# Worksheet for April 2

MATH 24 — SPRING 2014

*Sample Solutions*

**(1)** Show that the matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

are linearly independent in $\mathsf{M}_{2\times 2}(\mathbb{Z}_2)$.

*Solution* — Because the field $\mathbb{Z}_2$ only has two elements, namely $0$ and $1$, there are only eight linear possible combinations

$$a\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + b\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + c\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

When exactly one of $a, b, c$ is $1$, we simply obtain the three original matrices:

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

When exactly two of $a, b, c$ are $1$, we obtain the three matrices:

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Finally, when $a = b = c = 1$, we obtain the matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Since none of these are the zero matrix, no nontrivial linear combination of the three given matrices equals zero. Therefore, the three matrices are linearly dependent.

For a more systematic approach that also works with larger fields, we can look at the system of coordinate equations that arise from

$$a\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + b\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + c\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

namely

$$\begin{aligned} a + b \qquad &= 0 \\ a + b + c &= 0 \\ c &= 0 \\ b + c &= 0 \end{aligned}$$

The third equation forces $c = 0$. Then the last equation forces $b = 0$ too. Finally, the remaining two equation force $a = 0$. Therefore, the only way to obtain the zero matrix as a linear combination of the three given matrices is the trivial combination $a = b = c = 0$.

**(2)** Determine whether the set

$$\left\{ \begin{pmatrix} i & 0 \\ 0 & i \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} 0 & i \\ 0 & 0 \\ i & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

is linearly independent in $\mathsf{M}_{3\times 2}(\mathbb{C})$.

*Solution* — Since $i^2 = -1$, we see that

$$i \begin{pmatrix} i & 0 \\ 0 & i \\ 0 & 0 \end{pmatrix} + i \begin{pmatrix} 0 & 0 \\ i & 0 \\ 0 & i \end{pmatrix} + i \begin{pmatrix} 0 & i \\ 0 & 0 \\ i & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

is a linear dependency among these matrices.

Rather than simply guessing a linear dependency, let's proceed in a more systematic way. From

$$x_1 \begin{pmatrix} i & 0 \\ 0 & i \\ 0 & 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 & 0 \\ i & 0 \\ 0 & i \end{pmatrix} + x_3 \begin{pmatrix} 0 & i \\ 0 & 0 \\ i & 0 \end{pmatrix} + x_4 \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \end{pmatrix} + x_5 \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

We obtain the following system of coordinate equations:

$$\begin{aligned} ix_1 \qquad\qquad + x_4 \qquad &= 0 \\ ix_2 \qquad + x_4 \qquad &= 0 \\ ix_3 + x_4 \qquad &= 0 \\ ix_1 \qquad\qquad\qquad + x_5 &= 0 \\ ix_2 \qquad\qquad + x_5 &= 0 \\ ix_3 \qquad + x_5 &= 0 \end{aligned}$$

While intimidatingly large, this system is almost already in echelon form. Subtracting the first equation from the fourth, the second from the fifth, and the third from the sixth, we obtain:

$$\begin{aligned} ix_1 \qquad\qquad + x_4 \qquad &= 0 \\ ix_2 \qquad + x_4 \qquad &= 0 \\ ix_3 + x_4 \qquad &= 0 \\ - x_4 + x_5 &= 0 \end{aligned}$$

where the last two equations were omitted since they were identical to the fourth.

At this point, we see that $x_5$ is a slack variable, so we could pick any value for $x_5$ and we will be able to solve the system. It follows that the system has infinitely many solutions and therefore the system does have solutions other than $x_1 = x_2 = x_3 = x_4 = x_5 = 0$. In fact, solving the system for $x_5 = t$, we obtain $x_1 = x_2 = x_3 = it$ and $x_4 = x_5 = t$ as the general solution; the one we found above corresponds to choosing $t = 1$.

**(3)** For $1 \leq i, j \leq 17$ let $E^{i,j}$ denote the $17 \times 17$ matrix whose $(i, j)$-th entry is $1$ and all of whose other entries are zero. Show that

$$S = \{E^{i,j} : 1 \leq i, j \leq 17\}$$

is linearly independent in $\mathsf{M}_{17\times 17}(F)$.

*Solution* — Since $S$ contains 289 matrices, it's not practical to write down the coordinate equations in long form. Fortunately, it makes sense to use $\Sigma$-notation in linear algebra just like in calculus (except that infinite series don't make much sense). The typical linear combination of the matrices in $S$ can be written:

$$\sum_{i=1}^{17} \sum_{j=1}^{17} a_{ij} E^{ij}.$$

By definition of $E^{ij}$, the $(i, j)$-th entry of the result of this sum is simply $a_{ij}$. Indeed, the $(i, j)$-th entry of $a_{ij}E^{ij}$ is $a_{ij}$ and all other summands have $(i, j)$-th entry $0$. It follows that the only way to obtain the zero matrix as a result is to have $a_{ij} = 0$ for all $1 \leq i, j \leq 17$. Therefore, the set $S$ is indeed linearly independent.

**(4)** Is the set $\{(1, 1, 0), (1, 0, 1), (0, 1, 1)\}$ linearly independent in $F^3$?

*Solution* — This is a trick question since the answer depends on what the field $F$ is. If $F$ has characteristic $2$, i.e., $1 + 1 = 0$ as in $\mathbb{Z}_2$, then

$$(1, 1, 0) + (1, 0, 1) + (0, 1, 1) = (0, 0, 0)$$

is a nontrivial linear dependency of the vectors in the set. However, if $1 + 1 \neq 0$, then the vectors in the set are linearly independent!

