Homework #10 Solutions

p 348, #10 The keys to this exercise are the following.

Lemma 1. *Let V be a vector space over a field F. If $\{v_1, \ldots, v_n\}$ is a linearly independent set in V and $w \notin \langle v_1, \ldots, v_n \rangle$ then $\{v_1, \ldots, v_n, w\}$ is linearly independent as well.*

Proof. Let $a_1, \ldots, a_n, b \in F$ so that $a_1 v_1 + \cdots + a_n v_n + bw = 0$. If $b \neq 0$ then we have

$$w = (-b^{-1}a_1)v_1 + \cdots + (-b^{-1}a_n)v_n \in \langle v_1, \ldots, v_n \rangle$$

which is a contradiction. It follows that $b = 0$ and so $0 = a_1 v_1 + \cdots + a_n v_n + bw = a_1 v_1 + \cdots + a_n v_n$, which implies, via the linear independence of $v_1, \ldots, v_n$, that $a_1 = \cdots = a_n = 0$. That is, the only linear combination of $v_1, \ldots, v_n, w$ that equals 0 is the trivial combination. Hence, $\{v_1, \ldots, v_n, w\}$ is linearly independent. $\square$

Lemma 2. *Let V be a vector space over a field F. If $\{v_1, \ldots, v_n\}$ is a basis for V and $\{w_1, \ldots, w_m\}$ is a linearly independent set in V then $m \leq n$.*

Proof. The proof of Theorem 19.1 can be used, word for word. $\square$

Now let $S = \{v_1, v_2, \ldots, v_n\}$ be a set of linearly independent vectors in a finite dimensional vector space V. If $\langle S \rangle = V$ then S is a basis for V and we are finished. Otherwise we can find a vector $w_1 \in V$, $w_1 \notin \langle S \rangle$ and according to the first lemma $S_1 = S \cup \{w_1\}$ is linearly independent in V. If $\langle S_1 \rangle = V$ then S_1 is a basis and we are finished. Otherwise, we can repeat the steps above to create a linearly independent set $S_2 = S \cup \{w_1, w_2\}$. We continue building linearly independent sets S_i in V this way. This process cannot continue indefinitely since the second lemma gives an upper bound on the size of linearly independent sets in V. Thus, there must be an m so that $S_m = S \cup \{w_1, \ldots, w_m\}$ actually spans V and therefore is a basis.

p 348, #20 Let U be a proper subspace of V with basis $\{v_1, \ldots, v_m\}$. Since U is proper, $\{v_1, \ldots, v_m\}$ cannot be a basis for V. According to exercise 10, then, there are vectors $w_1, w_2, \ldots, w_n$ ($n \geq 1$) so that $\{v_1, \ldots, v_m, w_1, \ldots, w_n\}$ is a basis for V. But then

$$\dim U = m < m + n = \dim V$$

as claimed.

p 349, #22 Let V be a vector space of dimension n over $\mathbb{Z}_p$ with basis $\{v_1, v_2, \ldots, v_n\}$. Then every element of V can be written in the form $a_1 v_1 + a_2 v_2 + \cdots + a_n v_n$ for some unique scalars $a_1, a_2, \ldots, a_n \in \mathbb{Z}_p$. Because there are exactly p choices for each a_i and different scalars result in different elements of V, we conclude immediately that there are p^n elements in V.

p 365, #4 We see that in $\mathbb{C}$ we have

$$x^4 = (x^2 - i)(x^2 + i) = (x - \sqrt{i})(x + \sqrt{i})(x - i\sqrt{i})(x + i\sqrt{i})$$

so that the splitting field for $x^4 + 1$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{i}, i\sqrt{i})$. However, since $i \in \mathbb{Q}(\sqrt{i})$, the splitting field can be written more simply as $\mathbb{Q}(\sqrt{i})$.

p 365, #8 Since $f(x) = x^3 + x + 1$ has no zeros in $\mathbb{Z}_2$ it is irreducible over this field. Therefore, if a is a root of $f(x)$ then the set $\{1, a, a^2\}$ is a basis for $\mathbb{Z}_2(a)$ over $\mathbb{Z}_2$. It follows that $\mathbb{Z}_2(a)$ has exactly 8 elements: $0, 1, a, a^2, 1 + a, 1 + a^2, a + a^2, 1 + a + a^2$. Using the fact that $a^3 + a + 1 = 0$ the multiplication table for $\mathbb{Z}_2(a)$ is as follows.

