Homework 3

Matt Swartz and John Tippie

Problem 1 (Golan 124). Let F be a field and let $(K, \bullet)$ be an associative unital F-algebra. If A and B are subsets of K, we let $A \bullet B$ be the set of all elements of K of the form $a \bullet b$, with $a \in A$ and $b \in B$ (in particular, $\emptyset \bullet B = A \bullet \emptyset = \emptyset$). We know that the set V of all subsets of K is a vector space over GF(2). Is $(V, \bullet)$ a GF(2)-algebra? If so, is it associative? Is it unital?

Solution. We will define symmetric difference as vector addition on V. $**$That is, define vector addition in V by adding strings "bitwise" modulo 2. That is

$$\begin{aligned} i + j &= (i_0, i_1, \ldots, i_{n-1}) + (j_1, \ldots, j_{n-1}) \\ &= (i_0, i_1, \ldots, i_{n-1}) + (j_1, \ldots, j_{n-1}) \\ &= (i_0 + j_0, i_1 + j_1, \ldots, i_{n-1} + j_{n-1}) \end{aligned}$$

where for each $0 \leq k < n$, the k-th element of $i + j$ is

$$i_k + j_k = \begin{cases} 0, & i_k = j_k \\ 1, & i_k \neq j_k. \end{cases}$$

Clearly the latter addition is commutative, and therefore, the vector addition is commutative: $i + j = j + i$. The zero vector $\mathbf{0} = (0, \ldots, 0)$ is the additive identity, and each vector is its own additive inverse, that is, $-v = v$.$**$

Let $u, v, w, x \in V$. The conditions we need to satisfy in order to show that $(V, \dot{})$ is a associative unital GF(2)-algebra are as follows:

1. $u \bullet (v + w) = u \bullet v + u \bullet w$,
2. $(u + v) \bullet w = u \bullet w + v \bullet w$,
3. $a(v \bullet w) = (av) \bullet w = v \bullet (aw)$,
4. $v \bullet (w \bullet y) = (v \bullet w) \bullet y$, (associative)
5. $v \bullet 1_F = v = 1_F \bullet v$. (unital)

The information between the two $**$'s at the beginning of this problem was taken directly from Matthew Corley and Melissa Murphy's write-up of Homework 2.

Problem 2 (Golan 132). Let F be a field and let L be the set of all polynomials $f(X) \in F[X]$ satisfying the condition that $f(-a) = -f(a)$ for all $a \in F$. Is L a subspace of $F[X]$?

Solution. L is the set of odd polynomials (i.e. only odd powers of x). To show that L is a subspace of $F[X]$, we need to show that L is a vector space in its own right with respect to the addition and scalar multiplication defined on F. Let the additive identity be the zero polynomial. To show that L is closed under vector (i.e.,polynomial) addition, let $f, g \in L$. Then $f(X)+g(X) = \sum_{i=0}^{\infty} a_{2i+1}X^{2i+1} + \sum_{i=0}^{\infty} b_{2i+1}X^{2i+1} = \sum_{i=0}^{\infty}(a_{2i+1}+b_{2i+1})X^{2i+1} = \sum_{i=0}^{\infty} c_{2i+1}X^{2i+1} \in L$. Let $c \in F$, then $cf(X) = c\sum_{i=0}^{\infty} a_{2i+1}X^{2i+1} = \sum_{i=0}^{\infty} ca_{2i+1}X^{2i+1} = \sum_{i=0}^{\infty} b_{2i+1}X^{2i+1} \in L$. Thus, L is a subspace of $F[X]$.

Problem 3 (Golan 133). Let F be a field and let L be the set of all polynomials $f(X) \in F[X]$ satisfying the condition that $\deg(f)$ is even. Is L a subspace of $F[X]$?

Solution. L is the set of polynomials with the highest power of even order. To show that L is a subspace of $F[X]$, we need to show that L is a vector space in its own right with respect to the addition and scalar multiplication defined on F. This is not the case as we can see with the following counterexample. Let $f(X) = 1 + X - 3X^2$ and let $g(X) = 3X^2$. Both f and g are in L since their highest power is even. However, $f(X) + g(X) = 1 + X$ is not in L since its highest power is odd. Thus, L is not a subspace of $F[X]$.

