CLASSIFICATION OF QUATERNION ALGEBRAS OVER $\mathbb{Q}$

RAYMOND FRIEND

Abstract. Quaternion algebras over any field can be classified into two types: trivial matrix algebras, or division algebras. When we consider our field as $\mathbb{Q}$, we notice an infinite number of non-isomorphic quaternion division algebras, unlike its completion: $\mathbb{R}$, which has only two quaternion algebra isomorphism classes.

Contents

1. Introduction 1
2. The Quaternions 1
3. Isomorphisms and Splitting 3
4. Comparing Rational and Real Division Rings 6
References 8

1. Introduction

A complex number is a sum $a+bi$, where $a, b \in \mathbb{R}$ and $i^2 = -1$. These numbers are useful for calculations in $\mathbb{R}^2$ and as a completion of $\mathbb{R}$ algebraically. In the early 19th century, William Hamilton wished to express multiplication in higher dimensions; namely, in $\mathbb{R}^3$. He found a way to do so using not just one more imaginary unit, but two, birthing what are now known as the Quaternions.

We can extend the notion of Quaternions past being over the natural field $\mathbb{R}$, but some general field, F. And rather than require the imaginary units i, j each be square roots of -1, we may allow each to be square roots of any nonzero element of the field F. Generalizing in this way allows us to analyze general properties of quaternion algebras over any field. One important task when considering all quaternion algebras is determining which algebras are division rings. Division rings have the useful property that unique division operations may occur in the algebra.

The classification of quaternion algebras over $\mathbb{R}$ and $\mathbb{Q}$ differ greatly: while $\mathbb{R}$ only possesses two distinct quaternion algebras up to isomorphism, $\mathbb{Q}$ possesses an infinite amount.

2. The Quaternions

Definition 2.1 (Hamilton's Quaternions)**.** *Hamilton's quaternions* are

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\},$$

where the following multiplication conditions are imposed:

Date: December 12, 2016.

- $i^2 = j^2 = k^2 = -1$
- $ij = k, ji = -k, jk = i, kj = -i, ki = j, ik = -j$
- $\forall a \in \mathbb{R}, a$ commutes with i, j, and k.

Despite $\mathbb{H}$ being even more general than $\mathbb{R}$ and $\mathbb{C}$, we can generalize the quaternion structure over other fields. Let F be a field of characteristic $\neq 2$. This condition is important because a natural implication of $\text{char}(F) = 2$ is $1 = -1$, an undesirable, defective property. A *quaternion algebra over* F is an algebra A over F satisfying the following conditions:

- (Simple) its *radical* R is trivial,
- (Central) its *center* $Z = \{x \in A \mid xy = yx \text{ for all } y \in A\} = F$,
- $\dim_F(A) = 4$.

Define a *quaternion basis* $\{1, u, v, w\}$ as following the multiplicative relations: $u^2, v^2 \in F^\times, w = uv = -vu$, and every $c \in F$ commutes with u and v. If $u^2 = a$ and $v^2 = b$, then denote the ring algebra $(a, b)_F := F + Fu + Fv + Fw$. The multiplicative rules on u, v, and w are consistent with the axioms of a ring because we can realize the operations in $(a, b)_F$ as addition and multiplication of certain 2×2 matrices.

Each quaternion algebra over fixed field F is isomorphic to some algebra $(a, b)_F$. In particular, Hamilton's Quaternions $\mathbb{H} = (-1, -1)_\mathbb{R}$, and the matrix algebra $M_2(F) \cong (1, 1)_F$.

We may define the *conjugate* and *norm* of an element $q = x_0 + x_1u + x_2v + x_3w \in (a, b)_F$.

Definition 2.2. The *conjugate*, or *standard involution* in A, $\overline{q}$, of q is

$$\overline{q} = x_0 - x_1u - x_2v - x_3w.$$

These properties of conjugation are straightforward to derive:

$$\overline{q_1 + q_2} = \overline{q_1} + \overline{q_2},$$

$$\overline{\overline{q}} = q,$$

$$\overline{cq} = c\overline{q} \text{ for } c \in F,$$

$$\overline{q} = q \Leftrightarrow q \in F.$$

Definition 2.3. The *norm*, $N(q)$, of q is

$$N(q) = q\overline{q} = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2.$$

