B, and C with real entries, we have A(B+C) = AB + AC and (A+B)C = AC + BC.

Let  $A_{ij}=(a_{i,j}),\ B_{ij}=(b_{i,j})$  and  $C_{ij}=(c_{i,j}),$  where  $a_{i,j},b_{i,j},c_{i,j}\in\mathbb{R}$  for all  $1\leqslant I,j\leqslant n$ 

$$A(B+C) = \sum_{k=1}^{n} a_{i,k} (b_{k,j} + c_{k,j})$$

$$= \sum_{k=1}^{n} a_{i,k} b_{k,j} + a_{i,k} c_{k,j})$$

$$= \sum_{k=1}^{n} a_{i,k} b_{k,j} + \sum_{k=1}^{n} a_{i,k} c_{k,j})$$

$$= AB + AC$$

With these axioms, we can verify that real  $n \times n$  matrices form a ring.

- 4. (a) i.  $\mathbb{Z}_8$  is not a field since not every nonzero element has a multiplicative inverse. For example, 2 does not have a multiplicative inverse in  $\mathbb{Z}_8$ .
  - ii.  $\{0, 2, 4, 6\}$
  - (b) i.  $\mathbb{Z}_5$  is a field because 5 is a prime number. In lecture note page 5 we show that  $\mathbb{Z}_n$  is a field iff n is a prime number.
    - ii. Every nontrivial proper subset of  $\mathbb{Z}_5$  is an ideal since  $\mathbb{Z}_5$  is a finite field.

- 5. (a) To show that polynomials form a vector space over  $\mathbb{F}^n$ , we need to show that they satisfy the following properties:
  - 1. Closure under addition: If p(x) and q(x) are polynomials, then p(x) + q(x) is also a polynomial.

Proof: Let 
$$p(x) = \sum_{i=0}^{\infty} p_i x^i$$
 and  $q(x) = \sum_{i=0}^{\infty} q_i x^i$ , where  $p_i, q_i \in \mathbb{F}$ 

$$h(x) = p(x) + q(x) = \sum_{i=0}^{\infty} p_i x^i + q_i x^i$$
$$= \sum_{i=0}^{\infty} (p_i + q_i) x^i \in \mathbb{F}[x]$$

$$(p_i + q_i) \in \mathbb{F}$$

2. Closure under scalar multiplication: If p(x) is a polynomial and a is a scalar, then ap(x) is also a polynomial.

Let 
$$p(x) = \sum_{i=0}^{\infty} p_i x^i$$
, where  $p_i \in \mathbb{F}$ 

$$ap(x) = a \sum_{i=0}^{\infty} p_i x^i$$
$$= \sum_{i=0}^{\infty} a * p_i x^i$$

$$(a*p_i) \in \mathbb{F}$$

3. Associativity of addition: For any polynomials p(x), q(x), and h(x), h(x) + (p(x) + q(x)) = (h(x) + p(x)) + q(x).

Proof: Let  $p(x) = \sum_{i=0}^{\infty} p_i x^i$ ,  $q(x) = \sum_{i=0}^{\infty} q_i x^i$ , and  $h(x) = \sum_{i=0}^{\infty} h_i x^i$ , where  $p_i, q_i, h_i \in \mathbb{F}$ 

$$h(x) + (p(x) + q(x)) = \sum_{i=0}^{\infty} h_i x^i + (p_i x^i + q_i) x^i$$
$$= \sum_{i=0}^{\infty} (h_i + p_i) x_i + q_i x^i \in \mathbb{F}[x]$$
$$= (h(x) + p(x)) + q(x)$$

$$(p_i + q_i) \in \mathbb{F}.$$

4. Commutativity of addition: For any polynomials p(x) and q(x), p(x) + q(x) = q(x) + p(x).

Proof: Let  $p(x) = \sum_{i=0}^{\infty} p_i x^i$  and  $q(x) = \sum_{i=0}^{\infty} q_i x^i$ , where  $p_i, q_i \in \mathbb{F}$ 

$$p(x) + q(x) = \sum_{i=0}^{\infty} p_i x^i + q_i x^i$$
$$= \sum_{i=0}^{\infty} q_i x^i + p_i x^i$$
$$= q(x) + p(x)$$

5. Existence of zero vector: There exists a polynomial 0 such that for any polynomial p(x), p(x) + 0 = p(x).

Let  $p(x) = \sum_{i=0}^{\infty} p_i x^i$ , where  $p_i \in \mathbb{F}$  Let  $0(x) = \sum_{i=0}^{\infty} 0x^i$ , where  $p_i \in \mathbb{F}$ 

$$p(x) + 0(x) = \sum_{i=0}^{\infty} p_i x^i + 0x^i$$
$$= \sum_{i=0}^{\infty} (p_i + 0)x^i$$
$$= p(x)$$

