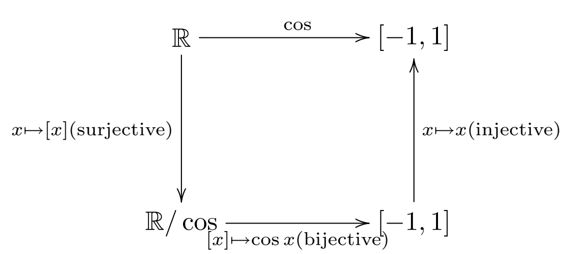
18-799F Algebraic Signal Processing Theory
Spring 2007
Solutions: Assignment 1

1. *(15 pts)*
   (a) $\langle 1\rangle = \{1\}$;
   $\langle x\rangle = \langle x^5\rangle = C_6$;
   $\langle x^2\rangle = \langle x^4\rangle = \{1, x^2, x^4\}$;
   $\langle x^3\rangle = \{1, x^3\}$.
   (b) $\langle 1\rangle : \{1\}$;
   $C_6 : \{x\}$ or $\{x^5\}$;
   $\langle x^2\rangle : \{x^2\}$ or $\{x^4\}$;
   $\langle x^3\rangle : \{x^3\}$.
   (c) $\langle 1\rangle = \{1\}$;
   $\langle x\rangle = \langle x^5\rangle = C_6 = \{x \mid x^6 = 1\}$;
   $\langle x^2\rangle = \langle x^4\rangle = \{x^2 \mid x^6 = 1\}$; setting $y = x^2$ yields $C_3 = \{y \mid y^3 = 1\}$;
   $\langle x^3\rangle = \{x^3 \mid x^6 = 1\}$; setting $y = x^3$ yields $C_2 = \{y \mid y^2 = 1\}$;

2. *(12 pts)*
   (a) Recall that $\cos x = \cos -x$ and $cosx = cosx + 2\pi k$ for $k \in \mathbb{Z}$. Then the partition is

   $$\mathbb{R}/\sim = \{[x] \mid x \in [0,\pi]\}, \text{ where } [x] = \{\pm x + 2\pi k, k \in \mathbb{Z}.\}$$

   (b) The commutative diagram for cos is:



3. *(17 pts)*
   (a) The operation is well-defined:
   Choose arbitrary $u \in [x]$ and $v \in [y]$. Then $u = x + kn$ and $v = y + ln$. Their product $uv = (x+kn)(y+ln) = xy+n(xl+ky+kln) \in [xy]$, thus $[uv] = [xy]$. So, the definition of the operation is independent of the chosen representatives.
   $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ is not a group because $[0] \in \mathbb{Z}/n\mathbb{Z}$ does not have an inverse.
   (b) The function is well-defined:
   Choose arbitrary $u \in [x]$. Then $u = x + kn$ and $u^2 = (x + kn)^2 = x^2 + n(2kx + k^2 n) \in [x^2]$, thus $[u^2] = [x^2]$. So, the definition of the function is independent of the chosen representative.
   (c) The function is well-defined:
   Choose arbitrary $u \in [x]$. Then $u = x + kn$ and $u + 1 = (x + kn) + 1 = (x + 1) + kn \in [x + 1]$, thus $[u + 1] = [x + 1]$. So, the definition of the function is independent of the chosen representative.

4. *(10 pts)*
   (a) (i) $\mathbb{Q}\backslash\{0\}$ is closed under multiplication.
   (ii) Multiplication of rational numbers is an associative operation.

(iii) Neutral element is $1 \in \mathbb{Q}\backslash\{0\}$.
(iv) For any $\frac{p}{q} \in \mathbb{Q}\backslash\{0\}$ its inverse it $\frac{q}{p} \in \mathbb{Q}\backslash\{0\}$.

(b) The minimal set of generators is $\{-1, p \mid p \in \mathbb{N}, p \text{ is prime}\}$.

5. *(20 pts)*

(a) $|D_8/C_4| = |D_8|/|C_4| = 2$.

(b) $D_8 = C_4 \cup yC_4$ since $y \notin C_4$.

(c) From b) we immediately see that $D_8 = \{1, x, x^2, x^3, x^4, yx, yx^2, yx^3, yx^4\}$.

