18-799F Algebraic Signal Processing Theory
Spring 2007
Assignment 1
Due Date: Jan. 31st 2:30pm (at the beginning of class)

1. *(15 pts)* Let $C_6 = \langle x \mid x^6 = 1 \rangle$ be the cyclic group of order 6.
   (a) Determine all subgroups (including the trivial ones $\langle 1 \rangle$ and C_6) of C_6.
   (b) For each subgroup, determine the minimum set of generators.
   (c) Express each subgroup using generators and relations.

2. *(12 pts)* The function $\cos : \mathbb{R} \to [-1, 1]$ induces the following equivalence relation on $\mathbb{R}$:
$$x \sim y \Leftrightarrow \cos x = \cos y.$$
   (a) Determine the partition $\mathbb{R}/\cos$ of $\mathbb{R}$ induced by cos.
   (b) Determine the canonical factorization of cos and draw the associated commutative diagram.

3. *(17 pts)* Which of the following is well-defined (give a counterexample or prove)?
   (a) The operation $[x] \cdot [y] = [xy]$ on $\mathbb{Z}/n\mathbb{Z}$.
   Is $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ a group? Explain your answer.
   (b) The function
$$f\colon \begin{array}{rcl} \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ [x] & \mapsto & [x^2] \end{array}$$
   (c) The function
$$f\colon \begin{array}{rcl} \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ [x] & \mapsto & [x+1] \end{array}$$

4. *(10 pts)* Consider the set of all rational numbers (excluding zero) with multiplication: $(\mathbb{Q} \setminus \{0\}, \cdot)$.
   (a) Show that $(\mathbb{Q} \setminus \{0\}, \cdot)$ is a group.
   (b) What are the generators of this group? Explain your answer.

5. *(20 pts)* Consider the dihedral group of order 8: $D_8 = \langle x, y \mid x^4 = y^2 = 1, xy = yx^{-1} \rangle$. As we discussed in the class, this is the group of symmetries of a square (x is a 90-degree rotation, and y is a reflection.) Obviously, one of its subgroups is a cyclic group of order 4: $C_4 = \langle x \mid x^4 = 1 \rangle \leq D_8$.
   (a) What is the index of C_4 in D_8?
   (b) Express D_8 as a union of left cosets of C_4.
   (c) What are the elements of D_8 (expressed in x and y)?
   (d) Prove that $C_4 \trianglelefteq D_8$.

6. *(15 pts)* $\mathbb{R}[x] = \{p(x) = \sum_{i=0}^{n} a_i x^i \mid n \in \mathbb{N}_0, a_i \in \mathbb{R}\}$ is the set of all polynomials with real coefficients ($\mathbb{N}_0 = \{0, 1, \dots\}$).
   For two polynomials $p(x), q(x) \in \mathbb{R}[x]$ we say that $p(x)$ *divides* $q(x)$ if $q(x) = p(x)r(x)$ for some $r(x) \in \mathbb{R}[x]$. We write this as $p(x) \mid q(x)$.
   (a) Let us fix some $p(x) \in \mathbb{R}[x]$. Prove that the following is an equivalence relation on $\mathbb{R}[x]$:
$$r(x) \sim s(x) \Leftrightarrow p(x) | (r(x) - s(x)).$$
   (b) Consider the group $(\mathbb{R}[x], +)$. Find a subgroup $H \leq \mathbb{R}[x]$, such that for $\sim$ defined above,
$$\mathbb{R}/\sim \; = \mathbb{R}[x]/H$$
   and show this holds.

(c) Is $(\mathbb{R}[x]/H, +)$ a group? Explain your answer.

7. *(11 pts)* Let $G = \{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{R}\}$.

   (a) Show that G is a group with respect to the multiplication $\cdot$ of matrices.

   (b) Show that

$$\begin{array}{cccc} \phi: & (\mathbb{R}, +) & \to & (G, \cdot) \\ & x & \mapsto & \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \end{array}$$

   is an isomorphism.

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

   (a) Let $H \leq G$ is of index 2 in G. Prove that $H \trianglelefteq G$.

   (b) Prove that $C_n = \langle x \mid x^n = 1 \rangle$ does not have non-trivial subgroups if and only if n is prime.
   Note: This shows that C_p, p prime, are *simple* groups, the only abelian ones in fact.