Solutions to Assignment 3

1. We prove the division algorithm by induction on $\deg(g)$. If $\deg(g) < \deg(f)$ then let $q = 0$, $r = g$.

So assume $\deg(g) = m \geq \deg(f) = n$; write
$f = a_n x^n + \dots + a_0$ with $a_n \neq 0$
$g = b_m x^m + \dots + b_0$ with $b_m \neq 0$.

Then $\deg\left(g - \frac{b_m}{a_n} x^{m-n} f \right) < m$.

By induction then $g - \frac{b_m}{a_n} x^{m-n} f = qf + r$ where $\deg(r) < n$

But then $g = \left(\frac{b_m}{a_n} x^{m-n} + q \right) f + r$ which is the desired form.

If $g = qf + r = q'f + r'$ with $\deg(r), \deg(r') < n$

then we have $(q - q')f = r' - r$. The degree of the RHS is $< n$ and so the LHS must be 0 i.e. $q = q'$ and then $r = r'$.

2. Following the hint we see that any $a \in \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_n}$ must satisfy $ma = 0$ since $m = \operatorname{lcm}(d_1, \dots d_n)$ and each $\mathbb{Z}_{d_i}$ is cyclic. This means in S we have $a^m = 1$ for all $a \in S$. Now $x^m - 1$ has at most m

solutions in K and so $|S| \le m$. But $|S| = d_1 \cdots d_n$ which gives $m = d_1 \cdots d_n$. So all the d_i's are co-prime which tells you that S is cyclic.

3. Check that φ_a is a linear map:

With D viewed as a vectorspace over $\mathbb{R}$,

$\varphi_a : D \to D$ is defined by $\varphi_a(b) = ab$.

$\varphi_a(b+c) = a(b+c) = ab + ac$. We also have

$\mathbb{R} \subseteq D$ and so $\varphi_a(\lambda b) = a(\lambda b) = \lambda ab$ since $\mathbb{R}$ is in the centre of D.

If $\dim(D) = n$ then we can identify D with a subring of $M_n(\mathbb{R})$ via the map $a \mapsto \varphi_a$ (viewed as a matrix relative to a fixed basis).

Now if $a \in D$ and p is the char. poly of a then

$p(a) = 0$. But D is a division ring so we have

either $a - r_i I = 0$ or $q_j(a) = 0$ for one of the quadratics q_j.

Let $V \subseteq D$ s.t. ~~tr~~. $V = \{a \in D : tr(a) = 0\}$. V is a subspace of D.

The claim that for any $a \in D$, the characteristic poly of a is either $(x-\lambda)^n$ or $q^t(x)$ for some irreducible quadratic q requires some proof.

If the char. poly f of a has two distinct irreducible factors then f can be written as gh where g, h have gcd 1. But then $g(a)$ and $h(a)$ both have no trivial kernel. But D is a division ring so $g(a) = h(a) = 0$.

So the minimal poly divides both g and h which is a contradiction. So in the case that the min poly is an irreducible q, the char poly is of the form q^t.

Now, if $q(x) = x^2 + bx + c$ then the trace of a is tb and if $a \in V$, we get $b = 0$. So for $a \in V$, $a \neq 0$ the minimal poly of a is $x^2 + c$ for some $c > 0$.

i.e. $a^2 = -cI$ for all $a \in V$. We identify a^2 with the number $-c$.

Checking $\langle\, ;\, \rangle$ is an inner product:

For $x, y \in V$, x^2, y^2 and $(x+y)^2$ are all real numbers under the identification ~~of~~ above. So $\langle x, y \rangle \in \mathbb{R}$.

It is clearly symmetric; let's see that it is linear

Notice: $\dfrac{x^2+y^2-(x+y)^2}{2} = \dfrac{-xy-yx}{2}$

so $\langle x, y+z\rangle = \dfrac{-x(y+z)-(y+z)x}{2} = \langle x,y\rangle + \langle x,z\rangle.$

For $\lambda \in \mathbb{R}$, $\langle \lambda x, y\rangle = \dfrac{-\lambda xy - y(\lambda x)}{2} = \lambda\langle x,y\rangle.$

Now $\langle x,x\rangle = \dfrac{x^2+x^2-4x^2}{2} = -x^2 \geq 0$ and equality holds only if $x=0$.

So $\langle \cdot,\cdot\rangle$ is an inner product on V.

For the chosen orthonormal basis, we check:

1) $\langle e_i, e_i\rangle = 1$ implies $-e_i^2 = 1$ so $e_i^2 = -1$ for all i.

2) If $i \neq j$ then $\langle e_i, e_j\rangle = 0$ i.e. $-e_ie_j - e_je_i = 0$

So $e_{ij} = -e_{ji}$

3) Let's compute $(e_1e_2 - e_i)(e_1e_2+e_i)$ for any $i>2$, if $m \geq 3$.

$$
\begin{aligned}
(e_1e_2 - e_i)(e_1e_2+e_i) &= e_1e_2e_1e_2 + e_1e_2e_i - e_ie_1e_2 - e_i^2 \\
&= -e_1^2e_2^2 + e_ie_1e_2 - e_ie_1e_2 + 1 \\
&= 0.
\end{aligned}
$$

So since D is a division ring, we have either $e_i = e_1 e_2$ or $e_i = -e_1 e_2$.

<u>So</u> m is at most 3.