(d) Two solutions:

(i) Use the solution of problem 8a (provided you solved the problem).

(ii) To show that $C_4 \trianglelefteq D_8$, we need to prove that for any $z \in D_8$: $zC_4z^{-1} = C_4$.
Case 1: $z = x^i$. Then $zC_4z^{-1} = \{x^ix^{-i}, x^ixx^{-i}, x^ix^2x^{-i}, x^ix^3x^{-i}\} = \{1, x, x^2, x^3\} = C_4$.
Case 2: $z = yx^i$. Since $xy = yx^{-1}$ and $(yx^i)^{-1} = x^{-i}y^{-1}$,

$$\begin{aligned} zC_4z^{-1} &= \{yx^ix^{-i}y^{-1}, yx^ixx^{-i}y^{-1}, yx^ix^2x^{-i}y^{-1}, yx^ix^3x^{-i}y^{-1}\} \\ &= \{1, x^{-1}, x^{-2}, x^{-3}\} = \{1, x^3, x^2, x\} = C_4. \end{aligned}$$

6. *(15 pts)*

(a) This is an equivalence relation because it is:

i. Reflexive: $p(x)|(s(x) - s(x)) \Rightarrow s(X) \sim s(x)$;

ii. Symmetric: $s(x) \sim q(x) \Rightarrow p(x)|(s(x) - q(x)) \Rightarrow p(x)|(q(x) - s(x)) \Rightarrow q(x) \sim s(x)$;

iii. Transitive: $s(x) \sim q(x), q(x) \sim r(x) \Rightarrow p(x)|(s(x) - q(x)), p(x)|(q(x) - r(x)) \Rightarrow p(x)|(s(x) - q(x) + q(x) - r(x)) \Rightarrow p(x)|(s(x) - r(x)) \Rightarrow s(x) \sim r(x)$.

(b) $H = \{s(x) \mid s(x) \text{ is such that } p(x)|s(x)\} = p(x)\mathbb{R}[x]$. This yields $r(x) \sim s(x) \Leftrightarrow p(x)|(r(x) - s(x)) \Leftrightarrow (r(x) - s(x)) \in H \Leftrightarrow r(x) + H = s(x) + H$.

(c) Since $(\mathbb{R}[x], +)$ is commutative and $(H, +) \trianglelefteq (\mathbb{R}[x], +)$, then $\mathbb{R}[x]/H$ is a group under addition.

7. *(11 pts)*

(a) G is closed under matrix multiplication: for any $x, y \in \mathbb{R}$: $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix} \in G$.

The neutral element is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G$.

Any element in G has an inverse, namely, for any $x \in \mathbb{R}$: $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Thus, G is a group under matrix multiplication.

(b) ϕ is a bijection, because it is

injective: for $x, y \in \mathbb{R}, x \neq y$, $\phi(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \phi(y)$;

surjective: for any $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, there is $x \in \mathbb{R}$, such that $\phi(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$.

ϕ is also a homomorphism since $\phi(x+y) = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \phi(x)\phi(y)$. Since ϕ is a bijective homomorphism, it is an isomorphism.

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

(a) Since $|G/H| = 2$, then $G = H \cup gH = H \cup gH$ for any $g \in G \setminus H$. Thus, $gH = Hg$ for any $g \in G \setminus H$. On the other hand, since H is a subgroup, $gH = Hg$ for any $g \in H$. Thus $gH = Hg$ for any $g \in G \setminus H \cup H = G$, and H is normal in G.

(b) We need to prove the following statement (which is equivalent to the problem question): C_n has non-trivial subgroups iff n is not prime.

Proof:

⇒: If C_n has a non-trivial subgroup $H < C_n$, then $n = |C_n| = |C_n/H| \cdot |H|$. Since $|H| \neq 1$, $|H| \neq n$, and $|H|$ divides n, n is a composite number.

⇐: If $n = km$ is not prime, then C_n has a proper (non-trivial) subgroup $H < G$ of order $m \neq 1, n$. In particular, a cyclic group of order k is a proper subgroup of C_n: $H = \langle x^m \mid x^n = 1 \rangle = \langle y \mid y^k = 1 \rangle < C_n$.