As with $\mathbb{H}$, $\overline{q}q = q\overline{q}$ in $(a, b)_F$, which may be checked by direct calculation. Thus, the norm is a multiplicative function $N : (a, b)_F \to F$. Since $\text{char}(F) \neq 2$, $(a, b)_F$ is noncommutative because u and v don't commute. We call a quaternion algebra A a *division algebra*, *division ring*, or *skew field*, if the two equations for given $a, b \neq 0 \in A$ are uniquely solvable for certain $x, y \in A$:

$$bx = a,$$

$$yb = a.$$

Remark 2.4. Along with the fact that each quaternion algebra is over a field F with multiplicative identity 1, we can establish some equivalent definitions of a division algebra.

- Each element has a two-sided inverse:
$$\forall\ q \in A, \exists\ q^{-1} \in A \text{ such that } qq^{-1} = q^{-1}q = 1,$$
- Only 0 has 0 norm:
$$N(q) = 0 \Rightarrow q = 0,$$
- No nontrivial zero divisors:
$$\text{For } p, q \in A,\ pq = 0 \Rightarrow p = 0 \text{ or } q = 0.$$

For example, below is a proof of the equivalence between the first and second conditions.

Proof. Given $q \in A^\times$, suppose $qq' = 1$ for some $q' \in A$. Then $N(q)N(q') = N(1) = 1$ in F by multiplicativity of N, so $N(q) \in F^\times$. Conversely, suppose $N(q) \in F^\times$. Since $N(q)$ commutes with all elements of $(a, b)_F$, the equation $N(q) = q\overline{q} = \overline{q}q$ can be written as
$$q \cdot \frac{1}{N(q)}\overline{q} = \frac{1}{N(q)}\overline{q} \cdot q = 1,$$
so $\overline{q}/N(q)$ is a 2-sided inverse of q. □

3. Isomorphisms and Splitting

An *isomorphism* between two quaternion algebras A and A' over a field F is a ring isomorphism $f : A \to A'$ that fixes the elements of F. Considering bases to these vector spaces helps to determine whether two quaternion algebras are isomorphic.

Definition 3.1. A basis of $(a, b)_F$ having the form $\{1, e_1, e_2, e_3\}$ where $e_1^2, e_2^2 \in F^\times$, and $e_1e_2 = -e_2e_1$ is called a *quaternionic basis* of $(a, b)_F$.

The defining basis $\{1, u, v, w\}$ of $(a, b)_F$ is a quaternionic basis. In any quaternionic basis, the three elements e_1, e_2, e_1e_2 anti-commute, and $(e_1e_2)^2 = -e_1^2e_2^2$. We can derive some basic isomorphisms between quaternion algebras by clever choices of bases:

(1) $\{1, v, u, vu\}$ is a quaternionic basis of $(a, b)_F$, so $(a, b)_F \cong (b, a)_F$,
(2) $\{1, u, w, uw\}$ is a quaternionic basis of $(a, b)_F$, so $(a, b)_F \cong (a, -ab)_F$,
(3) $\{1, v, w, vw\}$ is a quaternionic basis of $(a, b)_F$, so $(a, b)_F \cong (b, -ab)_F$,
(4) $\{1, cu, dv, (cu)(dv)\}$ is a quaternionic basis of $(a, b)_F$ for all $c, d \in F^\times$, so $(a, b)_F \cong \left(ac^2, bd^2\right)_F$.

Theorem 3.2. *For all $a \in F^\times$, $(a, 1)_F \cong M_2(F)$.*

Once proven, this theorem implies
$$\left(a, c^2\right)_F \cong (a, -a)_F \cong (a, 1)_F \cong M_2(F)$$

Proof. Send the basis $1, u, v, w$ of $(a, 1)_F$ to $M_2(F)$ as follows:
$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, u \mapsto \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}, v \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, w \mapsto \begin{pmatrix} 0 & -1 \\ a & 0 \end{pmatrix}.$$
Since $1 \neq -1$ in F, 1 and v are not sent to the same matrix. Extend this mapping by F-linearity to a function $f : (a, 1)_F \to M_2(F)$:
$$f : x_0 + x_1u + x_2v + x_3w \mapsto \begin{pmatrix} x_0 + x_2 & x_1 - x_3 \\ a(x_1 + x_3) & x_0 - x_2 \end{pmatrix}.$$

The image of $1, u, v, w$ in $M_2(F)$ is a linearly independent set, so by a dimension count this F-linear mapping $(a,1)_F \to M_2(F)$ is a bijection. Scalar $c \in F$ maps to $cI_2 \in M_2(F)$, so F is fixed point-wise. For completeness, f can be checked by direct calculation to preserve multiplication as a homomorphism. □

Definition 3.3. We call any quaternion algebra isomorphic to $M_2(F)$, including $M_2(F)$ itself, a *trivial*, or *split*, quaternion algebra over F. If $(a,b)_F \ncong M_2(F)$, we say $(a,b)_F$ is a *non-split* quaternion algebra over F.

