Assignment 3, Math 3EE3
Due Feb. 26 in class

(1) Prove the division algorithm for polynomials over an arbitrary field. That is, show that if F is a field and $f, g \in F[x]$ then there are unique $q, r \in F[x]$ such that $g = qf + r$ and $deg(r) < deg(f)$. Hint: prove this by induction on the degree of g.
(2) Prove that if S is a finite subgroup of the multiplicative group of a field K then S is cyclic. Hint: S is a finite abelian group and so by the fundamental theorem of finite abelian groups we can write S as the product of finitely many cyclic subgroups of prime power order i.e.
$$S \cong Z_{d_1} \times \ldots \times Z_{d_n}$$
where d_i is a power of a prime for all i. Let m be the least common multiple of the d_i's. Claim: $a^m = 1$ for all $a \in S$. Ask yourself how many solutions the polynomial $x^m - 1$ can have in K.

(3) In order to understand the role of the quarternions, we give the following proof; you should provide proofs for the statements in bold.

Theorem (Frobenius)**.** Show that if D is a finite-dimensional real division algebra then D is isomorphic to $\mathbb{R}, \mathbb{C}$ or $\mathbb{H}$; that is If D is a division ring and $\mathbb{R}$ is contained in the centre of D i.e. if $\mathbb{R} \subseteq D$ and for every $a \in D$ and $r \in \mathbb{R}$, $ar = ra$, and as an $\mathbb{R}$-vector space D is finite-dimensional then D is isomorphic to either the reals, the complex numbers or the quaternions.

Proof. Suppose D is as in the theorem and is n-dimensional as a real vector space. Consider the map φ from D to linear transformations on D defined by: for every $a \in D$, $\varphi_a : D \to D$ such that $\varphi_a(b) = ab$.

Check that for every $a \in D$, φ_a is a linear transformation.

By fixing a basis for D, we can identify the set of linear transformations on D with $M_n(\mathbb{R})$. In this way we can assume that $D \subseteq M_n(\mathbb{R})$ where $\mathbb{R}$ is identified with scalar multiples of I.

Now consider the trace map $tr : D \to \mathbb{R}$ sending $a \in D$ to $tr(a)$, the trace of the matrix a. The trace is a linear transformation; let V be the kernel of tr. Since $\mathbb{R}$ is one-dimensional as an $\mathbb{R}$ vector space, V is of co-dimension 1 in D and $\mathbb{R}$ together with V generates D.

Now fix $a \in D$ and let $p(x)$ be the characteristic polynomial of a. Over the reals, all polynomials factor into a product of linear and irreducible quadratic terms so
$$p(x) = \prod_{i=1}^{k}(x - r_i) \prod_{j=1}^{l} q_j(x)$$
where $r_i \in \mathbb{R}$ and q_j is an irreducible quadratic. By the Cayley-Hamilton Theorem, a satisfies its characteristic polynomial so $p(a) = 0$. Since D is a division ring, this means that either $a = rI$ for some $r \in \mathbb{R}$ or $q(a) = 0$ for some irreducible quadratic q. (**Why?**)

Now if $a \in V$ then $tr(a) = 0$ so either $a = 0$ or the minimal polynomial for a is of the form $q(x) = x^2 + bx + c$ where $b^2 < 4c$ i.e. q is irreducible over $\mathbb{R}$. The characteristic polynomial for a is then some power of q, say $q^t(x)$. Remembering that the trace of a is the coefficient of x^{2t-1} in the characteristic polynomial **conclude that if $tr(a) = 0$ then $b = 0$.** Therefore, if $a \in V$ and $a \neq 0$ then a satisfies $x^2 + c$ for some $c > 0$. So if $a \in V$ then $a^2 \in \mathbb{R}$ i.e. a^2 is a multiple of I and that multiple is ≤ 0. We say $a^2 \leq 0$.

Now define an inner product on V by

$$\langle x, y\rangle = \frac{x^2 + y^2 - (x+y)^2}{2}$$

Check that this is an inner product. Make sure you show that $\langle x, y\rangle$ is a real number.

Now suppose that $e_1, \ldots, e_m$ is an orthonormal basis for V with respect to this inner product.

Show that

(1) $e_i^2 = -1$ **for all** i**,**
(2) $e_i e_j = -e_j e_i$ **for** $i \neq j$**, and**
(3) if $m \geq 3$ **then** $(e_1e_2 - e_3)(e_1e_2 + e_3) = 0$**. Why does this show** $e_3 = \pm e_1 e_2$**?**

In fact, the calculation above show that $e_k = \pm e_1 e_2$ for any $k > 2$ i.e. $e_3 = \pm e_k$ for all $k \geq 3$. So m is at most 3. If $m = 0$ then $D = \mathbb{R}$. If $m = 1$ then $e_1^2 = -1$ and we see that $D \cong \mathbb{C}$. If $m > 1$ then in fact $m = 3$ since always e_1, e_2 and e_1e_2 are linearly independent. We have $e_1^2 = e_2^2 = -1$ and $e_1e_2 = -e_2e_1$ which are the defining equations for the quaternions so $D \cong \mathbb{H}$. $\square$