PAWS 2026: QUATERNION ALGEBRAS
PROBLEM SET 0

MATT BROE, DIVYASREE C-RAMACHANDRAN, XINYU FANG, ALEXANDER WANG

Welcome to PAWS! Below are the exercises for Problem Set 0, which are intended to provide some background on common vocabulary and concepts that will be used in this course.

You are absolutely not obligated (or expected) to finish all of these problems before our first meeting, but we recommend that you at least attempt the problems if you have not seen the material before. Most importantly, work on the problems that interest you!

(1) In this exercise we review basic properties of complex numbers.

Definition 1. The *complex numbers* are the elements of the set

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\},$$

where i is a symbol satisfying $i^2 = -1$. Addition and multiplication of complex numbers are defined via

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$
$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

(a) Write each of the following in the form $a + bi$:

$$(2 + 3i) + (4 - i), \qquad (2 + 3i)(4 - i), \qquad (1 + i)^4, \qquad i^{2026}.$$

(b) For $z = a + bi$, define its *complex conjugate* by $\overline{z} = a - bi$. Show that

$$z\overline{z} = a^2 + b^2.$$

Use this identity to write the following complex numbers in the form $a + bi$:

$$1/(3 + 4i), \qquad (3 + i)/(1 - i).$$

(c) For $z = a + bi \in \mathbb{C}$, define the matrix

$$M_z = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in M_2(\mathbb{R}).$$

Compute M_i and M_{2+3i}. Then verify that, for all $z, w \in \mathbb{C}$,

$$M_{z+w} = M_z + M_w \qquad \text{and} \qquad M_{zw} = M_z M_w.$$

(2) In this exercise, we define fields, and study some examples of fields.

Definition 2. A *field* is a commutative ring F with $1 \neq 0$ in which every nonzero element has a multiplicative inverse: for every $a \in F$ with $a \neq 0$, there is an element $a^{-1} \in F$ such that

$$aa^{-1} = a^{-1}a = 1.$$

Definition 3. A *field extension* K/F is an injective ring homomorphism $F \hookrightarrow K$, where K and F are fields.

(a) Decide which of the rings

$$\begin{aligned} &\mathbb{Z} \text{ (the integers)},\\ &\mathbb{Q} \text{ (the rational numbers)},\\ &\mathbb{R} \text{ (the real numbers)},\\ &\mathbb{C} \text{ (the complex numbers)} \end{aligned}$$

are fields. Explain why any example that is not a field fails to be one.

(b) Let

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}.$$

Express

$$(1+\sqrt{2}) + (3-2\sqrt{2}) \qquad \text{and} \qquad (1+\sqrt{2})(3-2\sqrt{2})$$

in the form $a + b\sqrt{2}$, with $a, b \in \mathbb{Q}$. More generally, show that the sum and product of two elements of $\mathbb{Q}(\sqrt{2})$ again belong to $\mathbb{Q}(\sqrt{2})$.

(c) Let $x = a + b\sqrt{2}$, and assume x is not zero. Show that $a^2 - 2b^2 \neq 0$ and that

$$x^{-1} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}.$$

Conclude that $\mathbb{Q}(\sqrt{2})$ is a field. Compute $(1+\sqrt{2})^{-1}$ in the form $a + b\sqrt{2}$.

(d) Show that every element of $\mathbb{Q}(\sqrt{2})$ can be written *uniquely* as $a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$. You may use the fact that $\sqrt{2} \notin \mathbb{Q}$.

(3) In this exercise, we review the notion of a vector space and some properties associated to them.

Definition 4. A *vector space* over a field F is a set V together with an operation $V \times V \to V$ (called *vector addition*) and an operation $V \times F \to V$ (called *scalar multiplication*), satisfying the following properties:

- $(V, +)$ forms an abelian group,
- $a(bv) = (ab)v$ for all $a, b \in F$ and $v \in V$,
- $a(u + v) = au + av$ and $(a + b)v = av + bv$ for all $a, b \in F$ and $u, v \in V$,
- $1v = v$.

In a first course in linear algebra, we often assume that $F = \mathbb{R}$. However, all of the definitions still work if we replace $\mathbb{R}$ with an arbitrary field! We will explore that in this exercise.

(a) If L/K is a field extension, show that L is a vector space over K.

(b) Let $[L : K]$ denote the dimension of L as a K-vector space. What is $[\mathbb{C} : \mathbb{R}]$? What is $[\mathbb{C} : \mathbb{Q}]$?

(c) Recall that for a F-vector space V, a set of elements $\{v_1, \dots, v_n\}$ are said to be *linearly independent* if

$$c_1 v_1 + \cdots + c_n v_n = 0 \implies c_1 = \cdots = c_n = 0$$

for elements $c_1, \dots, c_n \in F$. Show that inside the $\mathbb{Q}$-vector space $\mathbb{R}$, the elements $\sqrt{2}$ and $\sqrt{3}$ are linearly independent.

(d) Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Recall that this is the smallest field extension of $\mathbb{Q}$ which contains both a square root of 2 and a square root of 3.

(i) Show that $\sqrt{6} \in L$.