Definition 3.4. More generally, for a field extension $F \subset K$ and $a, b \in F^\times$, we say $(a,b)_F$ splits over K when $(a,b)_K \cong M_2(K)$.

In the classification of quaternion algebras, we wish to know whether or not $(a,b)_F \cong M_2(F)$. There are a few conditions essential to answering this question.

Lemma 3.5. *For $a \in F^\times$, the set of nonzero $x^2 - ay^2$ with $x, y \in F$ is a subgroup of $F^\times$.*

Proof. The number 1 has this form ($x = 1, y = 0$). Numbers of this form are closed under multiplication since

$$(x_1^2 - ay_1^2)(x_2^2 - ay_2^2) = (x_1x_2 + ay_1y_2)^2 - a(x_1y_2 + x_2y_1)^2.$$

Nonzero numbers of this form are closed under inversion using the identity: $1/t = t/t^2$:

$$\frac{1}{x^2 - ay^2} = \frac{(x^2 - ay^2)^2}{x^2 - ay^2} = \left(\frac{x}{x^2 - ay^2}\right)^2 - a\left(\frac{y}{x^2 - ay^2}\right)^2.$$

□

Definition 3.6 (Norm Subgroup)**.** For $a \in F^\times$, let $N_a = N_a(F)$ be the set of all nonzero $x^2 - ay^2$ where $x, y \in F$.

By Lemma 3.5, $N_a < F^\times$, and the field squared: $(F^\times)^2 \subset N_a$ using $y = 0$.

Theorem 3.7. *If a is a square in F, then $N_a = F^\times$.*

Proof. Write $a = c^2$ for some $c \in F^\times$. Then $x^2 - ay^2 = x^2 - c^2y^2 = x^2 - (cy)^2 = (x - cy)(x + cy)$. The change of variables $x' = x - cy$ and $y' = x + cy$ is invertible by $\mathrm{char}(F) = 2$ ($x = (x' + y')/2$, and $y = (y' - x')/(2c)$), so $N_a = \{x'y' : x', y' \in F^\times\}$, which assumes all values in $F^\times$ by choosing $y' = 1$. □

Remark 3.8. The converse of Theorem 3.7 is generally false: N_a could be $F^\times$ without a being a square in F.

Theorem 3.9. *If $b \in N_a$, then $(a,b)_F \cong M_2(F)$.*

Proof. Write $b = x_0^2 - ay_0^2$ with x_0 and y_0 in F. The ring $(a,b)_F$ has a quaternionic basis:

$$\{1, u, x_0v + y_0w, u(x_0v + y_0w)\}.$$

The fourth element is $x_0w + y_0av$ by the formulas for uv and uw. The change of base matrix from v, w to $x_0v + y_0w, ay_0v + x_0w$ has $\det \begin{pmatrix} x_0 & y_0 \\ ay_0 & x_0 \end{pmatrix} = b \neq 0$. Thus, the above set of four elements of $(a,b)_F$ is linearly independent over F, so it is a basis of $(a,b)_F$. This basis is quaternionic because $(x_0v + y_0w)^2 = bx_0^2 - aby_0^2 = b^2$, and u and $x_0v + y_0w$ anti-commute. Therefore, $b \in N_a \Rightarrow (a,b)_F \cong \left(a, b^2\right)_F \cong (a,1)_F \cong M_2(F)$. □

Example 3.10. When p is prime and $p = 2$ or $p \equiv 1 \pmod 4$, Fermat's two-square theorem says such a p is a sum of two squares in $\mathbb{Z}$. Therefore, $p \in N_{-1}(\mathbb{Q})$, meaning $(-1, p)_{\mathbb{Q}} \cong M_2(F)$.

