**Student: Yu Cheng (Jade)**

**Math 612**

**Homework #4**

**April 18, 2011**

## Dummit & Foote, Exercises 13.2

**Question 19** Let $K$ be an extension of $F$ of degree $n$.

a. For any $\alpha \in K$ prove that $\alpha$ acting by the left multiplication on $K$ is an $F$-linear transformation of $K$.

**Answer:** First we view $K$ as a vector space of $F$ since $K$ is an extension of $F$. Now we want to evaluate the map of left multiplication by a fixed element $\alpha \in K$, which we shall call $f_a : K \to K$, defined by $f_a(k) = \alpha k$, where $k \in K$. According to the definition of being a linear transformation, we want to show $f_a(x+y) = f_a(x) + f_a(y)$, and $f_a(cx) = cf_a(x)$where $x, y \in K$ and $c \in F$.

$$\begin{aligned} f_a(x+y) &= \alpha(x+y) \\ &= \alpha x + \alpha y \\ &= f_a(x) + f_a(y). \\ f_a(c \cdot x) &= \alpha \cdot cx \\ &= c \cdot \alpha x \\ &= c \cdot f_a(x). \end{aligned}$$

We've shown that $\alpha \in K$ acting by the left multiplication on $K$ is an $F$-linear transformation. This is done by viewing $K$ as a vector space of $F$ and proving the properties of being a linear transformation.

b. Prove that $K$ is isomorphic to a subfield of the ring of $n \times n$ matrices over $F$, so the ring of $n \times n$ matrices over $F$ contains an isomorphic copy of every extension of $F$ of degree $\leq n$.

**Answer:** In the previous question, we've shown that for any $\alpha \in K$, the map $f_a$ is a $F$-linear transformation. So the following map is well defined.

$$\varphi : K \to M_n(F)$$
$$\varphi : k \to f_k.$$

We can show that this map is a ring homomorphism from the field $K$ to the ring $M_n(F)$. We will first show that the map $\varphi$ preserves the addition operation.

$$\begin{aligned}
\varphi(k_1+k_2) &= f_{k_1+k_2} \\
f_{k_1+k_2}(x) &= (k_1+k_2)\cdot x \\
&= k_1x+k_2x \\
&= f_{k_1}(x)+f_{k_2}(x) \\
&= \varphi(k_1)+\varphi(k_2) \\
\Rightarrow \varphi(k_1+k_2) &= \varphi(k_1)+\varphi(k_2).
\end{aligned}$$

We now show that the map $\varphi$ preserves the multiplication operation, which is the function composition for $f_k$ and the matrix multiplication in $M_n(F)$.

$$\begin{aligned}
\varphi(k_1\cdot k_2) &= f_{k_1\cdot k_2} \\
f_{k_1\cdot k_2}(x) &= (k_1\cdot k_2)\cdot x \\
&= k_1k_2x \\
&= f_{k_1}(k_2x) \\
&= f_{k_1}(f_{k_2}(x)) \\
&= \varphi(k_1)\cdot\varphi(k_2) \\
\Rightarrow \varphi(k_1\cdot k_2) &= \varphi(k_1)\cdot\varphi(k_2).
\end{aligned}$$

We can show this ring homomorphism is injective, and hence $K\cong img(\varphi)\le M_n(F)$. Let $f_{k_1}=f_{k_2}$, we want to show this happens only when $k_1=k_2$.

$$\begin{aligned}
& f_{k_1}=f_{k_2} \\
\Rightarrow\quad & k_1x=k_2x \\
\Rightarrow\quad & k_1x-k_2x=0 \\
\Rightarrow\quad & (k_1-k_2)\,x=0,\ \forall x\in K \\
\Rightarrow\quad & k_1-k_2=0,\ \because K \text{ is an integral domain} \\
\Rightarrow\quad & k_1=k_2.
\end{aligned}$$

Therefore, $\varphi$ is an injective map, and $K\cong img(\varphi)\le M_n(F)$. Hence $M_n(F)$ contains an isomorphic copy of $K$, which is an extension of $F$ with degree $n$.

