18-799F Algebraic Signal Processing Theory
Spring 2007
Solutions: Assignment 2

1. *(30 pts)*

   (a) $\mathrm{GL}_n(\mathbb{R})$ is not closed under matrix addition: for any $A \in \mathrm{GL}_n(\mathbb{R})$: $A + (-A) = 0 \notin \mathrm{GL}_n(\mathbb{R})$. On the other hand, $\mathrm{GL}_n(\mathbb{R})$ is closed under matrix multiplication, since for $A, B \in \mathrm{GL}_n(\mathbb{R})$: $\det AB = \det A \det B \Rightarrow AB \in \mathrm{GL}_n(\mathbb{R})$; although this operation is not commutative. Thus, the most structure $\mathrm{GL}_n(\mathbb{R})$ has is $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ is **a multiplicative group**.

   (b) Suppose $\frac{p(x)}{q(x)}, \frac{t(x)}{s(x)} \in S$. Then $\frac{p(x)}{q(x)} + \frac{t(x)}{s(x)} = \frac{p(x)s(x)+t(x)q(x)}{q(x)s(x)} \in S$ and $\frac{p(x)}{q(x)} \cdot \frac{t(x)}{s(x)} = \frac{p(x)t(x)}{q(x)s(x)} = \frac{t(x)}{s(x)} \cdot \frac{p(x)}{q(x)}$, because the set of zeros of $q(x)s(x)$ is just the union of the sets of zeros of $q(x)$ and $s(x)$. In addition, $0, 1 \in S$, and for any $\frac{p(x)}{q(x)} \in S$, its additive inverse is $-\frac{p(x)}{q(x)} \in S$. Additionally, S is obviously commutative. Since multiplicative inverse does not always exist (e.g. $x - 2$ does not have an inverse in S), S is a commutative ring. Moreover, notice that S does not have any zero divisors, so S is actually **an integral domain**.

   (c) Notice that S is not closed under addition: $\frac{x+1}{x-1} + \frac{1}{x-1} = \frac{x+2}{x-1} \notin S$. However, it is easy to verify that $(S, \cdot)$ is **a commutative group**.

   (d) S is not closed under addition: $x^k - x^k = 0 \notin S$. However, S is closed under multiplication: $x^k x^l = x^l x^k = x^{kl} \in S$. Also there is a neutral element $1 \in S$, as well as any $x^k \in S$ has an inverse $x^{-k} \in S$. Thus, S is **a commutative group**. In fact, $S = \langle x \rangle_{\text{group}}$.

2. *(21 pts)* Let's define $i = \sqrt{-1}$.

   (a) - $\mathbb{R}[x]$ and $\mathbb{C}$ are rings;
   - $\phi(p(x) + q(x)) = (p + q)(i) = p(i) + q(i) = \phi(p(x)) + \phi(q(x))$;
   - $\phi(p(x)q(x)) = (pq)(i) = p(i)q(i) = \phi(p(x))\phi(q(x))$.

   Thus, ϕ is a ring homomorphism.

   (b) For any $z \in \mathbb{C}$, define $p_z(x) = \mathrm{Re} z + x \mathrm{Im} z \in \mathbb{R}[x]$. Then $p(i) = z$. Thus, ϕ is surjective.

   (c) $\ker \phi = \{t(x) \mid t(x) \in \mathbb{R}[x], t(i) = 0\}$. Since $i \notin \mathbb{R}$, $-i$ must also be a root of $t(x) \in \ker \phi$. Thus, $(x - i)(x + i) = x^2 + 1 | t(x)$ for each $t(x) \in \ker \phi$. It implies that $\ker \phi = (x^2 + 1)\mathbb{R}[x]$.
   The homomorphism theorem yields $\mathbb{R}[x]/(x^2 + 1)\mathbb{R}[x] \simeq \mathrm{im}\phi = \mathbb{C}$

3. *(14 pts)* Consider the following mapping:

$$\begin{array}{rrcl} \phi: & \mathrm{GL}_n(\mathbb{R}) & \to & \mathbb{R} \setminus \{0\} \\ & A & \mapsto & \det A \end{array}$$

   Observe that

   - $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ and $(\mathbb{R} \setminus \{0\}, \cdot)$ are groups;
   - $\phi(AB) = \det AB = \det A \det B = \phi(A)\phi(B)$;
   - $\ker \phi = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det A = 1\} = \mathrm{SL}_n(\mathbb{R})$.
   - For any $r \in \mathbb{R} \setminus \{0\}$ there exists $A \in \mathrm{GL}_n(\mathbb{R})$ such that $\det A = r$, namely $A = diag(r, 1, \ldots, 1)$. Thus, $\mathrm{im}\phi = \mathbb{R} \setminus \{0\}$.