Problem 4 (Golan 142). For a field F, compare the subsets $F[X^2]$ and $F[X^2 + 1]$ of $F[X]$.

Solution. $f(X) \in F[X]$ is defined as $\sum_{i=0}^{\infty} a_iX^i$, $f(X) \in F[X^2]$ is defined as $\sum_{i=0}^{\infty} a_{2i}X^{2i}$, and $f(X) \in F[X^2+1]$ is defined as $\sum_{i=0}^{\infty} a_{2i}(X^2+1)^i$. So, $F[X^2] = \{1, X^2, X^4, X^6, ...\}$ and $F[X^2+1] = \{1, X^2+1, (X^2+1)^2, (X^2+1)^3, ...\} = \{1, X^2+1, X^4+2X^2+1, X^6+3X^4+3X^2+1, ...\}$. $F[X^2] \subseteq F[X^2+1]$ since every element of $F[X^2+1]$ is of the form $\sum_{i=0}^{\infty} a_{2i}X^{2i}$ (e.g. $X^4+2X^2+1 = n_3+2n_2+n_1$ for $n_i \in F[X^2]$). Similarly, $F[X^2+1] \subseteq F[X^2]$ (e.g. $X^6 = m_4 - 3m_3 + 3m_2 - m_1$ for $m_i \in F[X^2+1]$). Thus, $F[X^2] = F[X^2+1]$.

Problem 5 (Golan 154). Let F be a field and let $K = F^{\mathbb{N}}$. Define operations $+$ and $\bullet$ on K by setting $f + g : i \mapsto f(i) + g(i)$ and $f \bullet g : i \mapsto \sum_{j+k=i} f(j)g(k)$. Show that K is a an associative and commutative unital F-algebra. Is it entire?

Solution. To show that K is an associative commutative unital F-algebra, we want to show the following conditions hold: let $u, v, w, x \in K, a \in F$

1. $u \bullet (v + w) = u \bullet x = \sum\limits_{j+k=i} u(j)x(k) = \sum\limits_{j+k=i} u(j)[v(k) + w(k)] = \sum\limits_{j+k=i} u(j)v(k) + \sum\limits_{j+k=i} u(j)w(k) = u \bullet v + u \bullet w,$
2. $(u + v) \bullet w = x \bullet w = \sum\limits_{j+k=i} x(j)w(k) = \sum\limits_{j+k=i} [u(j) + v(j)]w(k) = \sum\limits_{j+k=i} u(j)w(k) + \sum\limits_{j+k=i} v(j)w(k) = u \bullet w + v \bullet w,$
3. $a(v \bullet w) = a \sum\limits_{j+k=i} v(j)w(k) = \sum\limits_{j+k=i} [av(j)]w(k) = (av) \bullet w = \sum\limits_{j+k=i} v(j)[aw(k)] = v \bullet (aw),$
4. $v \bullet (w \bullet y) = \sum\limits_{j+k+l=i} v(j)(w(k)y(l)) = \sum\limits_{j+k+l=i} (v(j)w(k))y(l) = (v \bullet w) \bullet y$
5. $v \bullet 1_F = \sum\limits_{j=i} v(j)1_F = v(i) = v = \sum\limits_{k=i} 1_F v(k) = 1_F \bullet v$
6. $v \bullet w = \sum\limits_{j+k=i} v(j)w(k) = \sum\limits_{k+j=i} w(k)v(j) = w \bullet v,$

We can see from the simplest case where $i = 0$ that K is entire. For $v, w \in K$, $(v \bullet w)(0) = \sum\limits_{j+k=0} v(0)w(0) = 0$ only when $v(0)$ or $w(0)$ equals 0, or both. Therefore, K is entire.

