18-799F Algebraic Signal Processing Theory
Spring 2007
Solutions: Assignment 3

1. *(26 pts)*

   (a) $\mathbb{F}_n[x]$ is a vector space:

   (i) $(\mathbb{F}_n[x], +)$ is a commutative group;

   (ii) $\alpha, \beta \in \mathbb{F}$: $\alpha(\beta q(x)) = \alpha \sum_{i=0}^{n} \beta q_i x^i = \sum_{i=0}^{n} \alpha\beta q_i x^i = (\alpha\beta)q(x) \in \mathbb{F}_n[x]$;

   (iii) $(\alpha+\beta)q(x) = (\alpha+\beta)\sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n}(\alpha+\beta)a_i x^i = \sum_{i=0}^{n} \alpha a_i x^i + \sum_{i=0}^{n} \beta a_i x^i = \alpha q(x) + \beta q(x)$.

   Basis is $\{1, x, \dots, x^n\}$; $\dim \mathbb{F}_n[x] = n+1$.

   (b) $\mathrm{GL}_n(\mathbb{R})$ is not an additive group, so it cannot be a vector space.

   (c) Let $a(x), b(x), c(x), d(x), e(x), f(x) \in \mathbb{F}[x]$. Then

   (i) $\frac{a(x)}{b(x)} + \frac{c(x)}{d(x)} = \frac{a(x)d(x)+b(x)c(x)}{b(x)d(x)} \in \mathbb{F}(x)$;

   (ii) $\frac{a(x)}{b(x)} + (\frac{c(x)}{d(x)} + \frac{(e(x)}{f(x)}) = \frac{a(x)d(x)f(x)+c(x)b(x)f(x)+d(x)b(x)f(x)}{b(x)d(x)f(x)} = (\frac{a(x)}{b(x)} + \frac{c(x)}{d(x)}) + \frac{(e(x)}{f(x)}$;

   (iii) Neutral element $0 \in \mathbb{F}(x)$;

   (iv) The inverse of $\frac{a(x)}{b(x)}$ is $\frac{-a(x)}{b(x)} \in \mathbb{F}(x)$.

   (v) $\frac{a(x)}{b(x)} + \frac{c(x)}{d(x)} = \frac{a(x)d(x)+b(x)c(x)}{b(x)d(x)} = \frac{c(x)}{d(x)} + \frac{a(x)}{b(x)} \in \mathbb{F}(x)$;

   Thus, $\mathbb{F}(x)$ is a commutative group.

   Pick $\alpha, \beta \in \mathbb{F}$. Then

   - $\alpha(\beta\frac{a(x)}{b(x)}) = \frac{\alpha\beta a(x)}{b(x)} = (\alpha\beta)\frac{a(x)}{b(x)}$;
   - $(\alpha+\beta)\frac{a(x)}{b(x)} = \frac{(\alpha+\beta)a(x)}{b(x)} = \frac{\alpha a(x)}{b(x)} + \frac{\beta a(x)}{b(x)} = \alpha\frac{a(x)}{b(x)} + \beta\frac{a(x)}{b(x)}$.

   Thus, $\mathbb{F}(x)$ is a vector space.

   Since $\mathbb{F}[x] = \langle 1, x, x^2, \dots \rangle \subset \mathbb{F}(x)$ and $\dim F[x] = \infty$, $\dim \mathbb{F}(x) = \infty$. However, it is impossible to specify the basis of $\mathbb{F}(x)$.

   (d) Let $z \in \mathbb{C}$ and $\alpha, \beta \in \mathbb{R}$. Then

   (i) $(\mathbb{C}, +)$ is a commutative group;

   (ii) $\alpha(\beta z) = (\alpha\beta)z$;

   (iii) $(\alpha+\beta)z = \alpha z + \beta z$.

   Thus, $\mathbb{C}$ is a vector space. Its basis is $\{1, i = \sqrt{-1}\}$ and $\dim \mathbb{C} = 2$.

   (e) $\mathbb{R}$ is not closed under multiplication by complex numbers (e.g. $3 \cdot i = 3i \notin \mathbb{R}$), thus $\mathbb{R}$ cannot be a $\mathbb{C}$-vector space.

