PAWS 2026: QUATERNION ALGEBRAS
PROBLEM SET 5

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

We have reached our final problem set! This time, we will explore a few more interesting properties of p-adic fields and quaternion algebras over $\mathbb{Q}$.

Although we won't have a problem discussion session for this set, please feel free to post your questions, comments, and suggestions on Discord. We would be very happy to help!

(1) Let p and q be distinct primes. We will show that $\mathbb{Q}_p$ and $\mathbb{Q}_q$ are different as topological fields over $\mathbb{Q}$.
   (a) Recall that the p-adic valuation of p, $|p|_p = p^{-1}$. Show that the sequence $(p^n)_{n\geq 1}$ converges to 0 in $\mathbb{Q}_p$.
   (b) Show that the same sequence does not converge to 0 in $\mathbb{Q}_q$.
   (c) Deduce that the p-adic and q-adic topologies on $\mathbb{Q}$ are different, and hence that their completions $\mathbb{Q}_p$ and $\mathbb{Q}_q$ are not isomorphic as topological fields over $\mathbb{Q}$.

(2) In the notes, we show that for an odd prime p, the group $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Here, we show that for the 2-adic numbers, the group of square classes is slightly different.
   (a) Let $u \in \mathbb{Z}_2^\times$. Show that $u^2 \equiv 1 \pmod 8$.
   (b) Now suppose that $u \in \mathbb{Z}_2^\times$ satisfies $u^2 \equiv 1 \pmod 8$. Using induction, prove that for all n, there exists $x_n \in \mathbb{Z}/2^n\mathbb{Z}$ such that $x_{n+1} \equiv x_n \pmod{2^n}$ and $x_n^2 \equiv u \pmod{2^n}$.
      (i) **Base Case:** ($n \leq 3$) Find x_1, x_2, and x_3 such that $x_1 \equiv x_2 \pmod 2$, $x_2 \equiv x_3 \pmod 4$, and $x_i^2 \equiv u \pmod{2^i}$ for $i \in \{1,2,3\}$.
      (ii) **Inductive Step:** Suppose there exists $x_1, \ldots, x_n$ satisfying the inductive hypotheses. Then, write $x_{n+1} = x_n + c\cdot 2^n$ for $c \in \{0,1\}$. Since $x_n^2 \equiv u \pmod{2^n}$, we must have that $x_n^2 - u = k\cdot 2^n$ for some integer k. Show that c is always uniquely determined by k, so we can produce a x_{n+1} satisfying the inductive hypotheses. (Hint: Examine the equation $x_{n+1}^2 \equiv u \pmod{2^{n+1}}$, substituting $x_{n+1} = x_n + c\cdot 2^n$ and $x_n^2 = u + k\cdot 2^n$ when possible.) Note that this proof should use the fact that $n \geq 3$.
   (c) Conclude that $u \in \mathbb{Z}_2^\times$ is a square if and only if $u \equiv 1 \pmod 8$. What does the group of square classes in $\mathbb{Z}_2^\times$ look like?
   (d) Using the result of the previous part, and following the argument of Theorem 5.6 from the notes, show that $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^3$.

(3) Let $a, b \in \mathbb{Q}^\times$. Recall that the Hilbert symbol $(a,b)_v$ is $+1$ if the quaternion algebra $(a,b)_{\mathbb{Q}_v}$ splits and -1 otherwise, where $\mathbb{Q}_\infty = \mathbb{R}$. We will use the following important result, known as the *Hilbert reciprocity law*:

$$\prod_v (a,b)_v = 1,$$

where the product runs over all primes p, together with the real place $v = \infty$.
   (a) Following the computation of $(3,5)_v$ in the lecture notes, determine the Hilbert symbols

$$(-1,3)_\infty, \qquad (-1,3)_2, \qquad (-1,3)_p$$

   for every odd prime p. In particular, identify all the places where $(-1,3)$ is a division algebra.
   (b) Show that for fixed $a, b \in \mathbb{Q}^\times$, $(a,b)_p = 1$ for all but finitely many primes p.

(c) Recall the criterion for $(a,b)_{\mathbb{R}}$ to be split. Determine when $(a,b)_\infty = -1$.

(d) Suppose that $(a,b)_\infty = -1$. What can you conclude about the number of primes p for which $(a,b)_p = -1$? Justify your answer using Hilbert reciprocity.

(4) Fix a prime $p \equiv 3 \pmod 4$ and let $A = (-1,p)_{\mathbb{Q}_p}$. Recall that A is split if and only if $-X^2+pY^2 = 1$ has a solution with $X, Y \in \mathbb{Q}_p$. We saw in Problem Set 3 that A is a division algebra. We now show that A is split by *every* quadratic extension of $\mathbb{Q}_p$.

(a) Use the fact that $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 = \{1,-1,p,-p\}$, to conclude that $\mathbb{Q}_p$ has exactly three quadratic extensions:

$$K_1 = \mathbb{Q}_p(i), \qquad K_2 = \mathbb{Q}_p(\sqrt{p}), \qquad K_3 = \mathbb{Q}_p(\sqrt{-p}).$$

(b) Write down explicit solutions of $-X^2 + pY^2 = 1$ over K_1 and over K_2.

(c) Show that

$$x_0^2 + y_0^2 = -1$$

has a solution with $x_0, y_0 \in \mathbb{F}_p$.
You may use the following fact: if $x_0, y_0 \in \mathbb{F}_p$ satisfy the above equation, then there exist $x, y \in \mathbb{Z}_p$ reducing to x_0, y_0 modulo p, respectively, such that

$$x^2 + y^2 = -1.$$

(d) Let x_1, y_1 be as above and set

$$X = x_1, \qquad Y = \frac{y_1}{\sqrt{-p}} \in K_3.$$

Verify that $-X^2 + pY^2 = 1$, so A splits over K_3 as well.

(e) Conclude that every quadratic extension of $\mathbb{Q}_p$ splits A, even though A is a division algebra.

(5) In this exercise, we use local Hilbert symbols to distinguish quaternion algebras over $\mathbb{Q}$.
Consider

$$A = (2,3)_{\mathbb{Q}}, \qquad B = (2,5)_{\mathbb{Q}}, \qquad C = (3,7)_{\mathbb{Q}}.$$

(a) For each pair among A, B, C, find an odd prime p such that one of the two algebras splits over $\mathbb{Q}_p$ and the other does not. Hint: use Theorem 5.3 from the lecture notes.

(b) Use Lemma 5.15 to conclude that A, B, C are pairwise nonisomorphic over $\mathbb{Q}$.

(6) Let

$$A = (3,13)_{\mathbb{Q}}.$$

(a) Show that

$$(3,13)_\ell = 1$$

for every odd prime $\ell \notin \{3, 13\}$.

(b) Compute

$$(3,13)_3 \qquad \text{and} \qquad (3,13)_{13}.$$

(c) Compute $(3,13)_\infty$, and use Hilbert reciprocity to determine $(3,13)_2$.

(d) Use the Hasse–Minkowski theorem to conclude that A is split over $\mathbb{Q}$.

(e) Find a rational point on

$$3X^2 + 13Y^2 = 1.$$

Hint: Try $X = Y$.