HOMEWORK 10 (DUE: 11:15 AM, NOV 21 WED)

1. Do Exercise 17.A.1–7 in [Pin10].

1. For any $a, b, c \in \mathbb{Z}$, we have

- $(a \oplus b) \oplus c = a + b + c - 2 = a \oplus (b \oplus c), \quad a \oplus b = a + b - 1 = b \oplus a,$
  $a \oplus 1 = 1 \oplus a = a, \quad a \oplus (2 - a) = (2 - a) \oplus a = 1.$

Thus $(\mathbb{Z}, \oplus)$ is an abelian group with identity 1. Also for any $a \in \mathbb{Z}$, its
additive inverse is given by $2 - a$.

- $(a \odot b) \odot c = (ab - (a + b) + 2) \odot c = abc - ab - bc - ab + a + b + c,$
  $a \odot (b \odot c) = a \odot (bc - (b + c) + 2) = abc - ab - bc - ab + a + b + c.$

Thus $\odot$ is associative.

- $a \odot b = b \odot a = ab - (a + b) + 2$, thus $\odot$ is commutative.

- $a \odot (b \oplus c) = a \odot (b + c - 1) = ab + ac - 2a - b - c + 3,$
  $a \odot b \oplus a \odot c = ab + ac - 2a - b - c + 3.$

Thus distribution law holds. (The other half of the condition comes from
that $\odot$ is commutative.)

- $a \odot 2 = 2 \odot a = a$, thus 2 is the unity.

2. For any $a, b, c \in \mathbb{Q}$, we have

- $(a \oplus b) \oplus c = a + b + c + 2 = a \oplus (b \oplus c), \quad a \oplus b = a + b + 1 = b \oplus a,$
  $a \oplus (-1) = (-1) \oplus a = a, \quad a \oplus (-2 - a) = (-2 - a) \oplus a = -1.$

Thus $(\mathbb{Q}, \oplus)$ is an abelian group with identity $-1$. Also for any $a \in \mathbb{Q}$, its
additive inverse is given by $-2 - a$.

- $(a \odot b) \odot c = (ab + a + b) \odot c = abc + ab + ac + bc + a + b + c,$
  $a \odot (b \odot c) = a \odot (bc + b + c) = abc + ab + ac + bc + a + b + c.$

Thus $\odot$ is associative.

- $a \odot b = b \odot a = ab + a + b$, thus $\odot$ is commutative.

- $a \odot (b \oplus c) = a \odot (b + c + 1) = ab + ac + 2a + b + c + 1,$
  $a \odot b \oplus a \odot c = ab + ac + 2a + b + c + 1.$
Thus distribution law holds. (The other half of the condition comes from
that \( \circ \) is commutative)

- \( a \circ 0 = 0 \circ a = a \), thus 0 is the unity.

3. For any \( a, b, c, d, e, f \in \mathbb{Q} \), we have

- \((a, b) \oplus (c, d) \oplus (e, f) = (a + c + e, b + d + f) = (a, b) \oplus ((c, d) \oplus (e, f))\),
- \((a, b) \oplus (c, d) = (a + c, b + d) = (c, d) \oplus (a, b)\),
- \((a, b) \oplus (0, 0) = (0, 0) \oplus (a, b) = (a, b)\),
- \((a, b) \oplus (-a, -b) = (-a, -b) \oplus (a, b) = (0, 0)\).

Thus \((\mathbb{Q} \times \mathbb{Q}, \oplus)\) is an abelian group with identity \((0, 0)\). Also for any
\((a, b) \in \mathbb{Q} \times \mathbb{Q}\), its additive inverse is given by \((-a, -b)\).

- \((a, b) \circ (c, d) \oplus (e, f) = (ac - bd, ad + bc) \circ (e, f)\)
- \((ac - bde - bcf - aef, bce + ade + acf - bdf)\).

Thus \( \circ \) is associative.

- \((a, b) \circ (c, d) = (c, d) \circ (a, b) = (ac - bd, ad + bc)\), thus \( \circ \) is commutative.