Problem 6 (Golan 157). A *trigonometric polynomial* in $\mathbb{R}^{\mathbb{R}}$ is a function of the form $t \mapsto a_0 + \sum_{h=1}^{k}[a_h \cos(ht) + b_h \sin(ht)]$, where $a_0, \ldots, a_k, b_1, \ldots, b_k \in \mathbb{R}$. Show that the subset, K, of $\mathbb{R}^{\mathbb{R}}$ consisting of all trigonometric polynomials is an entire $\mathbb{R}$-algebra.

Solution. Let $f, g, h, l \in K$ and $a \in \mathbb{R}^{\mathbb{R}}$. To show that K is an entire $\mathbb{R}$-algebra, we want to show the following:
1. $f \bullet (g + h) = (a_0 + \sum_{h=1}^{k} a_h \cos(ht) + \sum_{h=1}^{k} b_h \sin(ht))[(c_0 + \sum_{h=1}^{k} c_h \cos(ht) + \sum_{h=1}^{k} d_h \sin(ht)) + (e_0 + \sum_{h=1}^{k} e_h \cos(ht) + \sum_{h=1}^{k} f_h \sin(ht))] = (a_0 + \sum_{h=1}^{k} a_h \cos(ht) + \sum_{h=1}^{k} b_h \sin(ht))(c_0 + \sum_{h=1}^{k} c_h \cos(ht) + \sum_{h=1}^{k} d_h \sin(ht)) + (a_0 + \sum_{h=1}^{k} a_h \cos(ht) + \sum_{h=1}^{k} b_h \sin(ht))(e_0 + \sum_{h=1}^{k} e_h \cos(ht) + \sum_{h=1}^{k} f_h \sin(ht)) = f \bullet g + f \bullet h$,
2. $(f + g) \bullet h = [(a_0 + \sum_{h=1}^{k} a_h \cos(ht) + \sum_{h=1}^{k} b_h \sin(ht)) + (c_0 + \sum_{h=1}^{k} c_h \cos(ht) + \sum_{h=1}^{k} d_h \sin(ht))](e_0 + \sum_{h=1}^{k} e_h \cos(ht) + \sum_{h=1}^{k} f_h \sin(ht)) = (a_0 + \sum_{h=1}^{k} a_h \cos(ht) + \sum_{h=1}^{k} b_h \sin(ht))(e_0 + \sum_{h=1}^{k} e_h \cos(ht) + \sum_{h=1}^{k} f_h \sin(ht)) + (c_0 + \sum_{h=1}^{k} c_h \cos(ht) + \sum_{h=1}^{k} d_h \sin(ht))(e_0 + \sum_{h=1}^{k} e_h \cos(ht) + \sum_{h=1}^{k} f_h \sin(ht)) = f \bullet h + g \bullet h$,
3. $a(f \bullet g) = a(a_0 + \sum_{h=1}^{k} a_h \cos(ht) + \sum_{h=1}^{k} b_h \sin(ht))(c_0 + \sum_{h=1}^{k} c_h \cos(ht) + \sum_{h=1}^{k} d_h \sin(ht)) = (aa_0 + a\sum_{h=1}^{k} a_h \cos(ht) + \sum_{h=1}^{k} b_h \sin(ht)) = (af) \bullet g = (a_0 + \sum_{h=1}^{k} a_h \cos(ht) + \sum_{h=1}^{k} b_h \sin(ht))(ac_0 + a\sum_{h=1}^{k} c_h \cos(ht) + \sum_{h=1}^{k} d_h \sin(ht)) = f \bullet (ag)$.