(ii) Show that $\sqrt{6}$ cannot be written as a $\mathbb{Q}$-linear combination of $\{1, \sqrt{2}, \sqrt{3}\}$. Conclude that the set $\{1, \sqrt{2}, \sqrt{3}\}$ does not span L as a $\mathbb{Q}$-vector space.

(iii) Assume that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, that is, we cannot write $\sqrt{3} = a + b\sqrt{2}$ for $a, b \in \mathbb{Q}$. Show that the set $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is linearly independent in L as a $\mathbb{Q}$-vector space. (Hint: Suppose $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0$. Rewrite this as $(a + b\sqrt{2}) + (c + d\sqrt{2})\sqrt{3} = 0$ and solve for $\sqrt{3}$.)

(iv) Assume that $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{3})$. Show that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ spans L, and is in fact a basis for L as a $\mathbb{Q}$-vector space. Conclude that $[L : \mathbb{Q}] = 4$.

(4) In this exercise, we review some basic notions about rings. All rings are assumed to have an identity, and all ring homomorphisms are assumed to preserve the identity. Rings are not necessarily commutative unless explicitly stated otherwise.

Definition 5. A subset $I \subseteq R$ is a *left ideal* (resp. *right ideal*) if it is an additive subgroup of R and $ri \in I$ (resp. $ir \in I$) for all $r \in R$ and $i \in I$. A *two-sided ideal* is both a left and a right ideal.

Definition 6. The *center* of a ring R is

$$Z(R) = \{z \in R : zr = rz \text{ for every } r \in R\}.$$

(a) Consider the map

$$\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}/6\mathbb{Z},$$
$$n \longmapsto \overline{n}.$$

(i) Show that φ is a ring homomorphism.

(ii) What is its kernel? Recall that

$$\ker(\varphi) = \{n \in \mathbb{Z} : \varphi(n) = \overline{0}\}.$$

(iii) Is $\ker(\varphi)$ an ideal of $\mathbb{Z}$?

(b) Consider the ring $R = M_2(\mathbb{R})$ and let

$$I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{R} \right\}.$$

(i) Show that I is a left ideal of R but not a right ideal.

(ii) Show that the center of R is

$$Z(R) = \{\lambda I_2 : \lambda \in \mathbb{R}\}.$$

(iii) Is R commutative? What about $Z(R)$?.

(5) In this exercise, we review the concept of an algebra over a field F.

Definition 7. An *algebra over a field* F (also referred to as a F*-algebra*) is a ring A together with a ring homomorphism $f : F \to A$ such that the subring $f(F)$ is contained in the center of A.

Definition 8. A F*-algebra homomorphism* (or *isomorphism*) between two F-algebras A and B is a ring homomorphism (isomorphism, respectively)

$$\varphi\colon A \longrightarrow B$$

such that

$$\varphi(c \cdot a) = c \cdot \varphi(a)$$

for all $c \in F$ and $a \in A$.

(a) Show that an algebra over F can be equivalently defined as a ring A containing the field F in its center and whose identity is the same as the identity of F.

(b) Verify that A has the structure of a vector space over F with scalar multiplication given by

$$c \cdot a = ca \in A$$

for all $c \in F$ and $a \in A$. (The *dimension* of A over F is its dimension as a F-vector space.)

(c) Verify that A has the structure of a vector space over F with scalar multiplication given by

$$c \cdot a = ac \in A$$

for all $c \in F$ and $a \in A$.

(d) Let $A = \mathbb{C} \times \mathbb{C}$ be the direct product ring (cf. [1, §7.6]). Give A a structure of an algebra over $\mathbb{C}$. Also show that it cannot be made into an algebra over either of the direct copies of $\mathbb{C}$ (e.g., via $i_1 : \mathbb{C} \to \mathbb{C} \times \mathbb{C},\ x \mapsto (x, 0)$).

(6) In this exercise, we will work through a very important example of a F-algebra.

Let $A = M_2(F)$ be the ring of 2×2 matrices with entries in F. (Feel free to take $F = \mathbb{C}$ or $\mathbb{R}$.)

(a) Show that A is an algebra over F.

(b) A *left (resp. right, two-sided) ideal* of A is a left (resp. right, two-sided) ideal of A as a ring. Describe all left and right ideals of A. (*Hint:* What do you notice about the row space of elements in a left ideal?)

(c) Show that A is *simple*, i.e., it has no nontrivial proper two-sided ideals.

(7) In this exercise, we review some basic properties of finite fields.

A *finite field* is a field with finitely many elements. For a prime number p, we write $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. More generally, for every integer $n > 0$, there is, up to isomorphism, a unique finite field with p^n elements, denoted by $\mathbb{F}_{p^n}$.

(a) What are the elements of $\mathbb{F}_p$?

(b) Find the multiplicative inverse of each nonzero element of $\mathbb{F}_3$.

(c) Consider the polynomial

$$f(x) = x^2 + 1 \in \mathbb{F}_3[x].$$

Does f have a root in $\mathbb{F}_3$? What is the smallest field containing $\mathbb{F}_3$ and a root of f? How many elements does this field have?

References

[1] David S. Dummit and Richard M. Foote, *Abstract Algebra*, 2nd ed., Prentice Hall, 1999.