- \((a, b) \circ ((c, d) \oplus (e, f)) = (a, b) \circ (c + e, d + f)\)
- \((ac - bd + ae - bf, ad + bc + be + af)\),
- \((a, b) \circ (c, d) \oplus (a, b) \circ (e, f) = (ac - bd + ae - bf, ad + bc + be + af)\).

Thus distribution law holds. (The other half of the condition comes from
that \( \circ \) is commutative)

- \((a, b) \circ (1, 0) = (1, 0) \circ (a, b) = (a, b)\), thus \((1, 0)\) is the unity.

4. It is a subset of \( \mathbb{C} \) with the usual multiplication and addition. Thus it suffices
to check that \( A \) is a subring of \( \mathbb{C} \). For \( a, b, c, d \in \mathbb{Z} \), we have

- \((a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in A\).
- \((a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bc) + (bc + ad)\sqrt{2} \in A\).
- \(1 = (1 + 0\sqrt{2}) \in A\).

Thus \( A \) is a subring of \( \mathbb{C} \) (with unity). In particular, 0 is the zero element, 1 is
the unity, and \(-a - b\sqrt{2}\) is the additive inverse of \( a + b\sqrt{2} \).

5. Let \( a, b \in \mathbb{Z} \) be such that \( a \circ b = 1 \). (Recall that 1 is the additive identity
of \( A \).) As \( ab - (a + b) + 2 = (a - 1)(b - 1) + 1 \), \( a \circ b = 1 \) if and only if
(a − 1)(b − 1) = 0. It means either a or b is the additive identity. It follows that there is no zero-divisor in A, thus A is the integral domain.

6. For any $a \in \mathbb{Q}$ such that $a \neq -1$, let us set $b = \frac{-a}{a+1}$. Then

$$a \odot b = \frac{-a^2}{a+1} + a - \frac{a}{a+1} = 0,$$

thus b is the multiplicative inverse of a.

7. For any $(a, b) \in \mathbb{Q} \times \mathbb{Q}$ such that $(a, b) \neq (0, 0)$, define $(c, d) = (\frac{-a}{a^2+b^2}, \frac{-b}{a^2+b^2})$. Then,

$$(a, b) \odot (c, d) = \left( \frac{a^2}{a^2+b^2} + \frac{b^2}{a^2+b^2}, \frac{-ab}{a^2+b^2} + \frac{ab}{a^2+b^2} \right) = (1, 0),$$

thus $(c, d)$ is the multiplicative inverse of $a$. In particular, $A$ is a field.

2. Do Exercise 17.C.1–3 in [Pin10].

1. For any $a, b, c, d, r, s, t, u, x, y, z, w \in \mathbb{R}$, we have

- $\left( \begin{array}{cc} a & b \\ c & d \end{array} \right) + \left( \begin{array}{cc} r & s \\ t & u \end{array} \right) + \left( \begin{array}{cc} x & y \\ z & w \end{array} \right) = \left( \begin{array}{cc} a+r+x & b+s+y \\ c+t+z & d+u+w \end{array} \right),$
- $\left( \begin{array}{cc} a & b \\ c & d \end{array} \right) + \left( \begin{array}{cc} r & s \\ t & u \end{array} \right) + \left( \begin{array}{cc} x & y \\ z & w \end{array} \right) = \left( \begin{array}{cc} a+r+x & b+s+y \\ c+t+z & d+u+w \end{array} \right),$
- $\left( \begin{array}{cc} a & b \\ c & d \end{array} \right) + \left( \begin{array}{cc} 0 & 0 \\ 0 & 0 \end{array} \right) = \left( \begin{array}{cc} a & b \\ c & d \end{array} \right),$
- $\left( \begin{array}{cc} a & b \\ c & d \end{array} \right) + \left( \begin{array}{cc} -a & -b \\ -c & -d \end{array} \right) = \left( \begin{array}{cc} 0 & 0 \\ 0 & 0 \end{array} \right),$

Thus $\mathcal{M}_2(\mathbb{R})$ is an abelian group with identity $\left( \begin{array}{cc} 0 & 0 \\ 0 & 0 \end{array} \right)$. Also for any $\left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in \mathcal{M}_2(\mathbb{R})$, its additive inverse is given by $\left( \begin{array}{cc} -a & -b \\ -c & -d \end{array} \right)$.

