MATH 416 Abstract Linear Algebra

Homework 2
Assigned: Fri. Sept. 5, 2025
Due: Fri. Sept. 12, 2025 (by 1pm)

Reminder: I encourage you to work together and use resources as needed. Please remember to state who you collaborated with and what resources you used.

Exercise 1 (3 points): Complex conjugate and roots of real polynomials
In this problem we will explore some key properties of complex numbers and build toward Euler's formula.

(a) **Real numbers via conjugation.** Let $z = x + iy \in \mathbb{C}$ with $x, y \in \mathbb{R}$, and let $z^* = x - iy$ denote its complex conjugate. Prove that

$$z = z^* \iff z \in \mathbb{R}.$$

Proof. ($\Rightarrow$) If $z = z^*$, we have

$$\begin{aligned} a + bi &= a - bi, && \text{assumption} && (1)\\ bi &= -bi, && \text{additive inverse exists} && (2)\\ b &= -b, && && (3) \end{aligned}$$

which is only possible if $b = 0$. That is, if $z \in \mathbb{R}$.

($\Leftarrow$) If $z \in \mathbb{R}$, then $b = 0$ and we have $z = a$, for some real number a. It immediately follows that $z^* = a^* = a$, because real numbers are invariant under complex conjugation (they lie on the x axis in the imaginary plane). $\square$

(b) **Cube roots of unity.** Solve the equation

$$z^3 = 1$$

for all complex numbers z. Plot the solutions in the complex plane and describe the geometric pattern you see.

This would be very challenging in standard form, so we use polar form. Let $z = re^{i\theta}$.

We then have

$$z^3 = r^3 \left(e^{i\theta}\right)^3. \tag{4}$$

Because $|1| = 1$, we know $r = 1$. To find the angles that solve this equation, note that we can write

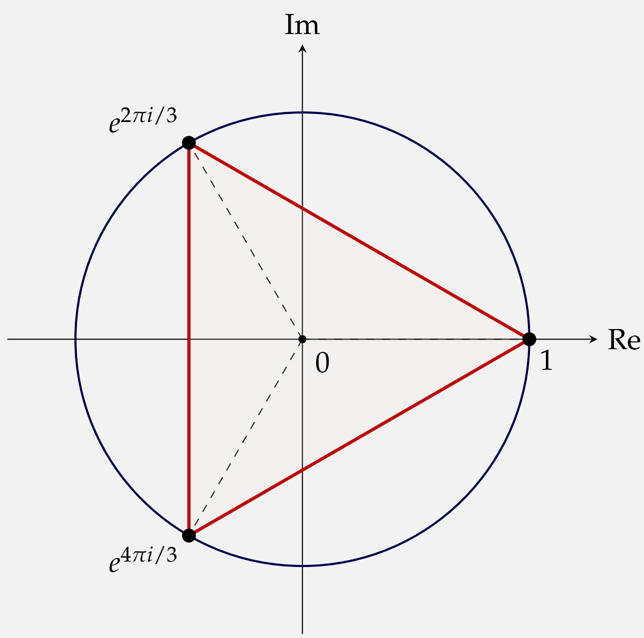
$$1 = e^{i \cdot 2\pi \cdot k}, \quad \forall k \in \mathbb{Z}. \tag{5}$$

This implies that the solutions we seek satisfy

$$e^{i3\theta} = e^{i \cdot 2\pi \cdot k}, \tag{6}$$

$$\implies \theta = \frac{2\pi k}{3}. \tag{7}$$

Geometrically, these form a triangle on the unit circle.



(c) **Euler's formula.** Recall the Taylor series expansions:

$$\begin{aligned} e^x &= \sum_{n=0}^{\infty} \frac{x^n}{n!}, \\ \cos x &= \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!}, \\ \sin x &= \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!}. \end{aligned}$$

Use these to prove Euler's most famous formula: $e^{i\theta} = \cos\theta + i\sin\theta$. Setting $\theta = \pi$ we obtain what many consider to be the most beautiful formulas in all of mathematics

$$e^{i\pi} + 1 = 0.$$

Proof. We start from the Taylor series expansions for the exponential, sine, and cosine functions. Substituting $x = i\theta$ into the exponential series yields

$$e^{i\theta} = \sum_{n=0}^{\infty} \frac{(i\theta)^n}{n!} = \sum_{n=0}^{\infty} \frac{i^{2n}\theta^{2n}}{(2n)!} + \sum_{n=0}^{\infty} \frac{i^{2n+1}\theta^{2n+1}}{(2n+1)!},$$

where we have broken the sum into its even and odd terms. Using $i^2 = -1$, we simplify:

$$i^{2n} = (i^2)^n = (-1)^n, \qquad i^{2n+1} = i \cdot (-1)^n.$$

Hence, the series becomes

$$e^{i\theta} = \sum_{n=0}^{\infty} (-1)^n \frac{\theta^{2n}}{(2n)!} + i \sum_{n=0}^{\infty} (-1)^n \frac{\theta^{2n+1}}{(2n+1)!} = \cos\theta + i\sin\theta.$$