Let's have $K'$ be an extension field of $F$, and $[K':F]=m<n$. From the previous conclusion, we know that $M_m(F)$ contains an isomorphic copy of $K'$. Since $M_m(F)$is a subring of $M_n(F)$, $M_n(F)$ also contains an isomorphic copy of $K'$. Therefore $M_n(F)$ contains an isomorphic copy of every extension of $F$ with degree $\le n$.

**Question 20-1** Show that if the matrix of the linear transformation "multiplication by $\alpha$" considered in the previous exercise is $A$ then $\alpha$ is a root of the characteristic polynomial for $A$.

**Answer:** As shown previously, we can view the "multiplication by $\alpha$" as a $F$-linear transformation, $A \in M_n(F)$. In other words, we have the following relation, where $\alpha, k \in K$ and $\alpha$ is fixed.

$$A \cdot k = \alpha \cdot k.$$

It is obvious that $\alpha$ is an eigenvalue of $A$, which is a root of $A$'s characteristic polynomial by definition. So $\alpha$ is a root of the characteristic polynomial of $A$.

**Question 20-2** This gives an effective procedure for determining an equation of degree $n$. Use this procedure to obtain the monic polynomial of degree $3$ satisfied by $\sqrt[3]{2}$ and by $1 + \sqrt[3]{2} + \sqrt[3]{4}$.

**Answer:** We will first determine the monic polynomial of degree $3$ satisfied by $\sqrt[3]{2}$. Basically, we need to determine the $F$-linear transformation $A$ that corresponds to $\sqrt[3]{2}$, and the characteristic polynomial of $A$ is the monic polynomial satisfied by $\sqrt[3]{2}$. Let's consider a basis of $K$ as a vector space over $F$. One such basis is $\left\{1, \sqrt[3]{2}, \sqrt[3]{4}\right\}$. A typical element in $K$ can be expressed as a vector over $F$.

$$\begin{aligned}
&k \in K \\
&k = a \cdot 1 + b \cdot \sqrt[3]{2} + c \cdot \sqrt[3]{4} \\
&k = \begin{bmatrix} a \\ b \\ c \end{bmatrix}, \ a, b, c \in F.
\end{aligned}$$

Plug this information in $A \cdot k = \alpha \cdot k$, we can solve $A$.

$$\begin{aligned}
A \cdot \begin{bmatrix} a \\ b \\ c \end{bmatrix} &= \sqrt[3]{2} \cdot \begin{bmatrix} a \\ b \\ c \end{bmatrix} \\
&= \sqrt[3]{2} \cdot \left(a \cdot 1 + b \cdot \sqrt[3]{2} + c \cdot \sqrt[3]{4}\right) \\
&= a \cdot \sqrt[3]{2} + b \cdot \sqrt[3]{4} + c \cdot 2 \\
&\Rightarrow \quad A = \begin{bmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.
\end{aligned}$$

Let's verify this solutions of $A$.

$$\begin{aligned} A \cdot \begin{bmatrix} a \\ b \\ c \end{bmatrix} &= \begin{bmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} a \\ b \\ c \end{bmatrix} \\ &= \begin{bmatrix} 2c \\ a \\ b \end{bmatrix} \\ &= 2c \cdot 1 + a \cdot \sqrt[3]{2} + b \cdot \sqrt[3]{4} \\ &= \sqrt[3]{2} \cdot \begin{bmatrix} a \\ b \\ c \end{bmatrix}. \end{aligned}$$

Now we find the characteristic polynomial of $A$.

$$\begin{aligned} det\left( x \cdot I_3 - \begin{bmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \right) &= det\left( \begin{bmatrix} x & 0 & -2 \\ -1 & x & 0 \\ 0 & -1 & x \end{bmatrix} \right) \\ &= x \cdot det\left( \begin{bmatrix} x & 0 \\ -1 & x \end{bmatrix} \right) - 2 \cdot det\left( \begin{bmatrix} -1 & x \\ 0 & -1 \end{bmatrix} \right) \\ &= x^3 - 2. \end{aligned}$$

The monic polynomial of degree $3$ satisfied by $\sqrt[3]{2}$ is $x^3 - 2$.

