MATH 210B

Name: Quin Darcy **Due Date:** 2/5/20
Instructor: Dr. Shannon **Assignment:** Homework 2

3. Find, with explanation, a basis for the following vector spaces:

(a) F^n over F (where F is a field).

Solution. Let $v_1 = (1, 0, \ldots, 0)$, $v_2 = (0, 1, 0, \ldots, 0), \ldots, v_n = (0, 0, \ldots, 1)$. Then define $S = \{v_i \mid 1 \leq i \leq n\}$. Assume that there exists $a_1, \ldots, a_n \in F$ such that

$$\sum_{i=1}^{n} a_i v_i = 0.$$

It follows that $(a_1, \ldots, a_n) = (0, \ldots, 0)$ which holds if and only if $a_i = 0$ for all i. Thus, S is linearly independent. Now take $w \in F^n$. Then for some $b_1, \ldots, b_n \in F$, we have that $w = (b_1, \ldots, b_n)$. Hence,

$$w = \sum_{i=1}^{n} b_i v_i \in \langle S \rangle.$$

Thus, $F^n = \langle S \rangle$. Therefore, S is a basis for F^n over F.

(b) $\mathbb{Q}[\sqrt{2}]$ over $\mathbb{Q}$.

Solution. Let $S = \{1, \sqrt{2}\}$. Let $a, b \in \mathbb{Q}$ such that $a + b\sqrt{2} = 0$. Then $\sqrt{2} = -\frac{a}{b}$. Since $a, b \in \mathbb{Q}$, then this equation holds only for $a = b = 0$. Thus, S is linearly independent. Now let $w \in \mathbb{Q}[\sqrt{2}]$. Then for some $a, b \in \mathbb{Q}$, $w = a + b\sqrt{2}$ which is a linear combination of the vectors from S. Hence, $\mathbb{Q}[\sqrt{2}] = \langle S \rangle$. Thus, S is a basis for $\mathbb{Q}[\sqrt{2}]$.

(c) $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ over $\mathbb{Q}[\sqrt{2}]$.

Solution. Let $S = \{1, \sqrt{3}\}$. Suppose for some $a, b \in \mathbb{Q}[\sqrt{2}]$ that $a + b\sqrt{3} = 0$. Then $\sqrt{3} = -\frac{a}{b}$ which has no solutions in $\mathbb{Q}[\sqrt{2}]$ apart from $a = b = 0$. Thus, S is linearly independent. Let $w \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Then for some $a, b, c, d \in \mathbb{Q}$, $w = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$. We can expand this to obtain that $w = (a + b\sqrt{2}) + (c + d\sqrt{2})\sqrt{3}$ which is a linear combination of S. Thus, $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \langle S \rangle$. Therefore, S is a basis.

(d) $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ over $\mathbb{Q}$.

Solution. Let $S = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. Letting $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0$, which implies $-a$ is the linear combination of irrational numbers with rational coefficients, this is only possible provided $a = b = c = d = 0$. Let $w \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Then $w = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ which is a linear combination of the elements of S. Thus, $w \in \langle S \rangle$ and S is a basis.

(e) $\{g(x) \in F[x] \colon g(x) = 0 \text{ or } \deg(g(x)) \leq n\}$ over F (F a field).

Solution. Let $S = \{1, x, x^2, \ldots, x^n\}$. Now suppose $a_0, \ldots, a_n \in F$ such that $\sum_{i=0}^{n} a_i x^i = 0$. Then since $0 \in F[x]$ denotes the function $f \colon \mathbb{N} \cup \{0\} \to F$, where $f(k) = 0$ for all $k \geq 0$, then equating $f(0) = a_0, f(1) = a_1, \ldots, f(n) = a_n$, it follows that $a_0 = a_1 = \cdots = a_n = 0$. Thus, S is linearly independent. Now let $g(x) \in \{g(x) \in F[x] \colon g(x) = 0 \text{ or } \deg(g(x)) \leq n\}$. Then $g(x) = \sum_{i=0}^{n} b_i x^i$ and so $g(x)$ is a linear combination of the elements of S. Thus, $g(x) \in \langle S \rangle$. Therefore, S is a basis.

4. (a) Assume that $x^3 + bx^2 + cx + d = (x-r)(x-s)(x-t)$. Express b, c, d in terms of r, s, t.

Solution. Taking our given factors, we can multiply them to obtain

$$\begin{aligned}(x-r)(x-s)(x-t) &= (x^2 - sx - rx + rs)(x-t) \\ &= x^3 - tx^2 - sx^2 + stx - rx^2 + rtx + rsx - rst \\ &= x^3 - (t+s+r)x^2 + (st+rt+rs)x - rst.\end{aligned}$$

Thus, $b = -t - r - s$, $c = rt + st + rs$, and $d = -rst$.

(b) Note that $x^3 - 2x^2 - 3 = (x^2+1)(x^2-3)$, and the roots of the polynomials are: $\alpha = i$, $\beta = -i$, $\gamma = \sqrt{3}$, $\delta = -\sqrt{3}$. Determine the group, G, of permutations of $\alpha, \beta, \gamma, \delta$ that when applied to these equations, give valid equations.