6. Existence of additive inverse: For any polynomial p(x), there exists a polynomial -p(x) such that p(x) + (-p(x)) = 0.

Let 
$$p(x) = \sum_{i=0}^{\infty} p_i x^i$$
, where  $p_i \in \mathbb{F}$   
Let  $-p(x) = \sum_{i=0}^{\infty} -p_i x^i$ , where  $p_i \in \mathbb{F}$ 

$$p(x) + (-p(x)) = \sum_{i=0}^{\infty} p_i x^i + (-p_i x^i)$$
$$= \sum_{i=0}^{\infty} (p_i - p_i) x^i$$
$$= \sum_{i=0}^{\infty} 0 x^i$$

7. Identity element of scalar multiplication: For any polynomial p(x), 1p(x) = p(x).

Let 
$$p(x) = \sum_{i=0}^{\infty} p_i x^i$$
, where  $p_i \in \mathbb{F}$  Let  $1 \in \mathbb{F}$ 

$$1 * p(x) = 1 * \sum_{i=0}^{\infty} p_i x^i$$
$$= \sum_{i=0}^{\infty} (1 * p_i) x^i$$
$$= \sum_{i=0}^{\infty} p_i x^i$$
$$= p(x)$$

8. Associativity of scalar multiplication: For any scalars a and b and polynomial p(x), a(bp(x)) = (ab)p(x).

Let 
$$p(x) = \sum_{i=0}^{\infty} p_i x^i$$
, where  $p_i \in \mathbb{F}$  Let  $a, b \in \mathbb{F}$ 

$$a(bp(x)) = a(b\sum_{i=0}^{\infty} p_i x^i)$$

$$= a\sum_{i=0}^{\infty} (b * p_i) x^i$$

$$= \sum_{i=0}^{\infty} (a * b) p_i x^i$$

$$= (a * b) \sum_{i=0}^{\infty} p_i x^i$$

$$= (a * b) p(x)$$

9. Distributivity of scalar multiplication over scalar addition: For any scalars a and b and polynomial p(x), (a+b)p(x) = ap(x) + bp(x).

Let 
$$p(x) = \sum_{i=0}^{\infty} p_i x^i$$
, where  $p_i \in \mathbb{F}$  Let  $a, b \in \mathbb{F}$ 

$$(a+b)p(x)) = (a+b)\sum_{i=0}^{\infty} p_i x^i$$

$$= a\sum_{i=0}^{\infty} (a+b) * p_i x^i$$

$$= \sum_{i=0}^{\infty} a * p_i x^i + bp_i x^i$$

$$= \sum_{i=0}^{\infty} a * p_i x^i + \sum_{i=0}^{\infty} bp_i x^i$$

$$= ap(x) + bp(x)$$

10. Distributivity of scalar multiplication over vector addition: For any scalar a and polynomials p(x) and q(x), a(p(x) + q(x)) = ap(x) + aq(x).

All of these properties can be verified using the basic properties of addition and multiplication of real numbers. Therefore, polynomials form a vector space over  $\mathbb{R}^n$ .

Let  $p(x) = \sum_{i=0}^{\infty} p_i x^i$ , where  $p_i \in \mathbb{F}$  Let  $q(x) = \sum_{i=0}^{\infty} q_i x^i$ , where  $q_i \in \mathbb{F}$  Let  $a \in \mathbb{F}$ 

$$a(p(x) + q(x)) = a \left( \sum_{i=0}^{\infty} p_i x^i + \sum_{i=0}^{\infty} p_i x^i \right)$$

$$= a \sum_{i=0}^{\infty} (p_i + q_i) x^i$$

$$= \sum_{i=0}^{\infty} a * p_i x^i + a q_i x^i$$

$$= \sum_{i=0}^{\infty} a * p_i x^i + \sum_{i=0}^{\infty} a q_i x^i$$

$$= a p(x) + a q(x)$$

(b) We consider  $+_R$  and  $\times_R$  to be standard operation.

