Quaternions and Sums of Squares Worksheet

Define the "vector space of Quaternions"

$$\mathbb{H} := \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\}$$

($\mathbb{R}$ is of course the real numbers). We view the real number line as a subset of $\mathbb{H}$ as follows: $\mathbb{R} \subset \mathbb{H}$ is the set of "scalar quaternions", which is the sub-vector space consisting of vectors $a + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{j}$ for $a \in \mathbb{R}$. Such quaternions will be denoted simply by a (so 3 denotes $3 + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}$, similarly to how $3 \in \mathbb{C}$ denotes $3 + 0 \cdot i$). Quaternions can be added (as vectors) and we define a distributive multiplication on $\mathbb{H}$. We define multiplication by $a \in \mathbb{R}$ (on either the left or the right) to be scalar multiplication: so $a \cdot \mathbf{h} = \mathbf{h} \cdot a = ah$ for $a \in \mathbb{R}$ and a vector $\mathbf{h} \in \mathbb{H}$. Multiplication is defined on-scalar basis vectors as follows:

$$\begin{array}{lll} \mathbf{i}^2 = -1 & \mathbf{j}^2 = -1 & \mathbf{k}^2 = -1 \\ \mathbf{ij} = \mathbf{k} & \mathbf{jk} = \mathbf{i} & \mathbf{ki} = \mathbf{j} \\ \mathbf{ji} = -\mathbf{k} & \mathbf{kj} = -\mathbf{i} & \mathbf{ik} = -\mathbf{j}. \end{array}$$

(mnemonic: all of $\mathbf{i}, \mathbf{j}, \mathbf{k}$ square to -1 and multiplying two basis vectors "in order" gives the third, "out of order" gives minus the third).

FACT. Multiplication of quaternions is associative. (You can take this on faith). To check it it would be enough to check that $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ for α, β, γ basis vectors. You can convince yourself that there is nothing to check when α, β, or $\gamma = 1$. The cases that need to be checked (up to symmetry provided by rotating the i, j, k around cyclically) are $\mathbf{iij}, \mathbf{ijj}, \mathbf{iji}, \mathbf{ijk}$, and $\mathbf{kji}$.

It follows that the quaternions are a non-commutative ring: you can add and multiply them like matrices[1]

[1] in fact there is a way to write 2×2 complex matrices $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\mathbf{i} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, and so on, in such a way that their products satisfy the relations above. These matrices are called "Pauli matrices" (they come from physics) and will not be used here.

1. Say $\mathbf{h} = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ and $\mathbf{h}' = a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}$. Write down a formula for $\mathbf{h} \cdot \mathbf{h}'$ (using distributivity).

2. Define $\overline{\mathbf{h}} := a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$. Show that $\overline{\mathbf{hh}'} = \overline{\mathbf{h}}' \cdot \overline{\mathbf{h}}$ (it's enough to check this for basis vectors $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$).

3. For $\mathbf{h}$ as above a quaternion, define $||\mathbf{h}|| = a^2 + b^2 + c^2 + d^2$.[2]. Show that $\mathbf{h} \cdot \overline{\mathbf{h}} = ||\mathbf{h}||$.

Deduce that $||\mathbf{h} \cdot \mathbf{h}'|| = ||\mathbf{h}|| \cdot ||\mathbf{h}'||$ (careful about order of multiplication.)

4. If $\mathbf{h} \neq 0$, define $\mathbf{h}^{-1} := \frac{\overline{\mathbf{h}}}{||\mathbf{h}||}$. Prove that $\mathbf{h} \cdot \mathbf{h}^{-1} = 1$. Deduce (by swapping $\mathbf{h}$ ad $\mathbf{h}^{-1}$, for example) that $\mathbf{h}^{-1} \cdot \mathbf{h} = 1$ as well. (I.e. $\mathbf{h}^{-1}$ acts as precisely the inverse of $\mathbf{h}$.) The fact that every nonzero quaternion has an inverse makes $\mathbb{H}$ a "division ring" or a "skew field".

[2] $||\mathbf{h}||$ is called the "norm" of the quaternion $\mathbf{h}$: the double lines are to distinguish it from the "absolute value", which is $|\mathbf{h}| = \sqrt{||\mathbf{h}||}$

Now we define $\mathbb{H}_{int}$, the "set of integral quaternions" to be the set $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, for $a, b, c, d \in \mathbb{Z}$ (integers). We say that an element $\mathbf{h}' \in \mathbb{H}_{int}$ is *left divisible* by $\mathbf{h} \in \mathbb{H}_{int}$ (write this as $\mathbf{h} \mid \mathbf{h}'$) if $\mathbf{h}' = \mathbf{h} \cdot q$, for some $q \in \mathbb{H}_{int}$. Notice that $\mathbf{h}'$ is left divisible by $\mathbf{h}$ if and only if $\overline{\mathbf{h}}'$ is *right* divisible by $\overline{h}$.