   Thus, ϕ is a group homomorphism with $\ker \phi = \mathrm{SL}_n(\mathbb{R})$. It follows that

   (a) $(\mathrm{SL}_n(\mathbb{R}), \cdot) = (\ker \phi, \cdot) \trianglelefteq (\mathrm{GL}_n(\mathbb{R}), \cdot)$; and using the homomorphism theorem,

   (b) $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \simeq (\mathbb{R} \setminus \{0\}, \cdot)$.

4. *(35 pts)*

(a) Assume, $p(x) \in \mathbb{C}[x]^\times$. Then there exists $q(x) \in \mathbb{C}[x]^\times$, such that $p(x)q(x) = 1$. However, $0 = \deg 1 = \deg p(x)q(x) = \deg p(x) + \deg q(x)$. This implies $\deg p(x) = \deg q(x) = 0$. Thus, $\mathbb{C}[x]^\times \subseteq \mathbb{C}$. On the other hand, for any $z \in \mathbb{C} \setminus \{0\}$ there is $\frac{1}{z} \in \mathbb{C} \setminus \{0\}$, such that $z\frac{1}{z} = 1$. Thus, $\mathbb{C} \setminus \{0\} \subseteq \mathbb{C}[x]^\times$. Since 0 does not have an inverse, we conclude that $\mathbb{C} \setminus \{0\} = \mathbb{C}[x]^\times$.

(b) Euclidean algorithm yields $\gcd(x^3 - x^2 + 2x - 2, x^2 - 1) = 3x - 3$:

$$\begin{aligned} x^3 - x^2 + 2x - 2 &= (x^2 - 1)(x - 1) + 3x - 3 \\ x^2 - 1 &= (3x - 3)\frac{1}{3}(x + 1) + 0 \end{aligned}$$

It follows that $(x^3 - x^2 + 2x - 2)\mathbb{C}[x] + (x^2 - 1)\mathbb{C}[x] = (3x - 3)\mathbb{C}[x] = (x - 1)\mathbb{C}[x]$.

(c) Since $p(x)\mathbb{C}[x]$ is a (two-sided) ideal in $\mathbb{C}[x]$, $\mathbb{C}[x]/p(x)\mathbb{C}[x]$ is a ring (with respect to addition and multiplication modulo $p(x)$).

(d) (i) For any $k \geq 0$, let $k = 4m + r$, where $m = \lfloor \frac{k}{4} \rfloor$ and $r = k \mod 4$. Then, using the assumption $x^4 - 1 = 0$,

$$\begin{aligned} x^k \mod (x^4 - 1) &= x^{4m+r} \mod (x^4 - 1) = (x^4)^m \cdot x^r \mod (x^4 - 1) \\ &= ((x^4 - 1) + 1)^m \cdot x^r \mod (x^4 - 1) = x^r = x^{k \mod 4}. \end{aligned}$$

(ii) For any $p(x) \in (\mathbb{C}[x]/(x^4 - 1)\mathbb{C}[x])^\times$ we have:

$$\begin{aligned} p(x) \in (\mathbb{C}[x]/(x^4 - 1)\mathbb{C}[x])^\times &\Leftrightarrow \exists q(x) \in (\mathbb{C}[x]/(x^4 - 1)\mathbb{C}[x])^\times : p(x)q(x) = 1 \mod (x^4 - 1) \\ &\Leftrightarrow p(x)q(x) = 1 + s(x)(x^4 - 1) \\ &\Leftrightarrow p(x)q(x) - s(x)(x^4 - 1) = 1 \\ &\Leftrightarrow \gcd(p(x), x^4 - 1) = 1. \end{aligned}$$

Thus, $(\mathbb{C}[x]/(x^4 - 1)\mathbb{C}[x])^\times = \{p(x) \mid p(x) \in \mathbb{C}[x]/((x^4 - 1)\mathbb{C}[x]), \gcd(p(x), x^4 - 1) = 1\}$. This is precisely the set of polynomials in $(\mathbb{C}[x]/(x^4 - 1)\mathbb{C}[x])^\times$ that have no zeros in $\{1, -1, i, -i\}$.