   (f) Let $\mathbb{Q}' = \mathbb{Q} + \sqrt{2}\mathbb{Q}$ and $a, b, c, d, e, f \in \mathbb{Q}$. Then

   (i) $(a+\sqrt{2}b) + (c+\sqrt{2}d) = (a+c) + (b+d)\sqrt{2} \in \mathbb{Q}'$;

   (ii) $(a+\sqrt{2}b) + ((c+\sqrt{2}d) + (e+\sqrt{2}f)) = (a+c+e) + \sqrt{2}(b+d+f) = ((a+\sqrt{2}b) + (c+\sqrt{2}d)) + (e+\sqrt{2}f)$;

   (iii) Neutral element $0 + 0\sqrt{2} \in \mathbb{Q}'$;

   (iv) For any $a+\sqrt{2}b \in \mathbb{Q}'$ its inverse is $-a-\sqrt{2}b \in \mathbb{Q}'$;

   (v) $(a+\sqrt{2}b) + (c+\sqrt{2}d) = (a+c) + \sqrt{2}(b+d) = (c+\sqrt{2}d) + (a+\sqrt{2}b)$.

   Thus, $\mathbb{Q}'$ is a commutative group.

   Pick $\alpha, \beta \in \mathbb{Q}$. Then

   - $\alpha(\beta(a+\sqrt{2}b)) = \alpha\beta a + \sqrt{2}\alpha\beta b = (\alpha\beta)(a+\sqrt{2}b)$;
   - $(\alpha+\beta)(a+\sqrt{2}b) = \alpha a + \beta a + \sqrt{2}\alpha b\sqrt{2}\beta b = \alpha(a+\sqrt{2}b) + \beta(a+\sqrt{2}b)$.

Thus, $\mathbb{Q}'$ is a vector space. Its basis is $\{1, \sqrt{2}\}$ and $\dim \mathbb{Q}' = 2$.

$\mathbb{Q}'$ is also a commutative ring with 1:

(i) $(\mathbb{Q}', +)$ is a commutative group;

(ii) Associativity under multiplication holds: $(a+\sqrt{2}b)((c+\sqrt{2}d)(e+\sqrt{2}f)) = (a+\sqrt{2}b)((ce + 2df + \sqrt{2}(de+cf))) = (ace + 2adf + 2bde + 2bcf) + \sqrt{2}(ade + acf + bce + 2bdf) = ((a + \sqrt{2}b)(c+\sqrt{2}d))(e+\sqrt{2}f))$;

(iii) Distributivity holds: $(a+\sqrt{2}b)((c+\sqrt{2}d)+(e+\sqrt{2}f)) = ((ac+2bd)+\sqrt{2}(ad+bc)) + ((ae+2bf)+\sqrt{2}(af+be)) = (a+\sqrt{2}b)(c+\sqrt{2}d) + (a+\sqrt{2}b)(e+\sqrt{2}f)$;

(iv) Commutativity under multiplication holds: $(a+\sqrt{2}b)(c+\sqrt{2}d) = (ac+2bd)+\sqrt{2}(ad+bc) = (c+\sqrt{2}d)(a+\sqrt{2}b)$;

(v) $1 \in \mathbb{Q}'$.

Moreover, $\mathbb{Q}'$ is a field. It is sufficient to show that $(\mathbb{Q}' \setminus \{0\}, \cdot)$ is a commutative group; in fact, it is sufficient to demonstrate that any element in $\mathbb{Q}' \setminus \{0\}$ has a multiplicative inverse. But for any $(a+\sqrt{2}b) \in \mathbb{Q}' \setminus \{0\}$ its inverse is $\frac{a}{a^2-2b^2} - \sqrt{2}\frac{b}{a^2-2b^2} \in \mathbb{Q}' \setminus \{0\}$.

(g) Since $\mathbb{R}[x]$ is a principle ideal domain, any ideal I in $\mathbb{R}[x]$ is generated by a single element, i.e. $I = p(x)\mathbb{R}[x]$ for some $p(x) \in \mathbb{R}[x]$. Notice that $\mathbb{R}[x]$ is commutative, so I is a two-sided ideal.

Let $p(x)a(x) \in p(x)\mathbb{R}[x] = I$ and $\alpha, \beta \in \mathbb{R}$. Then

(i) $(I, +)$ is obviously a commutative ring, since I is a subring of a commutative ring $(\mathbb{R}[x], +)$;

(ii) Obviously, $\alpha(\beta p(x)a(x)) = (\alpha\beta)p(x)a(x)$ and

(iii) $(\alpha+\beta)p(x)a(x) = \alpha p(x)a(x) + \beta p(x)a(x)$.

Thus, I is a vector space. Its basis is the basis of $\mathbb{R}[x]$ multiplied by $p(x)$, namely $\{p(x)x^i \mid i \geq 0\}$. $\dim I = \infty$.