Theorem 3.11. *A quaternion algebra $(a, b)_F$ that is not a division algebra is isomorphic to $M_2(F)$.*

Proof. Since we already know that $\left(c^2, b\right)_F \cong M_2(F)$, we can assume a is not a square in F. And since we assume F is not a division algebra, it must contain a nonzero element $q = x_0 + x_1u + x_2v + x_3w$ with $N(q) = 0$. Then

$$N(q) = 0 \Rightarrow x_0^2 - ax_1^2 - bx_2^2 + abx_3^2 = 0 \Rightarrow x_0^2 - ax_1^2 = b(x_2^2 - ax_3^2).$$

Since a is not a square in F, we must have $x_2^2 - ax_3^2 \neq 0$ by contradiction: if $x_2^2 - ax_3^2 = 0$, then $x_3 = 0$ since otherwise, we could solve for a to see it is a square in F, so also $x_2 = 0$. That implies $x_0^2 - ax_1^2 = 0$, so also $x_1 = 0$ and $x_0 = 0$, but then $q = 0$.

Solving for b,

$$b = \frac{x_0^2 - ax_1^2}{x_2^2 - ax_3^2} \in N_a,$$

so $(a, b)_F \cong M_2(F)$ by Theorem 3.9. □

Example 3.12. Let $A = (5, 11)_{\mathbb{Q}}$. Since for $h = 1 + 3u + v + w \neq 0$, $N(q) = 1^2 - (5) \cdot 3^2 - (11) \cdot 1^2 + (55) \cdot 1^2 = 0$, A is not a division algebra. Hence, by Theorem 3.11, $A \cong M_2(F)$.

Theorem 3.13 (Forward and Converse of Theorem 3.9)**.** *For a and b in $F^\times$, $(a, b)_F \cong M_2(F)$ if and only if $b \in N_a$.*

Proof. If $b \in N_a$, then $(a, b)_F \cong M_2(F)$ by Theorem 3.9. Conversely, suppose $(a, b)_F \cong M_2(F)$. To show $b \in N_a$, we can assume a is not a square in $F^\times$, since if a were a square then $N_a = F^\times$ by Theorem 3.7, so obviously $b \in N_a$. When $(a, b)_F$ is not a division ring and a is not a square, the proof of Theorem 3.11 shows $b \in N_a$. □

Corollary 3.14. *If F is an algebraically closed field, then for any $a, b \in F^\times$, $(a, b)_F \cong M_2(F)$.*

Example 3.15. The real, complex field $\mathbb{C}$ is algebraically closed (every element has a square root within $\mathbb{C}$), so any $(a, b)_{\mathbb{C}} \cong M_2(\mathbb{C})$.

We now can conclude that for some field F of characteristic $\neq 2$, $(a, b)_F$ being non-split is equivalent to being a division ring. And $(a, b)_F$ being split is equivalent to $b \in N_a$.

Theorem 3.16. *For $a, b \in F^\times$, the following conditions are equivalent for a split algebra:*

(1) $(a, b)_F \cong M_2(F)$,
(2) the equation $ax^2 + by^2 = 1$ has a solution (x, y) in F,
(3) the equation $ax^2 + by^2 = z^2$ has a solution (x, y, z) in F other than $(0, 0, 0)$.

The negation of each condition give us equivalent conditions for being a non-split quaternion algebra.

Theorem 3.13 equivalently says $(a, b)_F \cong (a, 1)_F$ if and only if $b \in N_a$. This statement may be generalized in the following theorem.

Theorem 3.17. *For $a, b, b' \in F^\times$, $(a,b)_F \cong (a,b')_F$ if and only if $b/b' \in N_a$.*

Proof. The backwards direction is simpler to perform first. Suppose $b/b' = x_0^2 - ay_0^2$ for some $x_0, y_0 \in F$. Let $\{1, u, v, uv\}$ be the quaternionic basis of $(a,b')_F$. We have that the same basis from Theorem 3.9: $\{1, u, x_0v + y_0w, u(x_0v + y_0w)\}$, is linearly independent, and is also a quaternionic basis of $(a,b')_F$. Here, $u^2 = a$ and $(x_0v + y_0w)^2 = b'x_0^2 - ab'y_0^2 = b'(b/b') = b$. Thus, $(a,b)_F \cong (a,b')_F$.