Solution. Noting that $i^2 = (-i)^2$, we find that $\alpha + \beta = 0$, $\alpha^2 + 1 = 0$, and $\alpha\gamma - \beta\delta = 0$ are all satisfied with $(\alpha\beta)$. Thus, $(\alpha\beta) \in G$. Similarly, noting that $(\sqrt{3})^2 = (-\sqrt{3})^2$, we find that $(\gamma\delta)$ satisfies $\gamma + \delta = 0$, $\gamma^2 - 3 = 0$, and $\alpha\gamma = \beta\delta = 0$. Thus, $(\gamma\delta) \in G$. Finally, since G is a group, then $(\alpha\beta)(\gamma\delta) \in G$. Hence, $G = \{(1), (\alpha\beta), (\gamma\delta), (\alpha\beta)(\gamma\delta)\}$.

5. Prove that $\mathbb{Z}[x]$ is not a PID by proving that

$$I = \{u(x)(x+2) + v(x)(x+4) \colon u(x), v(x) \in \mathbb{Z}[x]\}$$

is not a principle ideal.

Proof. Assume, for contradiction, that I is a principle ideal and let $f(x)$ be a generator of I. By assumption, we have that $(f(x)) = I$. Since $x+2 \in I$, then $x+2 \in (f(x))$ and so for some $q(x) \in \mathbb{Z}[x]$ we have that $f(x)q(x) = x+2$. Since $\mathbb{Z}$ is an integral domain and $\deg(x+2) = 1$, then $\deg(f(x)q(x)) = 1$. Thus, either $f(x) = 0$ and $\deg(q(x)) = 1$ or $\deg(f(x)) = 1$ and $\deg(q(x)) = 0$. In the first case, if $\deg(f(x)) = 0$, then $f(x)$ is a constant and $(f(x)) \neq I$. If $\deg(q(x)) = 0$, then $f(x) = a_0 + a_1 x$ and $q(x) = c$. Thus, $x + 2 = a_0 c + a_1 c x$. Equating coefficients we get that $a_0 c = 2$ and $a_1 c = 1$. Thus, $a_0 = \pm 2$, $a_1 = \pm 1$, and $c = \pm 1$. Hence, $f(x) = x+2$ or $f(x) = -x-2$, and in either case $f(x)$ is irreducible. Suppose $f(x) = x+2$. Then since $x+4 \in I$, then $x+4 \in (f(x))$ and for some $p(x) \in \mathbb{Z}[x]$, we have that $x+4 = (x+2)p(x)$. By a similar argument, it follows that $\deg(p(x)) = 0$ and $p(x) = c$. Hence, $x + 4 = cx + 2c$. This implies that $c = 1$ and $c = 2$ which is not possible. Thus, $f(x) \neq x+2$. Similarly, if $f(x) = -x-2$, then $x+4 = -cx - 2c$ which implies that $c = -1$ and $c = -2$. Thus, $f(x) \neq -x-2$. Therefore, $x + 2 \notin (f(x))$ and so $I \neq (f(x))$. $\square$

6. Assume that F is a field, and that $g(x) \in F[x]$. Assume that $g(x)$ is irreducible over $F[x]$. Prove that $F[x]/(g(x))_i$ is not an integral domain.

Proof. Since $g(x)$ is reducible, then for two polynomials $p(x), q(x) \in F[x]$ such that $\deg(p(x)) \geq 1$ and $\deg(q(x)) \geq 1$, we have that $g(x) = p(x)g(x)$. Note that

$$p(x)g(x) + (g(x))_i = \big(p(x) + (g(x))_i\big)\big(q(x) + (g(x))_i\big).$$

However, since $g(x) = p(x)q(x)$ and so $p(x)q(x) \in (g(x))_i$, then

$$g(x) + (g(x))_i = p(x)q(x) + (g(x))_i = (g(x))_i.$$

If $p(x)+(g(x))_i = (g(x))_i$, then $p(x) \in (g(x))_i$ and then for some $h(x) \in F[x]/(g(x))_i$ we would have $p(x) = g(x)h(x)$. However, since $g(x) = p(x)q(x)$, then $p(x) = p(x)q(x)h(x)$ and so $1 = q(x)h(x)$ which implies that $\deg(q(x)) = 0$ which contradicts our assumption. Thus, $p(x) + (g(x))_i$ is nonzero in $F[x]/(g(x))_i$. A similar argument shows $q(x)$ is nonzero. Thus, the product of two nonzero elements is equal to the zero and hence these two elements are zero divisors. Therefore, $F[x]/(g(x))_i$ is not an integral domain. □

7. Assume that E and F are fields, $c \in E$, $F \subseteq E$. Define $\theta \colon F[x] \to E$ by $\theta(f(x)) = f(c)$. Prove θ is a ring homomorphism.