5. **Extra credit problem** *(20 pts)*

(a) $(R, +)$ is a commutative group under component-wise addition because each $(R_i, +)$, $i = 1, \ldots, n$ is a commutative group: for any $a, b, c \in R$

- $a + b \in R$;
- $(a + b) + c = (a_1 + b_1, \ldots, a_n + b_n) + (c_1, \ldots, c_n) = (a_1 + b_1 + c_1, \ldots, a_n + b_n + c_n) = (a_1, \ldots, a_n) + (b_1 + c_1, \ldots, b_n + c_n) = a + (b + c)$;
- $a + b = (a_1 + b_1, \ldots, a_n + b_n) = (b_1 + a_1, \ldots, b_n + a_n) = b + a$;
- Neutral element in R is $(0, \ldots, 0)$.

Multiplication is associative in R: $(ab)c = (a_1b_1, \ldots, a_nb_n)(c_1, \ldots, c_n) = (a_1b_1c_1, \ldots, a_nb_nc_n) = (a_1, \ldots, a_n)(b_1c_1, \ldots, b_nc_n) = a(bc)$.
Distributivity law holds: $(a + b)c = ((a_1 + b_1)c_1, \ldots, (a_n + b_n)c_n) = (a_1c_1 + b_1c_1, \ldots, a_nc_n + b_nc_n) = (a_1c_1, \ldots, a_nc_n) + (b_1c_1, \ldots, b_nc_n) = ac + bc$.
Multiplicative identity in R is $(1, \ldots, 1)$.
Thus, $(R, +, \cdot)$ is a ring.

(b) Recall that $\mathbb{C}[x]/p(x)\mathbb{C}[x] = \{q(x) \mid q(x) \in \mathbb{C}[x], \deg q(x) < \deg p(x)\}$. As we discussed in the class, it is a ring under addition and multiplication $\mod p(x)$. Also, in the previous problem we proved that $\bigoplus_{i=1}^n \mathbb{C}[x]/(x - \alpha_i)\mathbb{C}[x]$ is a ring. Thus, ϕ is a ring-to-ring mapping.
Next, we prove that ϕ is a ring homomorphism:

$$\begin{aligned} \phi(t(x) + s(x)) &= (t(\alpha_1) + s(\alpha_1), \ldots, t(\alpha_n) + s(\alpha_n)) \\ &= (t(\alpha_1), \ldots, t(\alpha_n)) + (s(\alpha_1), \ldots, s(\alpha_n)) = \phi(t(x)) + \phi(s(x)); \\ \phi(t(x)s(x)) &= (t(\alpha_1)s(\alpha_1), \ldots, t(\alpha_n)s(\alpha_n)) = (t(\alpha_1), \ldots, t(\alpha_n))(s(\alpha_1), \ldots, s(\alpha_n)) = \phi(t(x))\phi(s(x)). \end{aligned}$$

Recall that any polynomial $s(x)$, such that $\deg s(x) < n = \deg p(x)$ is uniquely defined by its values in n points. This fact is known as *the Unisolvence Theorem* and is used in polynomial interpolation. The only such $s(x)$ that maps n points to 0 is a zero polynomial. Thus, ϕ is injective because $\ker \phi = \{0\}$.

ϕ is also surjective for the above reason: for any $(\beta_1, \ldots, \beta_n) \in \bigoplus_{i=1}^n \mathbb{C}[x]/(x-\alpha_i)\mathbb{C}[x]$, there is a polynomial $s(x) \in (\mathbb{C}[x]/p(x)\mathbb{C}[x])$ that maps α_i to β_i $(i = 1, \ldots, n)$.

So, ϕ is a bijective ring homomorphism, i.e. ϕ is an isomorphism. Thus,

$$\mathbb{C}[x]/p(x)\mathbb{C}[x] \cong \bigoplus_{i=1}^{n} \mathbb{C}[x]/(x-\alpha_i)\mathbb{C}[x].$$