(h) Since $p(x)\mathbb{R}[x]$ is an ideal in $\mathbb{R}[x]$, $(\mathbb{R}[x]/p(x)\mathbb{R}[x], +, \cdot)$ is a ring. Since

$$\alpha(a(x) \mod p(x)) \mod p(x) = (\alpha a(x)) \mod p(x)$$

and

$$a(x) + (b(x) \mod p(x)) \mod p(x) = (a(x)+b(x)) \mod p(x),$$

it is obvious that associativity and distributivity holds. Thus, $\mathbb{R}[x]/p(x)\mathbb{R}[x]$ is an $\mathbb{R}$-vector space. Its basis is $\{x^i \mid i = 0, \ldots, \deg p(x) - 1\}$ and $\dim \mathbb{R}[x]/p(x)\mathbb{R}[x] = \deg p(x)$.

2. *(56 pts)*

(a) ϕ is a linear mapping:

$$\phi(a\begin{pmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\end{pmatrix} + b\begin{pmatrix}\beta_1\\ \beta_2\\ \beta_3\end{pmatrix}) = a\alpha_1 + a\alpha_2 + a\alpha_3 + b\beta_1 + b\beta_2 + b\beta_3 = a\phi(\begin{pmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\end{pmatrix}) + b\phi(\begin{pmatrix}\beta_1\\ \beta_2\\ \beta_3\end{pmatrix}).$$

- $\ker\phi = \{\begin{pmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\end{pmatrix} \mid \alpha_1+\alpha_2+\alpha_3 = 0\} = \langle \begin{pmatrix}1\\ 0\\ -1\end{pmatrix}, \begin{pmatrix}0\\ 1\\ -1\end{pmatrix}\rangle$; $\dim\ker\phi = 2$; thus, the mapping is not injective;
- $\mathrm{im}\phi = \mathbb{R}$ and $\dim \mathrm{im}\phi = 1$; thus, the mapping is surjective;
- $\mathbb{R}^3/\ker\phi \simeq \mathbb{R}$.

(b) ϕ is a linear mapping:

$$\phi(a\begin{pmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\end{pmatrix} + b\begin{pmatrix}\beta_1\\ \beta_2\\ \beta_3\end{pmatrix}) = a\alpha_1 + b\beta_1 = a\phi(\begin{pmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\end{pmatrix}) + b\phi(\begin{pmatrix}\beta_1\\ \beta_2\\ \beta_3\end{pmatrix}).$$

- $\ker\phi = \{\begin{pmatrix}0\\ \alpha_2\\ \alpha_3\end{pmatrix}\} = \langle \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix}\rangle$; $\dim\ker\phi = 2$; thus, the mapping is not injective;
- $\mathrm{im}\phi = \mathbb{R}$ and $\dim \mathrm{im}\phi = 1$; thus, the mapping is surjective;
- $\mathbb{R}^3/\ker\phi \simeq \mathbb{R}$.

(c) ϕ is not a linear mapping. E.g. $\phi(1-1) = 0 \neq 2 = \phi 1 + \phi(-1)$.

(d) ϕ is not a linear mapping. E.g. $\phi(i+i) = \frac{\pi}{2} \neq \pi = \phi(i) + \phi(i)$, where $i = \sqrt{-1}$.

(e) ϕ is a linear mapping:

$$\phi(aq(x) + bs(x)) = x(aq(x) + bs(x)) = axq(x) + bxs(x) = a\phi(q(x)) + b\phi(s(x)).$$

- $\ker\phi = \{q(x) \in \mathbb{F}[x] \mid xq(x) = 0\} = \{0\}$. Thus, the mapping is injective. The basis of $\ker\phi$ is an empty set, its dimension is 0;
- $\mathrm{im}\phi = x\mathbb{F}[x]$, its dimension is ∞. Since $x\mathbb{F}[x] \neq \mathbb{F}[x]$, the mapping is not surjective.
- $\mathbb{F}[x]/\ker\phi = \mathbb{F}[x] \simeq x\mathbb{F}[x]$.

(f) ϕ is not a linear mapping because $\mathbb{Z}$ is not a vector space.