To show that polynomials form a ring over  $\mathbb{F}$ , we need to verify that they satisfy the following axioms of a ring:

1. Addition is closed: If p(x) and q(x) are polynomials, then p(x) + q(x) is also a polynomial.

Proof: Let 
$$p(x) = \sum_{i=0}^{\infty} p_i x^i$$
 and  $q(x) = \sum_{i=0}^{\infty} q_i x^i$ , where  $p_i, q_i \in \mathbb{F}$ 

$$h(x) = p(x) + q(x) = \sum_{i=0}^{\infty} p_i x^i + q_i x^i$$
$$= \sum_{i=0}^{\infty} (p_i + q_i) x^i \in \mathbb{F}[x]$$

$$(p_i + q_i) \in \mathbb{F}$$

2. Multiplication is closed: If p(x) and q(x) are polynomials, then p(x)q(x) is also a polynomial.

Proof: Let  $p(x) = \sum_{i=0}^{\infty} p_i x^i$  and  $q(x) = \sum_{j=0}^{\infty} q_j x^j$ , where  $p_i, q_j \in \mathbb{F}$ 

$$p(x)q(x) = \sum_{i=0}^{\infty} p_i x^i \sum_{j=0}^{\infty} q_j x^j$$
$$= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} (p_i q_j) x^{i+j} \in \mathbb{F}[x]$$

$$(p_iq_j) \in \mathbb{F}$$

3. The additive identity exists.

There exists a polynomial 0 such that for any polynomial p(x), p(x) + 0 = p(x)

Let 
$$p(x) = \sum_{i=0}^{\infty} p_i x^i$$
, where  $p_i \in \mathbb{F}$  Let  $0(x) = \sum_{i=0}^{\infty} 0x^i$ , where  $p_i \in \mathbb{F}$ 

$$p(x) + 0(x) = \sum_{i=0}^{\infty} p_i x^i + 0x^i$$
$$= \sum_{i=0}^{\infty} (p_i + 0)x^i$$
$$= p(x)$$

4. The additive inverse exists.

For any polynomial p(x), there exists a polynomial -p(x) such that p(x) + (-p(x)) = 0.

Let 
$$p(x) = \sum_{i=0}^{\infty} p_i x^i$$
, where  $p_i \in \mathbb{F}$   
Let  $-p(x) = \sum_{i=0}^{\infty} -p_i x^i$ , where  $p_i \in \mathbb{F}$ 

$$p(x) + (-p(x)) = \sum_{i=0}^{\infty} p_i x^i + (-p_i x^i)$$
$$= \sum_{i=0}^{\infty} (p_i - p_i) x^i$$
$$= \sum_{i=0}^{\infty} 0x^i$$

### 5. Associative with addition.

For any polynomials p(x), q(x), and h(x), h(x) + (p(x) + q(x)) = (h(x) + p(x)) + q(x).

Proof: Let  $p(x) = \sum_{i=0}^{\infty} p_i x^i$ ,  $q(x) = \sum_{i=0}^{\infty} q_i x^i$ , and  $h(x) = \sum_{i=0}^{\infty} h_i x^i$ , where  $p_i, q_i, h_i \in \mathbb{F}$ 

$$h(x) + (p(x) + q(x)) = \sum_{i=0}^{\infty} h_i x^i + (p_i x^i + q_i) x^i$$
$$= \sum_{i=0}^{\infty} (h_i + p_i) x_i + q_i x^i \in \mathbb{F}[x]$$
$$= (h(x) + p(x)) + q(x)$$

$$(p_i + q_i) \in \mathbb{F}.$$

### 6. Commutative with addition.

For any polynomials p(x) and q(x), p(x) + q(x) = q(x) + p(x).

Proof: Let 
$$p(x) = \sum_{i=0}^{\infty} p_i x^i$$
 and  $q(x) = \sum_{i=0}^{\infty} q_i x^i$ , where  $p_i, q_i \in \mathbb{F}$ 

$$p(x) + q(x) = \sum_{i=0}^{\infty} p_i x^i + q_i x^i$$
$$= \sum_{i=0}^{\infty} q_i x^i + p_i x^i$$
$$= q(x) + p(x)$$

### 7. The multiplication identity exist.

There exists a polynomial 1 such that for any polynomial p(x), 1p(x) = p(x).

Let  $p(x) = \sum_{i=0}^{\infty} p_i x^i$ , where  $p_i \in \mathbb{F}$  Let  $1 \in \mathbb{F}$ 

$$1 * p(x) = 1 * \sum_{i=0}^{\infty} p_i x^i$$
$$= \sum_{i=0}^{\infty} (1 * p_i) x^i$$
$$= \sum_{i=0}^{\infty} p_i x^i$$
$$= p(x)$$

## 8. Associative with multiplication.

For any polynomials p(x), q(x), and r(x), (p(x)q(x))r(x) = p(x)(q(x)r(x)).