Conversely, we assume $(a,b)_F \cong (a,b')_F$. Either both are division rings or both are not division rings.

First suppose $(a,b)_F$ and $(a,b')_F$ are not division rings. Both are isomorphic to $M_2(F)$, so $b \in N_a$ and $b' \in N_a$ by Theorem 3.13. Since $N_a < F^\times$, $b/b' \in N_a$ by closure.

Finally, suppose $(a,b)_F$ and $(a,b')_F$ are division rings, implying a is not a square in F. With the same standard basis $\{1, u, v, uv\}$ of $(a,b')_F$, our initial assumption gives that $(a,b')_F$ contains another quaternionic basis $\{1, u_0, v_0, u_0v_0\}$, where

$$u_0^2 = a, v_0^2 = b, u_0v_0 = -v_0u_0.$$

The polynomial $T^2 - a$ is irreducible over F since a is not a square in F, and both u and u_0 are roots of this polynomial in $(a,b')_F$. By a theorem proved in [3] (Theorem 16.8), $u = qu_0q^{-1}$ for some nonzero $q \in (a,b)_F$. Set $\widetilde{v} = qv_0q^{-1}$, so $\widetilde{v}^2 = (qv_0q^{-1})(qv_0q^{-1}) = qv_0^2q^{-1} = qbq^{-1} = b$. Then

$$u_0v_0 = -v_0u_0 \Rightarrow (qu_0q^{-1})(qv_0q^{-1}) = -(qv_0q^{-1})(q0_0q^{-1}) \Rightarrow u\widetilde{v} = -\widetilde{v}u.$$

The elements of $(a,b')_F$ that anti-commute with u are $Fv + Fw$, so $\widetilde{v} = xv + yw$ for some $x, y \in F$. Then

$$b = \widetilde{v}^2 = (xv + yw)^2 = b'x^2 - b'ay^2 = b'(x^2 - ay^2) \Rightarrow \frac{b}{b'} \in N_a.$$

□

4. Comparing Rational and Real Division Rings

It turns out that classifying the quaternion algebras over $\mathbb{R}$ is much easier than doing so over $\mathbb{Q} < \mathbb{R}$. In fact,

Theorem 4.1. *For field $\mathbb{R}$, there are only two isomorphism classes for quaternion algebras:*

$$(a,b)_{\mathbb{R}} \cong \begin{cases} \mathbb{H} & \text{if } a < 0 \text{ and } b < 0, \\ M_2(\mathbb{R}) & \text{if } a > 0 \text{ or } b > 0. \end{cases}$$

Proof. Assume $a > 0$ and $b \in \mathbb{R}^\times$. (We see that because $(a,b)_F \cong (b,a)_F$, the roles of a and b are interchangeable and thus it is sufficient to only consider this case when at least one of a and b are positive). Because a is positive, $a = c^2$ for some $c \in \mathbb{R}$. Then, by Theorem 3.2, $(a,b)_{\mathbb{R}} \cong \left(c^2, b\right)_{\mathbb{R}} \cong (1,b)_{\mathbb{R}} \cong M_2(\mathbb{R})$.

Now assume both $a, b < 0$. Recall that one property of the quaternion algebra $(a,b)_F$ by definition is that center$(a,b)_F = F$. In [3] (pp. 219-220), a theorem of Frobenius states that any division ring with center $\mathbb{R}$ that is finite-dimensional as a vector space over $\mathbb{R}$ is isomorphic to either $\mathbb{R}$ or $\mathbb{H}$.

Now notice that $\nexists\, c \in \mathbb{R}$ such that $c^2 = a$. Thus, we must introduce another vector $u \in (a,b)_{\mathbb{R}} \backslash \mathbb{R}$ to complete $\mathbb{R}$ algebraically, where $u^2 = a$. Thus, $\dim (a,b)_{\mathbb{R}} > 1$, and by the Frobenius' theorem, $(a,b)_{\mathbb{R}} \cong \mathbb{H}$. □

It is quite easy, then, to classify the quaternion algebras over $\mathbb{R}$. This is not the case for $\mathbb{Q}$, however.

Lemma 4.2. *There are infinitely many prime numbers p congruent to 3 mod 4.*

Proof. We first prove the claim that if $a \equiv 3 \pmod 4$, then $\exists$ prime p such that $p \mid a$ and $p \equiv 3 \pmod 4$. Clearly, all primes dividing such an a are odd. Suppose all such primes are congruent to 1 (mod 4). Then their product would also be $a \equiv 1$ (mod 4), a contradiction.