Proof. Let $f(x) \in F[x]$. Then $\theta(f(x)) = f(c) \in E$ by definition. Thus, $\theta(F[x]) \in E$. Now let $f(x), g(x) \in F[x]$ such that $f(x) = g(x)$. Then if $f(x) = \sum\limits_{i=0}^{n} a_i x^i$ and $g(x) = \sum\limits_{i=0}^{m} b_i x^i$, then $n = m$ and $a_i = b_i$. Thus, $\theta(f(x)) = f(c) = g(c) = \theta(g(x))$. Hence, θ is well-defined. Now consider

$$f(x) + g(x) = \sum_{i=0}^{n} a_i x^i + \sum_{j-0}^{m} b_i x^i = \sum_{k=0}^{r} d_i x^i.$$

Then

$$\theta(f(x) + g(x)) = \sum_{k=0}^{r} d_i c^i.$$

Next, we consider

$$\theta(f(x)) + \theta(g(x)) = \sum_{i=0}^{n} a_i c^i + \sum_{j=0}^{m} b_i c^i.$$

Combining like terms we see that $d_i = a_i + b_i$ and thus $\theta(f(x)+g(x)) = \theta(f(x))+\theta(g(x))$. Now if $f(x)g(x) = \sum_{k=0}^{s} d_i x^i$, then

$$\theta(f(x)g(x)) = \sum_{k=0}^{s} d_i c^i \quad \text{and} \quad \theta(f(x))\theta(g(x)) = \left(\sum_{i=0}^{n} a_i c^i\right)\left(\sum_{j=0}^{m} b_i c^i\right).$$

By the definition of polynomial multiplication we get that $d_i = \sum_{k=0}^{i} a_k b_{i-k}$ and so $\theta(f(x)g(x)) = \theta(f(x))\theta(g(x))$. Therefore, θ is a homomorphism of rings. □

9. Let R be a UFD and Q its field of quotients. Let $h(x) = \sum_{i=0}^{n} d_i x^i \in R[x]$. If there exists a prime $p \in R$ such that $p \mid d_i$ for $0 \leq i \leq n-1$, $p \nmid d_n$, and $p^2 \nmid d_0$, then $h(x)$ is irreducible in $Q[x]$. Apply this result to $x^3 + 6x^2 + 3x + 3 \in \mathbb{Z}[x]$.

   Solution. In this case we have that $n = 3$ and if we select $p = 3$, then $p \mid d_0$, $p \mid d_1$, $p \mid d_2$, $p \nmid d_1$, and $p^2 \nmid d_0$. Thus, $x^3 + 6x^2 + 3x + 3$ is irreducible in $\mathbb{Q}[x]$.

10. Assume that p is prime, and define $\varphi\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ by $\varphi(q) = \hat{q}$, where $\hat{q}(m) = [q(m)]$. φ is a ring homomorphism. Assume that there exists $g(x), h(x) \in \mathbb{Z}[x]$ such that $f(x) = g(x)h(x)$, where $\deg(f(x)) \geq 1$, $\deg(g(x)) \geq 1$, and $\deg(h(x)) \geq 1$. If $\varphi(f(x))$ is irreducible in $\mathbb{Z}_p[x]$, then $f(x)$ is irreducible in $\mathbb{Z}[x]$. Using this result, determine if $f(x) = x^4 + 15x^3 + 7$ is irreducible in $\mathbb{Z}[x]$.

    Solution. Letting $p = 2$ we get that $\varphi(f(x)) = x^4 + x^3 + [1]$. Setting this equal to the product of two degree 2 polynomials as in

$$\begin{aligned} x^4 + x^3 + [1] &= ([a]x^2 + [b]x + [c])([d]x^2 + [e]x + [f]) \\ &= [ad]x^4 + ([ae + bd])x^3 + ([af + be + cd])x^2 + ([bf + ce])x + [cf]. \end{aligned}$$

    we obtain the following relationships
    (i) $[ad] = [1] \to [a] = [d] = [1]$;
    (ii) $[cf] = [1] \to [c] = [f] = [1]$;
    (iii) $[ae + bd] = [e + b] = [1] \to ([b] = [1]$ and $[e] = [0])$ or $([b] = [0]$ and $[e] = [1])$;
    (iv) $[bf + ce] = [b + e] = [0]$;
    At this point we see that (iii) and (vi) contradict each other and so $\phi(f(x))$ does not factor into two degree 2 polynomials. We now try

$$\begin{aligned} x^4 + x^3 + [1] &= ([a]x^3 + [b]x^2 + [c]x + [d])([e]x + [f]) \\ &= [ae]x^4 + ([af + be])x^3 + ([bf + ce])x^2 + ([cf + de])x + [df]. \end{aligned}$$

    This gives
    (i) $[ae] = [1] \to [a] = [e] = [1]$;
    (ii) $[df] = [1] \to [d] = [f] = [1]$;
    (iii) $[af + be] = [1 + b] = [1] \to [b] = [0]$;
    (iv) $[bf + ce] = [c] = [0]$;
    (v) $[cf + de] = [de] = [1] = [0]$;
    Clearly, (v) is impossible and so $\varphi(f(x))$ cannot be factored into the product of third and first degree polynomials. Hence, $\varphi(f(x))$ is irreducible in $\mathbb{Z}_2[x]$ and by the result proven on Canvas, $f(x)$ is irreducible in $\mathbb{Z}[x]$.