Proof: Let  $p(x) = \sum_{i=0}^{\infty} p_i x^i$  and  $q(x) = \sum_{j=0}^{\infty} q_j x^j$  and  $r(x) = \sum_{k=0}^{\infty} r_k x^k$ , where  $p_i, q_j, r_k \in \mathbb{F}$ 

$$(p(x)q(x))r(x) = \left(\sum_{i=0}^{\infty} p_i x^i \sum_{j=0}^{\infty} q_j x^j\right) \sum_{k=0}^{\infty} r_k x^k$$

$$= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} (p_i q_j) x^{i+j} \sum_{k=0}^{\infty} r_k x^k$$

$$= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} (p_i q_j) r_k x^{(i+j)+k}$$

$$= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} p_i (q_j r_k) x^{i+(j+k)}$$

$$= \sum_{i=0}^{\infty} p_i x^i \left(\sum_{j=0}^{\infty} q_j x^j \sum_{k=0}^{\infty} r_k x^k\right)$$

$$= \sum_{i=0}^{\infty} p_i x^i (q(x)r(x))$$

$$= p(x) (q(x)r(x)) \in \mathbb{F}[x]$$

#### 9. Multiplication distributes over addition.

For any polynomials p(x), q(x), and r(x), p(x)(q(x) + r(x)) = p(x)q(x) + p(x)r(x).

Proof: Let 
$$p(x) = \sum_{i=0}^{\infty} p_i x^i$$
 and  $q(x) = \sum_{j=0}^{\infty} q_j x^j$  and  $r(x) = \sum_{j=0}^{\infty} r_j x^j$ , where  $p_i, q_j, r_k \in \mathbb{F}$ 

$$p(x)(q(x) + r(x)) = \sum_{i=0}^{\infty} p_i x^i (\sum_{j=0}^{\infty} q_j x^j + \sum_{j=0}^{\infty} r_j x^j)$$

$$= \sum_{i=0}^{\infty} p_i x^i (\sum_{j=0}^{\infty} (q_j + r_j) x^j)$$

$$= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} p_i x^i (q_j + r_j) x^j$$

$$= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} (p_i q_j + p_i r_j) x^{i+j}$$

$$= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} (p_i q_j x^{i+j} + p_i r_j x^{i+j})$$

$$= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} p_i q_j x^{i+j} + \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} p_i r_j x^{i+j}$$

$$= p(x) q(x) + p(x) r(x) \in \mathbb{F}[x]$$

With these axioms, we can verify that polynomials form a ring.

(c) Polynomials satisfy all the properties of a ring, as shown in the part(b). To show that multiplication is commutative, we need to show that for any polynomials p(x) and q(x), p(x)q(x) = q(x)p(x).

Proof: Let 
$$p(x) = \sum_{i=0}^{\infty} p_i x^i$$
 and  $q(x) = \sum_{j=0}^{\infty} q_j x^j$ , where  $p_i, q_j \in \mathbb{F}$ 

$$p(x)q(x) = \sum_{i=0}^{\infty} p_i x^i \sum_{j=0}^{\infty} q_j x^j$$

$$= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} (p_i q_j) x^{i+j}$$

$$= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} (q_j p_i) x^{j+i}$$

$$= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} (q_j p_i) x^{j+i} \in \mathbb{F}[x]$$

Therefore, polynomials form a commutative ring.

#### 6. 2.1.1 from textbook:

- 7. 2.1.2 from textbook:
- 8. 2.1.3 from textbook:
- 9. 2.1.4 from textbook:
  - 2.1.7 from textbook:
- 10. 2.1.5 from textbook:
- 11. 2.2.1 from textbook:
- 12. 2.2.2 from textbook:
- 13. 2.2.3 from textbook:
- 14. 2.3.2 from textbook:
- 15. 2.3.3 from textbook:
- 16. 2.3.10 from textbook:
- 17. 2.3.12 from textbook:
- 18. 6.6.1 from textbook:
- 19. 6.6.2 from textbook:
- 20. A set  $v_1, v_2, v_3$  is a basis of  $\mathbb{R}^3$  if  $v_1, v_2, v_3$  is a set of linear independent vectors that generates  $\mathbb{R}^3$ .

Let 
$$v_1 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$
 Let  $v_2 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$  Let  $v_3 = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$ 

 $\begin{array}{l} \text{In } \mathbb{R}^3 \colon \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ which indicate that } v_1, v_2, v_3 \text{ are linear independent. Because the rank is 3, so } v_1, v_2, v_3 \text{ spans } \mathbb{R}^3 \text{ which is a basis of } \mathbb{R}^3. \end{array}$ 

In 
$$(\mathbb{Z}_2)^3$$
:  $(v_1 + v_2) + v_3 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$  which is linear dependent. So it is not a basis.