	0	1	a	a^2	$1+a$	$1+a^2$	$a+a^2$	$1+a+a^2$
0	0	0	0	0	0	0	0	0
1	0	1	a	a^2	$1+a$	$1+a^2$	$a+a^2$	$1+a+a^2$
a	0	a	a^2	$1+a$	$a+a^2$	1	$1+a+a^2$	$1+a^2$
a^2	0	a^2	$1+a$	$a+a^2$	$1+a+a^2$	a	$1+a^2$	1
$1+a$	0	$1+a$	$a+a^2$	$1+a+a^2$	$1+a^2$	a^2	1	a
$1+a^2$	0	$1+a^2$	1	a	a^2	$1+a+a^2$	$1+a$	$a+a^2$
$a+a^2$	0	$a+a^2$	$1+a+a^2$	$1+a^2$	1	$1+a$	a	a^2
$1+a+a^2$	0	$1+a+a^2$	$1+a^2$	1	a	$a+a^2$	a^2	$1+a$

p 366, #10 Let $f(x) = x^3 + x + 1$. Then, since we are in characteristic 2 and $f(a) = a^3 + a + 1 = 0$,

$$\begin{aligned} f(a^2) &= a^6 + a^2 + 1 \\ &= (a^3 + a)^2 + 1 \\ &= 1^2 + 1 \\ &= 0 \end{aligned}$$

and

$$\begin{aligned} f(a^2 + a) &= (a^2 + a)^3 + (a^2 + a) + 1 \\ &= (a^2 + a)a + a^2 + a + 1 \\ &= a^3 + a^2 + a^2 + a + 1 \\ &= a^3 + a + 1 \\ &= 0. \end{aligned}$$

p 366, #16 If $f(x) = x^4 + x + 1$ and $\beta \in E/\mathbb{Z}_2$ is a root of $f(x)$ then, since we are working in characteristic 2,

$$\begin{aligned} f(\beta+1) &= (\beta+1)^4 + (\beta+1) + 1 \\ &= \beta^4 + 1 + \beta \\ &= 0 \end{aligned}$$

and

$$\begin{aligned} f(\beta^2) &= (\beta^2)^4 + \beta^2 + 1 \\ &= (\beta^4)^2 + \beta^2 + 1 \\ &= (\beta+1)^2 + \beta^2 + 1 \\ &= \beta^2 + 1 + \beta^2 + 1 \\ &= 0. \end{aligned}$$

However, this reasoning applies equally well to *any* root of $f(x)$. Thus, since β^2 is a root, so too is β^2+1. Finally, since $f(x)$ is irreducible of degree 4 over $\mathbb{Z}_2$, the elements $\beta, \beta+1, \beta^2, \beta^2+1$ are all distinct in $\mathbb{Z}_2(\beta) \subset E$. It follows that

$$f(x) = (x-\beta)(x-(\beta+1))(x-\beta^2)(x-(\beta^2+1))$$

over E.

p 366, #22 If $f(x), g(x) \in F[x]$ are relatively prime then we know from previous work that there exist $r(x), s(x) \in F[x]$ so that $r(x)f(x) + s(x)g(x) = 1$. Let $c(x)$ be any common divisor of $f(x)$ and $g(x)$ in $K[x]$. Then there exist $\widehat{f}(x), \widehat{g}(x) \in K[x]$ so that $f(x) = c(x)\widehat{f}(x)$ and $g(x) = c(x)\widehat{g}(x)$. Then we have

$$1 = r(x)f(x) + s(x)g(x) = c(x)(r(x)\widehat{f}(x) + s(x)\widehat{g}(x))$$

which means that $c(x)$ is a unit in $K[x]$, i.e. $\deg c(x) = 0$. Since $c(x)$ was an arbitrary common divisor of $f(x)$ and $g(x)$ in $K[x]$, we conclude that $f(x)$ and $g(x)$ have no common divisors in $K[x]$ of positive degree. That is, $f(x)$ and $g(x)$ are relatively prime in $K[x]$.