(g) ϕ is a linear mapping:

$$\phi(aq(x) + bs(x)) = aq'(x) + bs'(x) = a\phi(q(x)) + b\phi(s(x)).$$

- $\ker\phi = \{q(x) \in \mathbb{F}[x] \mid q'(x) = 0\} = \mathbb{F}$. Thus, the mapping is not injective. The basis of $\ker\phi$ is $\{1\}$, its dimension is 1;
- $\mathrm{im}\phi = \mathbb{F}[x]$, its dimension is ∞. Also, the mapping is surjective.
- $\mathbb{F}[x]/\ker\phi = \mathbb{F}[x]/\mathbb{F} \simeq \mathbb{F}[x]$.

(h) ϕ is a linear mapping:

$$\phi(aq(x) + bs(x)) = aq'(x) + bs'(x) = a\phi(q(x)) + b\phi(s(x)).$$

- $\ker\phi = \{q(x) \in \mathbb{F}_n[x] \mid q'(x) = 0\} = \mathbb{F}$. Thus, the mapping is not injective. The basis of $\ker\phi$ is $\{1\}$, its dimension is 1;
- $\mathrm{im}\phi = \mathbb{F}_{n-1}[x]$, its dimension is n. Since $\mathbb{F}_{n-1}[x] \neq \mathbb{F}_n[x]$, the mapping is not surjective.
- $\mathbb{F}_n[x]/\ker\phi = \mathbb{F}_n[x]/\mathbb{F} \simeq \mathbb{F}_{n-1}[x]$.

3. *(18 pts)*

(a) Let $U = x^{n+1}\mathbb{F}[x]$. Then

(i) $\mathbb{F}_n[x] \cap U = \{0\}$;

(ii) $\mathbb{F}_n[x] + U = \langle 1, x, \dots, x^n\rangle + \langle x^{n+1}, x^{n+2}, \dots\rangle = \langle 1, x, \dots, x^n, x^{n+1}, x^{n+2}, \dots\rangle = \mathbb{F}[x]$.

Thus, $\mathbb{F}_n[x] \oplus U = F[x]$.

(b) The basis of U is $\{x^{n+1}, x^{n+2}, \dots\}$; its dimension is ∞.

(c) Since $\mathbb{F}[x]/\mathbb{F}_n[x] \simeq U$, the basis of $\mathbb{F}[x]/\mathbb{F}_n[x]$ is $\{x^{n+i} + \mathbb{F}_n[x] \mid i > 0\}$ and the dimension is ∞.

4. *(20 pts)*

(a) We learned in the class that $\mathbb{F}[x]/p(x)$ is a ring (actually, a Euclidean domain). To show that it is a field, we only need to demonstrate that every non-zero element in $\mathbb{F}[x]/p(x)$ has an inverse. Let $q(x)$ be such an element. Since $p(x)$ is irreducible over $\mathbb{F}$,

$$\begin{aligned}\gcd(q(x), p(x)) = 1 \quad &\Rightarrow \quad \exists s(x), t(x) \in \mathbb{F}[x]/p(x)\colon q(x)s(x) + p(x)t(x) = 1\\ &\Rightarrow \quad (q(x)s(x) + p(x)t(x)) \mod p(x) = 1 \mod p(x)\\ &\Rightarrow \quad q(x)s(x) \equiv 1 \mod p(x)\end{aligned}$$

Thus, $s(x)$ is the inverse of $q(x)$ in $\mathbb{F}'$.

(b) Since $\mathbb{F}'$ is a ring, $(\mathbb{F}', +)$ is a commutative group. The associativity and distributivity laws over $\mathbb{F}$ hold (obvious). Thus, $\mathbb{F}'$ is an $\mathbb{F}$-vector space.

Let $n = \deg p(x)$. Consider $B = \{1, x, \ldots, x^{n-1}\}$ - a set of n independent elements of $\mathbb{F}'$. On one hand, $B \subset \mathbb{F}'$, so $\langle B \rangle \subseteq \mathbb{F}'$. On the other hand, any element $q(x) \in \mathbb{F}'$ can be written as $q(x) = \sum_{i=0}^{n-1} a_i x^i \in \langle B \rangle$, so $\mathbb{F}' \subseteq \langle B \rangle$. Thus, $\mathbb{F}' = \langle B \rangle$, B is the basis of $\mathbb{F}'$, and $\dim \mathbb{F}' = n$.

(c) Over $\mathbb{Q}$: $\mathbb{Q}/(x^2 - 2)$;

Over $\mathbb{R}$: $\mathbb{R}/(x^2 + 2)$;

Over $\mathbb{C}$: no extension field exists for $\mathbb{C}$ since any polynomial is completely reducible over $\mathbb{C}$ (it is an *algebraically closed* field).