Let $f = a_0 + \sum_{h=1}^{k}[a_h \cos(ht) + b_h \sin(ht)] = a_0 + b_0$ and $g = c_0 + \sum_{h=1}^{k}[c_h \cos(ht) + d_h \sin(ht)] = a_0 + d_0$. If $f, g \neq 0$, then $f \bullet g = (a_0 + b_0)(c_0 + d_0) = a_0c_0 + a_0d_0 + b_0c_0 + b_0d_0$. Here, we have 4 cases:
1. $a_0 = 0, b_0 \neq 0, c_0 = 0, d_0 \neq 0 \Rightarrow (a_0 + b_0)(c_0 + d_0) = b_0d_0 \neq 0$
2. $a_0 = 0, b_0 \neq 0, c_0 \neq 0, d_0 = 0 \Rightarrow (a_0 + b_0)(c_0 + d_0) = b_0c_0 \neq 0$
3. $a_0 \neq 0, b_0 = 0, c_0 = 0, d_0 \neq 0 \Rightarrow (a_0 + b_0)(c_0 + d_0) = a_0d_0 \neq 0$
4. $a_0 \neq 0, b_0 = 0, c_0 \neq 0, d_0 = 0 \Rightarrow (a_0 + b_0)(c_0 + d_0) = a_0c_0 \neq 0$

Thus, K is an entire $\mathbb{R}$-algebra.

Problem 7 (Golan 163). Let $F = \mathbb{Q}$. Is the subset

$$\left\{ \begin{bmatrix} 4 \\ 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix} \right\}$$

of F^3 linearly independent? What happens if $F = \mathrm{GF}(5)$?

Solution. To see if the given subset of F^3 is linearly independent, we can perform row operations to reach a RREF form of the matrix

$$\begin{bmatrix} 4 & 1 & 1 \\ 2 & 0 & 3 \\ 1 & 0 & 4 \end{bmatrix}$$

.
We proceed as follows:

$$\begin{bmatrix} 4 & 1 & 1 \\ 2 & 0 & 3 \\ 1 & 0 & 4 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 4 \\ 4 & 1 & 1 \\ 2 & 0 & 3 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & -15 \\ 0 & 0 & 5 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & -15 \\ 0 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Thus, the subset is linearly independent. If $F = GF(5)$, we see that the subset is not linearly independent. If we add 3 times row 3 to row two, we get a row of zeros.

Problem 8 (Golan 177). Show that the subset

$$\left\{ \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 0 \\ 1 \end{bmatrix} \right\}$$

is a linearly independent subset of $\mathrm{GF}(p)^3$ if and only if $p \neq 3$.

Solution. Let $p = 3$. Perform row reductions as follows:

$$\begin{bmatrix} 1 & 0 & 2 \\ 2 & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{bmatrix}$$

Thus, The set is linearly dependent if $p = 3$.

Let $p \neq 3$. Then if we set
$a \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix} + b \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} = c \begin{bmatrix} 2 \\ 0 \\ 1 \end{bmatrix}$, we get the system of equations $a = 2c, 2a + b = 0, 2b = c$.
Substituting, we then get $2(2c) + b = 0 \Rightarrow 4c + b = 0 \Rightarrow 4(2b) + b = 0 \Rightarrow 9b = 0$, which only happens if $p = 3$. Thus, if $p \neq 3$, then the set is linearly independent.

Clarification/amplification of Props 5.12 and 5.13. Let V be a vector space, and let $\{W_\omega : \omega \in \Omega\}$ be a collection of subspaces of V. Recall that $\sum_{\omega \in \Omega} W_\omega$ denotes the subspace of all (finite) linear combinations of vectors in $\{W_\omega : \omega \in \Omega\}$, which is equivalent to the subspace of vectors w of the form $w = \sum_{\lambda \in \Lambda} w_\lambda$, where $w_\lambda \in W_\lambda$ and Λ is a finite subset of Ω.
We call the set $\{W_\omega : \omega \in \Omega\}$ *independent* if and only if it satisfies the following condition: If Λ is a finite subset of Ω, if $w_\lambda \in W_\lambda$ for each $\lambda \in \Lambda$, and if $\sum_{\lambda \in \Lambda} w_\lambda = 0_V$, then $w_\lambda = 0_V$ for all $\lambda \in \Lambda$.