Now suppose a finite number of primes congruent to 3 mod 4, listed $p_1 = 3, p_2, ..., p_n$. Take $a = 4p_1p_2 \cdots p_n - 1$. We see that $p_i \nmid a$ for all $i = 1, ..., n$, since each $p_i \mid 4p_1p_2 \cdots p_n$, and each $p_i \geq 3$. By the previous claim, a must have a prime factor p such that $p \equiv 3 \pmod 4$: a contradiction to $p_i \nmid a$, since $p = p_i$ for some $1 \leq i \leq n$. Thus, there must be infinitely many primes congruent to 3 (mod 4). □

Theorem 4.3. *For distinct primes p and q that are 3 mod 4, $(-1, p)_{\mathbb{Q}}$ is not isomorphic to $(-1, q)_{\mathbb{Q}}$.*

Proof. If $(-1, p)_{\mathbb{Q}} \cong (-1, q)_{\mathbb{Q}}$, then $q/p \in N_{-1}(\mathbb{Q})$ by Theorem 3.17, so $q/p = x^2 + y^2$ for some rational numbers x, y. Write x and y with a common denominator $x = m/d, y = n/d$, with $m, n, d \in \mathbb{Z}$ and $d \neq 0$. Then

$$qd^2 = p\left(m^2 + n^2\right).$$

Since primes $p \neq q$, $m^2 + n^2 \equiv 0 \pmod q$. That implies m and n are divisible by q (because -1 is not a square mod q), so qd^2 is divisible by q^2, and thus $q \mid d$. In the equation $qd^2 = p(m^2 + n^2)$, the numbers m, n, d are all divisible by q, so we can divide through by q^2 and get a similar equation where m, n, and d are replaced by $m/q, n/q$, and d/q. Repeating this argument ad infinitum, d is divisible by arbitrarily high powers of q, a contradiction. □

Remark 4.4. By the infinitude of primes, p, congruent to 3 mod 4, each forming a quaternion algebra $(-1, p)_{\mathbb{Q}}$ not congruent to any other $(-1, q)_{\mathbb{Q}}$, there are infinitely many non-isomorphic quaternion algebras over $\mathbb{Q}$. In fact, since -1 is not a quadratic residue modulo p when $p \equiv 3 \pmod 4$, $(-1, p)_{\mathbb{Q}}$ is a division ring.

Now we can establish some conditions on $(a, b)_{\mathbb{Q}}$ to determine whether it is trivial, or if it is a division ring.

Theorem 4.5. *Let b be a prime number, and a be any quadratic non-residue mod b, i.e. $x^2 \equiv a \mod b$ has no solutions $\mathbb{Z}$. Then the algebra $A = (a, b)_{\mathbb{Q}}$ is a division algebra.*

Proof. Suppose A is not a division algebra, or, equivalently, $A \cong M_2(F)$. Then $\exists\ q \in A^\times$ with norm $N(q) = x_0 - ax_1^2 - bx_2^2 + abx_3^2 = 0$. We may assume that x_0, x_1, x_2, x_3 have no common factors, since any common factor d may be factored from each and preserve the equation for a new set of $x_i' = x_i/d$.

Considering this equation mod b, it follows that

$$x_0^2 \equiv ax_1^2 \pmod b.$$

If b does not divide x_1, then x_1^2 is a quadratic residue mod b, and a product of a quadratic residue and a quadratic non-residue is a quadratic non-residue, contradicting our congruence relation. Thus, $b \mid x_1$, and hence $b \mid x_0$, showing $x_2^2 \equiv ax_3^2$

(mod b). By the same argument, we have that $b \mid x_2$ and $b \mid x_3$, in contradiction with our assumption. □

Example 4.6. The rings $(2,3)_{\mathbb{Q}}$ and $(2,5)_{\mathbb{Q}}$ are division rings since 2 is not a quadratic residue modulo 3, nor modulo 5.

References

[1] K. Conrad. *Quaternion Algebras.*
[2] S. Katok. *Fuchsian Groups.* The University of Chicago Press. Chicago. 1992.
[3] T. Y. Lam. *A First Course in Noncommutative Rings.* Springer-Verlag. New York. 1991.