- $\left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \left( \begin{array}{cc} r & s \\ t & u \end{array} \right) \left( \begin{array}{cc} x & y \\ z & w \end{array} \right) = \left( \begin{array}{cc} arx + btx + asz + buz & asw + bwu + ary + bty \\ crx + dtx + csz + dus & csw + duw + cry + dty \end{array} \right),$
- $\left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \left( \begin{array}{cc} r & s \\ t & u \end{array} \right) \left( \begin{array}{cc} x & y \\ z & w \end{array} \right) = \left( \begin{array}{cc} arx + btx + asz + buz & asw + bwu + ary + bty \\ crx + dtx + csz + dus & csw + duw + cry + dty \end{array} \right).$

Thus the multiplication is associative.

2. We observed above that \((\begin{smallmatrix}1 & 0 \\ 0 & 1 \end{smallmatrix})\) is the unity. Also, \((\begin{smallmatrix}0 & 1 \\ 0 & 0 \end{smallmatrix}) = (\begin{smallmatrix}0 & 1 \\ 0 & 0 \end{smallmatrix})(\begin{smallmatrix}1 & 1 \\ 0 & 0 \end{smallmatrix}) \neq (\begin{smallmatrix}1 & 1 \\ 0 & 0 \end{smallmatrix})(\begin{smallmatrix}1 & 0 \\ 0 & 0 \end{smallmatrix}) = (\begin{smallmatrix}1 & 0 \\ 0 & 1 \end{smallmatrix})\), thus \(M_2(\mathbb{R})\) is not commutative.

3. \((\begin{smallmatrix}0 & 0 \\ 0 & 0 \end{smallmatrix}) = (\begin{smallmatrix}0 & 1 \\ 0 & 0 \end{smallmatrix})(\begin{smallmatrix}1 & 0 \\ 0 & 0 \end{smallmatrix})\), thus \((\begin{smallmatrix}0 & 1 \\ 0 & 0 \end{smallmatrix})\) and \((\begin{smallmatrix}1 & 0 \\ 0 & 0 \end{smallmatrix})\) are zero-divisors of \(M_2(\mathbb{R})\). Thus \(M_2(\mathbb{R})\) is not an integral domain and thus not a field as well.


1. Let \(a^n = 0\) for some \(n \in \mathbb{Z}_{>0}\). Then \(1 - a^n = 1 + a^n\) and thus

\[
1 = (1 - a)(1 + a + \cdots + a^{n-1}) = (1 + a + \cdots + a^{n-1})(1 - a),
\]

\[
1 = (1 + a)(1 - a + \cdots + (-1)^{n-1}a^{n-1}) = (1 - a + \cdots + (-1)^{n-1}a^n)(1 + a).
\]

Therefore \(1 + a\) and \(1 - a\) are both units. Also \(a - 1\) is a unit as it is a product of two units \(-1\) and \(1 - a\).

2. Let \(a^n = 0\) for some \(n \in \mathbb{Z}_{>0}\). Then \((xa)^n = x^n a^n = 0\), thus \(xa\) is nilpotent.

3. Let \(a^n = b^m = 0\) for some \(m, n \in \mathbb{Z}_{>0}\). Then

\[
(a + b)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} a^k b^{m+n-k}.
\]

But for any \(0 \leq k \leq m + n\), either \(k \geq n\) or \(m + n - k \geq m\), thus \(a^k = 0\) or \(b^{m+n-k} = 0\). In other words, all the terms in the RHS is zero. Thus \((a + b)^{m+n} = 0\), which means that \(a + b\) is nilpotent.

4. Let \(a, b\) be two unipotent elements. Then \(1 - ab = (1 - a) + a(1 - b)\), and by part 2 and 3 it is nilpotent. Thus \(ab\) is unipotent.

5. Let \(a\) be a unipotent element. Then \(1 - a\) is nilpotent, thus \((1 - a) - 1 = -a\) is invertible by part 1. It follows that the product of two units -1 and \(-a\), namely \(a\), is also invertible.
References