This proves Euler's formula:

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

Setting $\theta = \pi$, we find

$$e^{i\pi} = \cos\pi + i\sin\pi = -1 + i \cdot 0 = -1,$$

so that

$$e^{i\pi} + 1 = 0,$$

which is Euler's famous identity. □

Exercise 2 (10 points): **A Matrix Representation of Powers of i**

We recall that a *group* is a set G together with a binary operation $\cdot$ satisfying the following axioms:

1. **Closure:** For all $a, b \in G$, the product $a \cdot b \in G$.
2. **Associativity:** For all $a, b, c \in G$, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. **Identity:** There exists an element $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$.
4. **Inverses:** For each $a \in G$, there exists $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

(a) Show that the set

$$G = \{1, i, -1, -i\}$$

with multiplication of complex numbers as the operation is a group. (This group is sometimes called the *cyclic group of order 4*.)

Solution. Closure for small groups is perhaps most intuitively seen via a multiplication table.

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Associativity follows directly from the associativity of complex numbers. Clearly, $1 \in G$, so we have an identity (that is $e = 1$). Inverses can be verified directly:

$$1 \cdot 1 = 1,\ i \cdot (-i) = 1,\ -1 \cdot (-1),\ -i \cdot i = 1, \tag{8}$$

therefore, for ever element of $a \in G$, there exists an element $b \in G$ such that $a \cdot b = e$.

(b) Recall that a rotation in the plane by an angle θ can be written as

$$R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

Which matrix should represent multiplication by i? Compute its powers M^2, M^3, and M^4.

Solution. Thinking about the unit circle in the complex plane, we suspect that multiplication by i in the complex plane should correspond to a counterclockwise rotation by

$\pi/2$ radians. The rotation matrix by angle θ is

$$R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

Taking $\theta = \frac{\pi}{2}$ gives

$$M = R\left(\tfrac{\pi}{2}\right) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Compute powers:

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

$$M^3 = M^2 M = (-I)M = -M = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},$$

$$M^4 = M^2 M^2 = (-I)(-I) = I.$$

(c) Compare your results to the powers of i. What correspondence do you notice between the set $\{1, i, -1, -i\}$ and the set $\{I, M, M^2, M^3\}$, where I is the 2×2 identity matrix?

Solution. The powers of i are

$$i^1 = i, \quad i^2 = -1, \quad i^3 = -i, \quad i^4 = 1.$$

The correspondence is

$$i \longleftrightarrow M, \qquad -1 \longleftrightarrow M^2, \qquad -i \longleftrightarrow M^3, \qquad 1 \longleftrightarrow M^4 = I,$$

since the respective powers match (both have order 4 and the same multiplication table).

(d) Show that the set

$$H = \{I, M, M^2, M^3\}$$

forms a group under matrix multiplication. (You should check closure, identity, and inverses explicitly. Associativity comes for free since matrix multiplication is associative.)

- *Closure:* Products of powers of M are powers of M (e.g. $M^a M^b = M^{a+b}$), and exponents are taken modulo 4, so multiplication stays inside H.
- *Identity:* $I \in H$ is the identity matrix.
- *Inverses:* Each element has an inverse in H: $I^{-1} = I$, $M^{-1} = M^3$, $(M^2)^{-1} = M^2$, $(M^3)^{-1} = M$. (These follow since $M^4 = I$.)
- *Associativity:* Matrix multiplication is associative, so this axiom holds automatically.

Hence H is a group (in fact a cyclic subgroup of $\mathrm{GL}_2(\mathbb{R})$ generated by M).

(e) Conclude that the mapping

$$\varphi : G \to H, \quad \varphi(1) = I,\ \varphi(i) = M,\ \varphi(-1) = M^2,\ \varphi(-i) = M^3$$

is a group homomorphism. (In fact, φ is also an isomorphism onto H.) In this way, we have found a *matrix representation* of the cyclic group of order 4.

Define φ by

$$\varphi(1) = I, \quad \varphi(i) = M, \quad \varphi(-1) = M^2, \quad \varphi(-i) = M^3.$$

For any $a, b \in G$ we have $\varphi(ab) = \varphi(a)\varphi(b)$ because both sides correspond to the same exponent arithmetic modulo 4 (e.g. $\varphi(i \cdot i) = \varphi(i^2) = \varphi(-1) = M^2 = M \cdot M = \varphi(i)\varphi(i)$). Thus φ is a group homomorphism, i.e. a representation of G by 2×2 real matrices.
Moreover, φ is bijective onto H by construction (it is one-to-one on the four distinct elements and its image is exactly H), so φ is an isomorphism from G onto H. In representation-theoretic language, φ is an injective (faithful) 2-dimensional real representation of the cyclic group of order 4.