Similarly, for $1 + \sqrt[3]{2} + \sqrt[3]{4}$, we first determine a basis of $K$ as a vector space over $F$. One such basis is $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$. Plug this information in $A \cdot k = \alpha \cdot k$, we can solve $A$.

$$\begin{aligned} A \cdot \begin{bmatrix} a \\ b \\ c \end{bmatrix} &= \left(1 + \sqrt[3]{2} + \sqrt[3]{4}\right) \cdot \begin{bmatrix} a \\ b \\ c \end{bmatrix} \\ &= \left(1 + \sqrt[3]{2} + \sqrt[3]{4}\right) \cdot \left(a \cdot 1 + b \cdot \sqrt[3]{2} + c \cdot \sqrt[3]{4}\right) \\ &= (a + 2b + 2c) + (a + b + 2c) \cdot \sqrt[3]{2} + (a + b + c) \cdot \sqrt[3]{4} \\ &\Rightarrow \quad A = \begin{bmatrix} 1 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{bmatrix}. \end{aligned}$$

Let's verify this solutions of $A$.

$$A \cdot \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 1 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} a \\ b \\ c \end{bmatrix}$$

$$
\begin{aligned}
&= \begin{bmatrix} a+2b+2c \\ a+b+2c \\ a+b+c \end{bmatrix} \\
&= (a+2b+2c)\cdot 1 + (a+b+2c)\cdot \sqrt[3]{2} + (a+b+c)\cdot \sqrt[3]{4} \\
&= \left(1+\sqrt[3]{2}+\sqrt[3]{4}\right)\cdot \begin{bmatrix} a \\ b \\ c \end{bmatrix}.
\end{aligned}
$$

Now we find the characteristic polynomial of $A$.

$$
\begin{aligned}
det\left(x\cdot I_3 - \begin{bmatrix} 1 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{bmatrix}\right) &= det\left(\begin{bmatrix} x-1 & -2 & -2 \\ -1 & x-1 & -2 \\ -1 & -1 & x-1 \end{bmatrix}\right) \\
&= (x-1)\cdot det\left(\begin{bmatrix} x-1 & -2 \\ -1 & x-1 \end{bmatrix}\right) + 2\cdot det\left(\begin{bmatrix} -1 & -2 \\ -1 & x-1 \end{bmatrix}\right) \\
&\quad -2\cdot det\left(\begin{bmatrix} -1 & x-1 \\ -1 & -1 \end{bmatrix}\right) \\
&= x^3-3x^2-3x-1.
\end{aligned}
$$

The monic polynomial of degree $3$ satisfied by $1+\sqrt[3]{2}+\sqrt[3]{4}$ is $x^3-3x^2-3x-1$.

**Question 21-1** Let $K=\mathbb{Q}\left(\sqrt{D}\right)$ for some squrefree integer $D$. Let $\alpha=a+b\sqrt{D}$ be an element of $K$. Use the basis, $\left\{1,\sqrt{D}\right\}$ for $K$ as a vector space over $\mathbb{Q}$ and show that the matrix of the linear transformation "multiplication by $\alpha$" on $K$ considered in the previous exercises has the matrix $\begin{bmatrix} a & bD \\ b & a \end{bmatrix}$.

**Answer:** We will first show that the matrix of the linear transformation "multiplication by $\alpha$" on $K$ considered in the previous exercises has the matrix $\begin{bmatrix} a & bD \\ b & a \end{bmatrix}$. We use the given basis $\left\{1,\sqrt{D}\right\}$ to express a typical element in $K=\mathbb{Q}\left(\sqrt{D}\right)$.

$$
\begin{aligned}
&k\in K \\
&k = x\cdot 1 + y\cdot\sqrt{D} \\
&k = \begin{bmatrix} x \\ y \end{bmatrix},\ a,b\in\mathbb{Q}.
\end{aligned}
$$

Plug this information in $A \cdot k = \alpha \cdot k$, we can solve $A$.

