Worksheet for May 8

MATH 24 — SPRING 2014

Sample Solutions

Recall that $\mathbb{Z}_2$ is the field with exactly two elements, 0 and 1. The addition and multiplication rules for $\mathbb{Z}_2$ are summarized in the followng two tables:

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

A good mnemonic to remember this is to think of 0 as meaning 'even' and 1 as meaning 'odd'. So $1+1=0$ because two odd numbers add to an even number and $1\times 0=0$ because an odd number times an even number results in an even number.

(A) How many polynomials of degree n with coefficients in $\mathbb{Z}_2$ are there? How many of them split over $\mathbb{Z}_2$?

Solution — A polynomial of degree n has the form

$$c_nt^n + c_{n-1}t^{n-1} + \cdots + c_1t + c_0$$

where $c_n \neq 0$. Since coefficients are in $\mathbb{Z}_2$, we must have $c_n = 1$ and we have two choices for each of $c_{n-1},\dots,c_1,c_0$. Combining all these choices, we see that there are exactly 2^n polynomials of degree n with coefficients in $\mathbb{Z}_2$.

In order to split over $\mathbb{Z}_2$, a polynomial of degree n must have the form $(t-0)^{m_0}(t-1)^{m_1} = t^{m_0}(t+1)^{m_1}$ where $m_0+m_1 = n$. There are $n+1$ possibilities for $m_0+m_1 = n$, each of which gives rise to a different polynomial since the smallest nonzero coefficient of the expansion of $t^{m_0}(t+1)^{m_1}$ is the coefficient of t^{m_0}.

Since $n+1$ is much smaller than 2^n, very few polynomials with coefficients in $\mathbb{Z}_2$ split completely into linear factors. In fact, fewer than 1% of polynomials of degree 11 split and fewer than 0.01% of polynomials of degree 18 split.

(B) Consider the following three matrices over the two-element field $\mathbb{Z}_2$:

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

1.– Compute the characteristic polynomials of A, B, C.

Solution —
$$\det(A - tI) = t^3 + t = t(t+1)^2,$$
$$\det(B - tI) = t^3 + t^2 = t^2(t+1),$$
$$\det(C - tI) = t^3 + 1 = (t+1)(t^2+t+1).$$

Note that $t^2 + t + 1$ has no roots in $\mathbb{Z}_2$ so it doesn't factor any further.

2.– Compute bases for the eigenspaces of A, B, C.

Solution — For A, we have

$$\mathsf{E}_0 = \mathsf{N}(L_A) = \operatorname{span}\{(1,1,0)\}$$

and

$$\mathsf{E}_1 = \mathsf{N}(L_A - I) = \operatorname{span}\{(0,1,0),(0,0,1)\}.$$

For B, we have

$$\mathsf{E}_0 = \mathsf{N}(L_B) = \operatorname{span}\{(0,1,1)\}$$

and

$$\mathsf{E}_1 = \mathsf{N}(L_B - I) = \operatorname{span}\{(0,1,0)\}.$$

For C, we have $\mathsf{E}_0 = \{0\}$ since 0 is not an eigenvalue, but

$$\mathsf{E}_1 = \mathsf{N}(L_C - I) = \operatorname{span}\{(1,1,1)\}.$$

3.– If possible, find an invertible matrix Q such that QAQ^{-1} is diagonal. Do the same for B and C.

Solution — Only A is diagonalizable. For B, the algebraic and geometric multiplicities of 0 do not agree. For C, the characteristic polynomial does not split completely into linear factors.

From above, an eigenbasis for A is $\beta = \{(1,1,0),(0,1,0),(0,0,1)\}$. The change of coordinates matrix from β-coordinates to standard coordinates is

$$Q^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

which is actually its own inverse.

To be sure, we can check that

$$QAQ^{-1} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

(C) Let A, B, C be the same matrices as above.

1.– Use Theorem 5.22 to find a basis for the L_A-cyclic subspace generated by e_1.

Solution — For A, we find that $e_1 = (1,0,0)$, $Ae_1 = (0,1,0)$, are linearly independent but $A^2e_1 = Ae_1$. So $\{(1,0,0),(0,1,0)\}$ is a basis for the L_A cyclic subspace generated by e_1.

For B, we find that $e_1 = (1,0,0)$, $Be_1 = (0,1,1)$, are linearly independent but $B^2e_1 = 0$. So $\{(1,0,0),(0,1,1)\}$ is a basis for the L_B cyclic subspace generated by e_1.

For C, we find that $e_1 = (1,0,0)$, $Ce_1 = (0,1,0)$, $C^2e_1 = (0,0,1)$ are linearly independent but $C^3e_1 = e_1$. So $\{(1,0,0),(0,1,0),(0,0,1)\}$ is a basis for the L_C cyclic subspace generated by e_1.

2.– Verify Theorem 5.21 for the L_A-invariant subspace you just computed.

Solution — Using 5.22 and the fact that $A^2e_1 + Ae_1 = 0$, we arrive at the characteristic polynomial $t^2 + t = t(t+1)$ for the restriction of L_A to the L_A cyclic subspace generated by e_1. This is visibly a factor of the characteristic polynomial $t(t+1)^2$ we found earlier.

Using 5.22 and the fact that $B^2e_1 = 0$, we arrive at the characteristic polynomial t^2 for the restriction of L_B to the L_B cyclic subspace generated by e_1. This is visibly a factor of the characteristic polynomial $t^2(t+1)$ we found earlier.

Using 5.22 and the fact that $C^3e_1 = e_1$, we arrive at the characteristic polynomial $t^3 + 1$ for the restriction of L_C to the L_C cyclic subspace generated by e_1. This is visibly a factor of the characteristic polynomial $t^3 + 1$ we found earlier.

Repeat for L_B and L_C.