That was a lot of jargon! Why did I assign this problem in the first place? It is one of the simplest examples of *representation theory* – the study of how abstract algebraic objects (like groups) can be expressed concretely as matrices acting on vector spaces. This translation turns algebra into linear algebra, where we have powerful tools to analyze symmetry and structure. Representation theory is central in modern mathematics and physics: it underlies the classification of elementary particles in quantum mechanics, explains patterns in molecular vibrations, and even shapes number theory. Remarkably, representation theory of groups over finite fields played a crucial role in Andrew Wiles's celebrated proof of Fermat's Last Theorem, showing how deep and far-reaching these ideas can be.

Exercise 3 (4 points): **Vector spaces**

Let V be a vector space over a field $\mathbb{F}$. Use the axioms of vector spaces to show the following.

(a) Prove that the zero vector $0 \in V$ is unique.

Proof. Suppose 0 and $0'$ are zero vectors (i.e. additive identities) in V such that $0 \neq 0'$. Then,

$$
\begin{aligned}
0 &= 0 + 0', && 0' \text{ is an additive identity,} && (9)\\
0 &= 0' + 0, && \text{commutativity} && (10)\\
0 &= 0' && 0 \text{ is an additive identity,} && (11)
\end{aligned}
$$

and we have a contradiction. Thus, the zero vector in V is unique. □

(b) Show that for any $v \in V$, the additive inverse $-v$ is unique.

Proof. Suppose there are two unequal additive inverses u, w. This implies $v + u = 0$ and $v + w = 0$. We can then write

$$
\begin{aligned}
w &= w + 0, && \text{Additive identity} && (12)\\
&= w + (v + u), && \text{By assumption} && (13)\\
&= (w + v) + u, && \text{Associativity} && (14)\\
&= 0 + u, && \text{Additive inverse} && (15)\\
&= u, && \text{Additive identity} && (16)
\end{aligned}
$$

□

(c) Let $v \in V$ and $\lambda \in \mathbb{F}$. Prove that $0 \cdot v = 0$ and $\lambda \cdot 0 = 0$, where the first 0 is the scalar 0 and the second 0 is the zero vector.

Proof. In the first case,

$$
\begin{aligned}
0v &= (0 + 0)v, && \text{Additive identity in } \mathbb{F} && (17)\\
&= 0v + 0v, && \text{Distributivity} && (18)\\
0 &= 0v && \text{Additive inverse} && (19)
\end{aligned}
$$

In the second case,

$$\lambda 0 = \lambda(0+0), \qquad \text{Additive identity in } V \tag{20}$$

$$= \lambda 0 + \lambda 0, \qquad \text{Distributivity} \tag{21}$$

$$0 = \lambda 0 \qquad \text{Additive inverse} \tag{22}$$

$\square$

(d) Show that if $\lambda v = 0$ for some $\lambda \in \mathbb{F}$ and $v \in V$, then either $\lambda = 0$ or $v = 0$.

Proof. Suppose $\lambda v = 0$ for some $\lambda \in \mathbb{F}$ and $v \in V$. If $\lambda = 0$, we are done. Now assume $\lambda \neq 0$. Since $\mathbb{F}$ is a field, λ has a multiplicative inverse $\lambda^{-1} \in \mathbb{F}$. Multiply both sides of the equation $\lambda v = 0$ by λ^{-1}:

$$\lambda^{-1}(\lambda v) = \lambda^{-1} \cdot 0.$$

By associativity of scalar multiplication,

$$(\lambda^{-1}\lambda)v = 0.$$

But $\lambda^{-1}\lambda = 1$, so

$$1 \cdot v = 0,$$

which means $v = 0$.
Therefore, if $\lambda v = 0$ then either $\lambda = 0$ or $v = 0$, as desired. $\square$

Remark: This argument relies crucially on the fact that the scalars come from a field, where every nonzero element has a multiplicative inverse. If instead we allowed the scalars to come from a ring with zero divisors, the statement can fail. For example, over $\mathbb{Z}/6\mathbb{Z}$ we have

$$2 \cdot 3 = 0 \quad \text{in } \mathbb{Z}/6\mathbb{Z},$$

even though neither 2 nor 3 is zero in this ring. Thus, the conclusion "$\lambda v = 0$ implies $\lambda = 0$ or $v = 0$" is special to vector spaces over *fields*.