$$\begin{aligned} A \cdot \begin{bmatrix} x \\ y \end{bmatrix} &= \alpha \cdot \begin{bmatrix} x \\ y \end{bmatrix} \\ &= \left(a \cdot 1 + b \cdot \sqrt{D}\right) \cdot \left(x \cdot 1 + y \cdot \sqrt{D}\right) \\ &= (ax + byD) + (ay + bx)\sqrt{D} \\ &\Rightarrow \quad A = \begin{bmatrix} a & bD \\ b & a \end{bmatrix}. \end{aligned}$$

**Question 21-2** Prove directly that the map $a + b\sqrt{D} \mapsto \begin{bmatrix} a & bD \\ b & a \end{bmatrix}$ is an isomorphism of the field $K$ with a subfield of the ring of $2 \times 2$ matrices with coefficients in $\mathbb{Q}$.

**Answer:** We will first prove the map $\varphi : K \to M_2(\mathbb{Q})$ defined by $\varphi : a + b\sqrt{D} \mapsto \begin{bmatrix} a & bD \\ b & a \end{bmatrix}$ is a ring homomorphism. We first verify that $\varphi$ preserves the addition operation.

$$\begin{aligned} \varphi\left(\left(a + b\sqrt{D}\right) + \left(c + d\sqrt{D}\right)\right) &= \varphi\left((a+c) + (b+d)\sqrt{D}\right) \\ &= \begin{bmatrix} a+c & (b+d)D \\ b+d & a+c \end{bmatrix} \\ \varphi\left(a + b\sqrt{D}\right) + \varphi\left(c + d\sqrt{D}\right) &= \begin{bmatrix} a & bD \\ b & a \end{bmatrix} + \begin{bmatrix} c & dD \\ d & c \end{bmatrix} \\ &= \begin{bmatrix} a+c & (b+d)D \\ b+d & a+c \end{bmatrix} \\ \Rightarrow \varphi\left(\left(a + b\sqrt{D}\right) + \left(c + d\sqrt{D}\right)\right) &= \varphi\left(a + b\sqrt{D}\right) + \varphi\left(c + d\sqrt{D}\right). \end{aligned}$$

We now verify that $\varphi$ preserves the multiplication operation.

$$\begin{aligned} \varphi\left(\left(a + b\sqrt{D}\right) \cdot \left(c + d\sqrt{D}\right)\right) &= \varphi\left((ac + bdD) + (ad + bc)\sqrt{D}\right) \\ &= \begin{bmatrix} ac + bdD & (ad+bc)D \\ ad + bc & ac + bdD \end{bmatrix} \\ \varphi\left(a + b\sqrt{D}\right) \cdot \varphi\left(c + d\sqrt{D}\right) &= \begin{bmatrix} a & bD \\ b & a \end{bmatrix} \cdot \begin{bmatrix} c & dD \\ d & c \end{bmatrix} \\ &= \begin{bmatrix} ac + bdD & (ad+bc)D \\ ad + bc & ac + bdD \end{bmatrix} \\ \Rightarrow \varphi\left(\left(a + b\sqrt{D}\right) \cdot \left(c + d\sqrt{D}\right)\right) &= \varphi\left(a + b\sqrt{D}\right) \cdot \varphi\left(c + d\sqrt{D}\right). \end{aligned}$$

So we've shown that $\varphi$ is a ring homomorphism. We now show that $\varphi$ is injective.

$$\begin{aligned}
& \begin{bmatrix} a_1 & b_1 D \\ b_1 & a_1 \end{bmatrix} = \begin{bmatrix} a_2 & b_2 D \\ b_2 & a_2 \end{bmatrix} \\
\Rightarrow \quad & a_1 = a_2,\ b_1 = b_2 \\
\Rightarrow \quad & a_1 + b_1\sqrt{D} = a_2 + b_2\sqrt{D}.
\end{aligned}$$

Therefore, $\varphi$ is an injective map, and $K \cong img\left(\varphi\right) \leq M_2\left(\mathbb{Q}\right)$. Hence $K$ is isomorphic to a subfield of $M_2\left(\mathbb{Q}\right)$.