MATH 340 Assignment 4, Fall 2017
Solutions to Additional Questions

Michael Monagan

Section 2.2: Subrings and Subfields

Find a subring of $\mathbb{Z}_8$ with 4 elements.
Is it a subfield? Justify your answer.

Consider the subset $R4 = \{[0], [2], [4], [6]\}$ of $\mathbb{Z}_8$.
One may easily check that it is closed under addition and multiplication. We also have $-[0] = [0], -[2] = [6], -[4] = [4], -[6] = [2]$ so it's also closed under negation. Thus $R4$ is a subring of $\mathbb{Z}_8$. Since $[2] \cdot [4] = [8] = [0]$, [2] and [4] are zero divisors so $R4$ is not a field.

Section 2.3: Review of Vector Spaces

Let $M_2(\mathbb{Z}_2) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \ : \ a, b, c, d \in \mathbb{Z}_2 \right\}$ and let $\mathbb{Z}_2^4 = \left\{ \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} : a, b, c, d \in \mathbb{Z}_2 \right\}$.

So $M_2(\mathbb{Z}_2)$ is the set of 2 by 2 matrices with entries in $\mathbb{Z}_2$ and $\mathbb{Z}_2^4$ is the set of vectors of dimension 4 over $\mathbb{Z}_2$. Show that the vectors spaces $M_2(\mathbb{Z}_2)$ and $\mathbb{Z}_2^4$ are isomorphic.

Let use define $\phi : M_2(\mathbb{Z}_2) \to \mathbb{Z}_2^4$ by

$$\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) = [a \ b \ c \ d]^T$$

then ϕ is invertible since

$$\phi^{-1}([a \ b \ c \ d]^T) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

so ϕ is bijective. For matrices $A, B \in M_2(\mathbb{Z}_2)$ and scalar $s \in \mathbb{Z}_2$ we have to show that $\phi(A + B) = \phi(A) + \phi(B)$ and $\phi(s \cdot A) = s \cdot \phi(A)$. Let

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \ \text{ and } \ B = \begin{bmatrix} e & f \\ g & h \end{bmatrix} \implies A + B = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}.$$

Thus

$$\phi(A+B) = \phi\left(\begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}\right) = \begin{bmatrix} a+e \\ b+f \\ c+g \\ d+h \end{bmatrix} = \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} + \begin{bmatrix} e \\ f \\ g \\ h \end{bmatrix} = \phi(A) + \phi(B).$$

And for scalar multiplication

$$\phi(s \cdot A) = \phi(s \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix}) = \phi(\begin{bmatrix} sa & sb \\ sc & sd \end{bmatrix}) = \begin{bmatrix} sa \\ sb \\ sc \\ sd \end{bmatrix} = s \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = s \cdot \phi(A).$$

Section 2.5: Polynomial Evaluation and Interpolation

Lemma 2.5.1 (i) says if R is an integral domain and $f(x) \in R[x]$ and $a \in R$ then (i) $f(a) = 0 \iff (x-a)|f(x)$.
Prove that this is also true for any commutative ring R with identity 1_R.

Proof ($\Rightarrow$) Since the leading coefficient of $x-a$ is 1_R, it is invertible so we can use the division theorem 2.4.3 to divide f by $x-a$ to get a quotient q and remainder r with $f = (x-a)q(x)+r$ with $r = 0$ or $\deg r < \deg(x-a) = 1$. The rest of the proof of Lemma 2.5.1 (i) goes through.