Exercise 4 (3 points): Subspaces

(i) Let $U, W \leq V$ be subspaces of a vector space V. Show that $U \cap W$ is also a subspace of V.

Proof. We can prove this using the conditions for a subspace in Lemma 1.34 of Axler (page 18 in the fourth edition).

(a) **Additive identity.** Because $U, W \leq V$, we know $0 \in U$ and $0 \in W$. Thus $0 \in U \cap W$ by definition of the intersection.

(b) **Closed under addition.** Let $u, w \in U \cap W$. This means $u, w \in U$ and $u, w \in W$. Because both of these are subspaces, we know $u + w \in U$ and $u + w \in W$. By the definition of the intersection, this implies $u + w \in U \cap W$.

(c) **Closed under scalar multiplication.** Same argument.

□

(ii) Prove that the subset $\{x \in \mathbb{F}^3 : x_1 x_2 x_3 = 0\} \subset \mathbb{F}^3$ is *not* a subspace of $\mathbb{F}^3$.

Proof. Because the conditions for a subspace (Lemma 1.34) hold if and only if, we just need to show that one of them does **not** hold in order to conclude a subset is not a subspace. Let U denote the subset in question.

(a) **Additive identity.** $(x_1, x_2, x_3) = (0, 0, 0)$ trivially satisfies $x_1 x_2 x_3 = 0$, thus $0 \in U$.

(b) **Closed under addition.** Consider the vector $u = (0, x_2, x_3)$ and $v = (x_1, x_2, 0)$ with $x_1, x_2, x_3 \neq 0$. Clearly $u, v \in U$; however, $u + v = (x_1, x_2, x_3)$ and $x_1 x_2 x_3 \neq 0$. Therefore $u + v \notin U$.

Because it is not closed under addition, we are done. □

(iii) Consider the subspace

$$U = \left\{ \begin{pmatrix} x \\ x \\ y \end{pmatrix} : x, y \in \mathbb{F} \right\} \leq \mathbb{F}^3.$$

Find another subspace $W \leq \mathbb{F}^3$ such that $\mathbb{F}^3 = U \oplus W$.

Solution. Any vector in U must be of the form

$$\begin{pmatrix} x \\ x \\ y \end{pmatrix} = x \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + y \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}. \tag{23}$$

Clearly, this does not reach the full space. The first vector in this column picture fixes the first and second entries to the be equal. A decent guess, then, is to consider all vectors with the first entries being opposites. Let's consider the subspace

$$W = \left\{ \begin{pmatrix} t \\ -t \\ 0 \end{pmatrix} : t \in \mathbb{F} \right\} \leq \mathbb{F}^3. \tag{24}$$

To show that it is a direct sum, we must first show that an arbitrary vector in $\mathbb{F}^3$ can be written as a sum of a vector in U and a vector in W. We must then show that this sum is unique. Let $a, b, c \in \mathbb{F}$. Then, we need

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} x \\ x \\ y \end{pmatrix} + \begin{pmatrix} t \\ -t \\ 0 \end{pmatrix} = \begin{pmatrix} x+t \\ x-t \\ y \end{pmatrix}. \tag{25}$$

For this to be true, we need

$$a = x + t, \tag{26}$$
$$b = x - t, \tag{27}$$
$$c = y. \tag{28}$$

We can solve for either x or t to find

$$x = \frac{a+b}{2} \quad \text{and} \quad t = \frac{a-b}{2}. \tag{29}$$

In other words, letting $v \in \mathbb{F}^3$ be arbitrary, we may always write $v = u + w$, where

$$u = \begin{pmatrix} \frac{a+b}{2} \\ \frac{a+b}{2} \\ c \end{pmatrix} \in U \quad \text{and} \quad w = \begin{pmatrix} \frac{a-b}{2} \\ \frac{-a+b}{2} \\ 0 \end{pmatrix} \in W. \tag{30}$$

Now, to show that this decomposition is unique, we will utilize Lemma 1.46 (direct sum of two subspaces) on page 23 of the fourth edition of Axler. This lemma tells us that a sum of subspaces $U + W$ is a direct sum if and only if $U \cap W = \{0\}$. Consider an arbitrary $u \in U \cap W$. By definition of the intersection, we must have $u \in U$ and $u \in W$. Thus, u must be able to be written as

$$u = \begin{pmatrix} x \\ x \\ y \end{pmatrix} \in U \quad \text{and} \quad u = \begin{pmatrix} t \\ -t \\ 0 \end{pmatrix} \in W. \tag{31}$$

For this to be true, we must have $y = 0$, $x = t$, and $x = -t$. However, this can only hold if $x = t = 0$. Thus, the only vector that is in both subspaces is the zero vector, and we are done.