Problem 9. Let

$$W_1 = \left\{ \begin{bmatrix} a \\ 0 \end{bmatrix} : a \in \mathbb{R} \right\},\ W_2 = \left\{ \begin{bmatrix} b \\ b \end{bmatrix} : b \in \mathbb{R} \right\},\ W_3 = \left\{ \begin{bmatrix} 0 \\ c \end{bmatrix} : a \in \mathbb{R} \right\}.$$

1. Would our textbook author describe $\{W_1, W_2, W_3\}$ as "pairwise disjoint?" (explain)
2. Describe the space $W_1 + W_2 + W_3$.
3. Describe the space $W_i + W_j$ for each pair $i \neq j$ in $\{1, 2, 3\}$.
4. Is the set $\{W_1, W_2, W_3\}$ independent?

Solution. 1. Our book would describe $\{W_1, W_2, W_3\}$ as "pairwise disjoint" since $W_1 \cap W_2 = 0_V$ and $W_2 \cap W_3 = 0_V$.
2. $W_1 + W_2 + W_3 = \left\{ \begin{bmatrix} d \\ e \end{bmatrix} : d, e \in \mathbb{R} \right\}$
3. $W_1 + W_2 = \left\{ \begin{bmatrix} d \\ b \end{bmatrix} : d, b \in \mathbb{R} \right\} = W_2 + W_3 = \left\{ \begin{bmatrix} b \\ d \end{bmatrix} : b, d \in \mathbb{R} \right\} = W_1 + W_3 = \left\{ \begin{bmatrix} a \\ c \end{bmatrix} : a, c \in \mathbb{R} \right\}.$
4. The set $\{W_1, W_2, W_3\}$ is not independent. Consider the example where $a = 1$ in W_1, $c = 1$ in W_3, and $b = -1$ in W_2. Then, their sum is zero and they are therefore dependent.

Problem 10. Below is an alleged theorem that attempts to combine Propositions 5.12 and 5.13 of the textbook. Prove it, or disprove it by providing a counterexample. If you find a counterexample, what additional hypothesis would fix the theorem?

Proposition. Suppose $\{W_\omega : \omega \in \Omega\}$ is a collection of subspaces of a vector space, and suppose, for each $\omega \in \Omega$, the set B_ω is a basis for W_ω. Then the following are equivalent:

1. The set $\{W_\omega : \omega \in \Omega\}$ is independent.
2. Every $w \in \sum_{\omega \in \Omega} W_\omega$ can be written as $w = \sum_{\lambda \in \Lambda} w_\lambda$ in exactly one way.
3. For every $\lambda \in \Omega$, $W_\lambda \cap \sum_{\omega \neq \lambda} W_\omega = \{0_V\}$.
4. The set $B = \bigcup_{\omega \in \Omega} B_\omega$ is a basis for $\sum_{\omega \in \Omega} W_\omega$.

The proof of Proposition 5.12 in the book covers (1) $\Rightarrow$ (2) and (2) $\Rightarrow$ (3), so we will leave it up to the reader to look those up. As for showing (3) $\Rightarrow$ (4), we see that the set $\{W_i : i \in \Omega\}$ is a pairwise disjoint collection of subspaces of V. For each $i \in \Omega$, let B_i be a basis of W_i. Then $V = \sum_{\omega \in \Omega} W_\omega \Rightarrow B = \bigcup_{\omega \in \Omega} B_\omega$ is a basis for $\sum_{\omega \in \Omega} W_\omega$, as can be seen in the book's proof of Proposition 5.13. Finally, to show that (4) $\Rightarrow$ (1), we need the added assumption that the bases do not intersect. Now, we can see that since every element of V can be written in a unique way as $\sum_{i \in \Lambda} w_i$, where Λ is some finite subset of Ω, which says that $V = \bigoplus_{i \in \Omega} W_i$, meaning the set $\{W_\omega : \omega \in \Omega\}$ is independent.

Final remark. We use $\bigoplus_{\omega \in \Omega} W_\omega$ to denote $\sum_{\omega \in \Omega} W_\omega$ *only when* the set $\{W_\omega : \omega \in \Omega\}$ is independent. When I mentioned this in class, instead of *only when*, I used the phrase *when and only when.* This is incorrect since the expression $\sum_{\omega \in \Omega} W_\omega$ does not necessarily imply that the set $\{W_\omega : \omega \in \Omega\}$ is dependent.