18-799F Algebraic Signal Processing Theory
Spring 2007
Assignment 2
Due Date: Feb. 7th 2:30pm (at the beginning of class)

1. *(30 pts)* Describe the structure of the following sets S with respect to addition and multiplication. Possible answers may include (but are not limited to):

   - $(S, +)$ is a group;
   - $(S, +)$ is a commutative group;
   - $(S, +, \cdot)$ is a ring;
   - $(S \setminus \{0\}, \cdot)$ is a group;
   - $(S \setminus \{0\}, \cdot)$ is a commutative group;
   - $(S, \cdot)$ is a commutative group;
   - $(S, +, \cdot)$ is a field.

   Only state the "most structure." Briefly explain why the set has the structure and give counterexamples to show that is has not more structure. (The comments in the parentheses make a loose connection to signal processing.)

   Additional information: As you know, α_i is a *zero* of a polynomial $f(x)$ if $f(\alpha_i) = 0$; in this case, if $deg(f) = n$ and $\alpha_i,\ i = 1 \dots n$, are the zeros of $f(x)$, you can write the polynomial as $f(x) = \prod_{i=0}^{n} (x - \alpha_i)$.

   (a) The set of real invertible matrices of size $n \times n$: $GL_n(\mathbb{R}) = \{A \in \mathbb{R}^{n \times n} \mid \text{exists } A^{-1} \in \mathbb{R}^{n \times n}\}$.

   (b) *(stable IIR filters)* Set of complex rational functions $S = \{\frac{p(x)}{q(x)} \mid p(x), q(x) \in \mathbb{C}[x],\ q(x) \neq 0, \text{ for every zero } \alpha \text{ of } q(x) : |\alpha| \leq 1\}$.

   (c) *(minimum-phase filters)* Set of complex rational functions $S = \{\frac{p(x)}{q(x)} \mid p(x), q(x) \in \mathbb{C}[x],\ q(x) \neq 0, \text{ for every zero } \alpha \text{ of } p(x) \text{ or } q(x) : |\alpha| \leq 1\}$.

   (d) *(shifts)* $S = \{x^n \mid n \in \mathbb{Z}\}$.

2. *(21 pts)*

   (a) Show that
   $$\phi: \ \mathbb{R}[x] \to \mathbb{C}, \quad p(x) \mapsto p(\sqrt{-1})$$
   is a ring homomorphism.

   (b) Show that ϕ is surjective.

   (c) Determine the kernel of ϕ and apply the homomorphism theorem to ϕ.

3. *(14 pts)* Recall that for square matrices $A, B \in \mathbb{R}^{n \times n}$, $\det(AB) = \det(A)\det(B)$ and $\det(A^{-1}) = \det(A)^{-1}$ (provided A is invertible).

   Let $SL_n(\mathbb{R}) = \{A \in \mathbb{R}^{n \times n} \mid det(A) = 1\}$. Show that

   (a) $(SL_n(\mathbb{R}), \cdot) \trianglelefteq (GL_n(\mathbb{R}), \cdot)$.

   (b) $(GL_n(\mathbb{R})/SL_n(\mathbb{R}), \cdot) \simeq (\mathbb{R} \setminus \{0\}, \cdot)$. (Hint: define a suitable homomophism and apply the homomorphism theorem).

4. *(35 pts)* In the class we asserted that $\mathbb{C}[x]$ is a Euclidean ring with respect to the usual polynomial division with rest and $\delta = deg$ (the degree, defined as $\deg(\sum_{i=0}^{n} a_i x^i) = n$.

   (a) Determine $\mathbb{C}[x]^\times$.

(b) Find $\gcd(x^3 - x^2 + 2x - 2, x^2 - 1)$ using the Euclidean algorithm. Write $(x^3 - x^2 + 2x - 2)\mathbb{C}[x] + (x^2 - 1)\mathbb{C}[x]$ as a principal ideal.

(c) Explain why $\mathbb{C}[x]/p(x)\mathbb{C}[x]$ is a ring with respect to addition and multiplication for any $p(x) \in \mathbb{C}[x]$.

(d) Recall that we can write $\mathbb{Z}/n\mathbb{Z} = \{[0], \dots, [n-1]\}$ simply as the set $\{0, \dots, n-1\}$ with addition and multiplication *mod* n. Similarly, we can view $\mathbb{C}[x]/p(x)\mathbb{C}[x]$ as the set of polynomials $\{q(x) \in \mathbb{C}[x] \mid deg(q) < deg(p)\}$ with addition and multiplication performed *mod* $p(x)$.

  (i) Compute x^i (for $i \geq 0$) in $\mathbb{C}[x]/((x^4 - 1)\mathbb{C}[x])$.

  (ii) Describe $(\mathbb{C}[x]/(x^4 - 1)\mathbb{C}[x])^\times$. What can you say about the zeros of its elements?

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

(a) Consider rings $(R_1, +, \cdot), \dots, (R_n, +, \cdot)$. Show that their Cartesian product $R = R_1 \times \cdots \times R_n = \{(a_1, \dots, a_n) \mid a_i \in R_i\}$ is also a ring with respect to component-wise addition and multiplication. What are its neutral elements with respect to addition and multiplication (i.e. its *zero* and *one*)?

(b) Consider $p(x) = \prod_{i=1}^n (x - \alpha_i) \in \mathbb{C}[x]$ with pairwise distinctive zeros (i.e. $i \neq j \Rightarrow \alpha_i \neq \alpha_j$). Prove that the mapping

$$\begin{array}{rrcl} \phi: & \mathbb{C}[x]/(p(x)\mathbb{C}[x]) & \to & \mathbb{C}[x]/(x - \alpha_1)\mathbb{C}[x] \times \cdots \times \mathbb{C}[x]/(x - \alpha_n)\mathbb{C}[x] \\ & q(x) & \mapsto & (q(\alpha_1), \dots, q(\alpha_n)) \end{array}$$

is a ring isomorphism. This fact is known as *Chinese Remainder Theorem*.