To see this formally, let's set up the coordinate equations for

$$x_1(1, 1, 0) + x_2(1, 0, 1) + x_3(0, 1, 1) = (0, 0, 0).$$

The resulting system is:

$$\begin{aligned} x_1 + x_2 \phantom{+ x_3} &= 0 \\ x_1 \phantom{+ x_2} + x_3 &= 0 \\ x_2 + x_3 &= 0 \end{aligned}$$

Subtracting the first equation from the second, we obtain:

$$\begin{aligned} x_1 + x_2 \qquad &= 0 \\ -x_2 + x_3 &= 0 \\ x_2 + x_3 &= 0 \end{aligned}$$

Adding the second equation to the third, we obtain:

$$\begin{aligned} x_1 + x_2 \qquad &= 0 \\ -x_2 + \ x_3 &= 0 \\ 2x_3 &= 0 \end{aligned}$$

In this last equation, 2 denotes $1 + 1$.

If the field $F$ has characteristic 2, then $2 = 0$ and the last equation reduces to $0 = 0$. In that case $x_3$ is a slack variable and we can pick any value for $x_3$ and we will still be able to solve the equations. Therefore, the system has at least one solution other than $x_1 = x_2 = x_3 = 0$, which means that the set is linearly dependent in $F^3$.

If the field $F$ does not have characteristic 2, then $2 \neq 0$ and we can multiply the last equation by the multiplicative inverse of 2 to obtain:

$$\begin{aligned} x_1 + x_2 \qquad &= 0 \\ -x_2 + x_3 &= 0 \\ x_3 &= 0 \end{aligned}$$

These equations tell us that $x_1 = -x_2$, $x_2 = x_3$, and $x_3 = 0$. Therefore, $x_1 = x_2 = x_3 = 0$ is the only solution to this system, which means that the set is linearly independent in $F^3$.

**(5)** Prove that if $S$ is a set of nonzero polynomials in $\mathsf{P}(F)$ such that no two have the same degree then $S$ is linearly independent in $\mathsf{P}(F)$.

*Solution* — I will formulate this solution in theorem-proof style.

**Theorem.** *Any set $S$ of nonzero polynomials in $\mathsf{P}(F)$ that contains at most one polynomial of each degree is linearly independent.*

*Proof.* Supppose, for the sake of contradiction, that there is a nontrivial linear dependency among elements of $S$. Specifically, suppose $f_1(x), f_2(x), \ldots, f_n(x)$ are distinct elements of $S$ and that $a_1, a_2, \ldots, a_n$ are nonzero scalars such that

$$a_1 f_1(x) + a_2 f_2(x) + \cdots + a_n f_n(x) = 0.$$

Note that we must have $n \geq 2$ since none of the polynomials in $S$ are zero.

Since $S$ contains at most one polynomials of each degree, the degrees of the polynomials $f_1(x), f_2(x), \ldots, f_n(x)$ must all be different. Renumbering the polynomials if necessary, we may assume that

$$\deg(f_1(x)) > \deg(f_2(x)) > \cdots > \deg(f_n(x)).$$

Since $a_1 \neq 0$, we may solve the above equation for $f_1(x)$ to obtain

$$f_n(x) = -\frac{a_2}{a_1} f_2(x) - \cdots - \frac{a_n}{a_1} f_n(x).$$

The right hand side is a linear combination of polynomials of degree at most $\deg(f_2(x))$, which means that $f_1(x)$ has degree at most $\deg(f_2(x))$ since linear combinations of polynomials never increase the degree. But this is impossible since we know that $\deg(f_1(x)) > \deg(f_2(x))$!

From this contradiction, we conclude that our hypothesis that there is a nontrivial linear dependency among elements of $S$ must be false and therefore that $S$ is linearly independent. □

There are a few interesting aspects to this proof:

- Since "$S$ is linearly independent" is a negative statement, a proof by contradiction was the most likely approach for this. Pay attention to disguised negatives: 'independent', 'nonzero', 'infinite', 'irrational', etc. When you see them, think about using tricks such as the contrapositive or proof by contradiction.

  For another example, compare Theorem 1.6 with its Corollary in Section 1.5. The two are contrapositives of each other but Theorem 1.6, which involves 'linear dependence', has an easy direct proof while the Corollary, which involves 'linear independence' does not have an easy direct proof.

- Note how the hypothesis that elements of $S$ are nonzero is actually important. We used it to show that $n \geq 2$ for the proposed linear dependency. Without this fact, all the mentions of $f_2(x)$ in the second paragraph could be meaningless!

  It's always tempting to think that expressions like $a_1 f_1(x) + \cdots + a_n f_n(x)$ necessarily involve multiple terms. However, the notation is meant to include $n = 1$ as a possibility, so make sure your argument works in that case too!

- The sentence "renumbering the polynomials if necessary, we may assume that [...]" is interesting. Since it makes no difference how the terms of a linear dependency are ordered, we can choose to order them in a way that is convenient for us. What is unusual is that we are making this choice after the fact. This is fine in this case since we could have made this choice before the fact but the proof would have been harder to follow.

  A common trap is to accidentally introduce new hypotheses in this process. If you do this, do make sure that you could have made the choices you want at the outset and without changing the hypotheses of the result you want to prove.