A SUBSTITUTE FOR WEDDERBURN’S THEOREM

Let \( p \neq 2 \) be an odd prime, \( \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \) the field of \( p \) elements, and
\[
W_p := \{a_0 \mathbf{1} + a_1 \mathbf{i} + a_2 \mathbf{j} + a_3 \mathbf{k} : a_r \in \mathbb{F}_p \}
\]
the quaternions over \( \mathbb{F}_p \), which is a 4-dimensional vector space over \( \mathbb{F}_p \) with basis \( \mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k} \), and multiplication uniquely defined by requiring \( \mathbb{F}_p \)-linearity, distributivity, associativity and
\[
i^2 = j^2 = -1, \quad i \cdot j = -j \cdot i = k, \quad j \cdot k = -k \cdot j = i
\]
so in particular \( k \cdot i = j \) because
\[
k \cdot i = (i \cdot j) \cdot i = (-j \cdot i) \cdot i = -j \cdot (i \cdot i) = -j \cdot -1 = j.
\]
This gives an associative but non-commutative ring, because \( i \cdot j = -j \cdot i \neq j \cdot i \) because \( p \neq 2 \) so that \(-1 \neq 1\). We define conjugate and norm as in the case of the standard Hamilton quaternions over \( \mathbb{R} \), by
\[
N(a_0 \mathbf{1} + a_1 \mathbf{i} + a_2 \mathbf{j} + a_3 \mathbf{k}) = a_0^2 + a_1^2 + a_2^2 + a_3^2
\]
so that
\[
N(\alpha) = \alpha \cdot \bar{\alpha} = \bar{\alpha} \cdot \alpha.
\]
Recall that a division ring is a ring (associative, with a unit element) so that every non-zero element is invertible.

**Proposition 0.1.** \( W_p \) is not a division ring\(^1\).

**Proof.** It suffices to show that there are zero divisors (since they can’t be invertible). One way to do it is to find a nonzero \( \alpha \in W_p \) so that its norm is zero (mod \( p \)), that is
\[
\alpha = a_0 \mathbf{1} + a_1 \mathbf{i} + a_2 \mathbf{j} + a_3 \mathbf{k} \neq 0
\]
with
\[
\alpha \bar{\alpha} = 0
\]
in \( W_p \), in other words we want to find a nonzero vector \((a_0, a_1, a_2, a_3) \in \mathbb{F}_p^4 \) so that
\[
a_0^2 + a_1^2 + a_2^2 + a_3^2 = 0
\]
We pick \( a_3 = 0, a_0 = 1 \), and then look for \( a_1, a_2 \in \mathbb{F}_p \) so that
\[
a_1^2 + a_2^2 = -(a_0^2 + a_1^2) = -1
\]
\[^1\text{This follows from Wedderburn’s theorem, but I want to avoid using it.}\]
which will suffice. So we want to see that the equation (1) has a solution in \( \mathbb{F}_p \). This will be done in the combinatorial Lemma below. \( \square \)

**Lemma 0.2.** Let \( p \neq 2 \) be an odd prime. Then there is a solution in \( \mathbb{F}_p \) of the equation

\[
(2) \quad a_1^2 + a_2^2 = -1
\]

**Proof.** Let \( \Box = \{ x^2 : a \in \mathbb{F}_p \} \) be the set of squares in \( \mathbb{F}_p \). Note that the number \( \# \Box \) of squares in \( \mathbb{F}_p \) is exactly \( (p+1)/2 \), because the map from nonzero elements \( \mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\} \) to \( (\mathbb{F}_p^*)^2 \) is exactly two-to one: \( x^2 = y^2 \) if and only if \( y = \pm x \), so that there are exactly \( (p-1)/2 \) nonzero squares in \( \mathbb{F}_p \), while zero is attained only once, altogether giving \( (p-1)/2 + 1 = (p+1)/2 \) squares in \( \mathbb{F}_p \).

Rewrite equation (2) as

\[
(3) \quad 1 + a_1^2 = -a_2^2
\]

Then the left hand side attains \( (p+1)/2 \) values, and the same holds for the right hand side. Because \( (p+1)/2 > \#\mathbb{F}_p/2 \), this means we have two subsets \( S_1 = \Box + 1, S_2 = -\Box \) of \( \mathbb{F}_p \) each of which is larger than half the size of the underlying set \( \mathbb{F}_p \), so must intersect! (if they were disjoint, then the size of their union will be the sum of their sizes, which is greater than \( \#\mathbb{F}_p \)). That is \( S_1 \cap S_2 \neq \emptyset \), which is precisely the statement that there are \( a_1, a_2 \in \mathbb{F}_p \) so that (3) has a solution. \( \square \)