For most of the rest of this worksheet, we will be proving the following result.

Factorization Theorem. Fix a prime p. Suppose $\mathbf{h} \in \mathbb{H}_{int}$ is an integral quaternion such that $||\mathbf{h}||$ is divisible by p but $\mathbf{h}$ itself is not divisible by p (i.e. one of a, b, c, d has remainder $\neq 0$ when divided by p). Then $\mathbf{h}$ is left divisible by some element $\tau \in \mathbb{H}_{int}$ such that $||\tau|| = p$.

We first treat the case $p = 2$ separately, then proceed by induction on p.

5. Prove that if $||\mathbf{h}||$ is even then $\mathbf{h}$ is left divisible by one of $1 + \mathbf{i}, 1 + \mathbf{j}, 1 + \mathbf{k}$ (which have norm 2). This proves the factorization theorem for $p = 2$.

6. Now assume p is an odd prime, and $\mathbf{h} \in \mathbb{H}_{int}$ an integer quaternion. Prove that there exist $q, r \in \mathbb{H}_{int}$ such that $qp + r = \mathbf{h}$, and such that $||r|| < p^2$. Hint: every number is equivalent modulo p to one of $-\frac{p-1}{2}, \ldots, \frac{p-1}{2}$.

7. Now assume p is an odd prime, and we have proven the factorization theorem for all $\ell < p$. Assume that $r \in \mathbb{H}_{int}$ is an integer quaternion such that p divides $||r||$. Suppose further that

$||r|| < p^2$. Write $||r|| = p \cdot e$ (for $e \in \mathbb{Z}$ an integer). The induction hypothesis then implies that the factorization theorem holds for primes ℓ which divide e. Applying it to $\overline{r}$, for each such ℓ, either $\ell \mid \overline{r}$ or $\overline{r} = \lambda_1 \cdot \overline{r}_1$. By inductively applying this procedure, deduce that (if ℓ does not divide r) we have $\overline{r} = \lambda_t \cdot \overline{r}_t$, for some $\lambda_t \in \mathbb{H}_{int}$ and $\overline{r}_t \in \mathbb{H}_{int}$ satisfying $||r_t|| = p$. Deduce (by conjugating once) that r is left divisible by r_t, proving the factorization theorem.

8. Show that there exists $\mathbf{h} = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{H}_{int}$ such that a, b, c, d are not all divisible by p but $||\mathbf{h}||$ is divisible by p (hint: take a to be any nonzero remainder mod p. Then we have seen that $-a$ is a sum of two squares mod p). Deduce that there is a quaternion $\mathbf{h} \in \mathbb{H}_{int}$ with norm $||\mathbf{h}|| = p$.

9. Conclude that every positive integer is the sum of four squares.

10. Bonus problems: **(a)** Prove that every Gaussian number $g \in \mathbb{G}$ (so $g = a + bi$ for a, b integers) has a decomposition as a product of Gaussian primes $g = \alpha_1 \cdot \cdots \cdot \alpha_n$. This decomposition is unique up to order and up modifying each α_i by a "unit" in $\mathbb{G}$, i.e. one of $U = \{1, i, -1, -i\}$. Up to multiplication by $U = \{1, i, -1, -i\}$, there is exactly one Gaussian

prime of norm 2, two Gaussian primes of norm p for primes $p \equiv 1 \mod 4$ and one Gaussian prime of norm p^2 for primes $p \equiv 3 \mod 4$ (and there are no other Gaussian primes).

(b) Deduce when a positive number n is a sum of squares (based on the prime factorization of n). Can you come up with a formula for the number of ways n can be written as $a^2 + b^2$ (assuming sign and order matters)? Hint: first find the number of Gaussian numbers of norm n up to multiplication by U.

(c) let A_n be the number of ways to express n as a sum $a^2 + b^2$ of two squares (here order matters and a, b can be positive or negative). Let $f(s) = \sum_{n=1}^{\infty} A_n/n^s$ (this is called a "Dirichlet series"). Show that

$$g(s) = 4 \prod_p f_p(s),$$

where

$$f_p(s) := \begin{cases} 1/(1-2^{-s}), & p = 2 \\ 1/(1-p^{-2s}), & p \equiv 3 \mod 4 \\ 1/(1-p^{-s})^2, & p \equiv 1 \mod 4 \end{cases}.$$

Here the product runs over all primes.