MAT217 HW 6
Due Tues. Mar. 26, 2013

1. Read Section 1.6 in Hoffman-Kunze and do exercises 3 and 9.

2. Prove that S_n, the set of permutations on n letters, is a group under composition. Show that S_n is abelian (its multiplication is commutative) if and only if $n < 3$.

3. Let $f : S_n \to \mathbb{Z}$ be a function that is multiplicative; that is, $f(\sigma\tau) = f(\sigma)f(\tau)$. Show that f must be one of the following three functions: identically zero, identically 1 or the signature function.

4. List the elements of S_4 and state which are odd and which are even.

5. Show that any element of S_n can be written as a product of disjoint cycles.

6. Show that if $T \subset S_n$ is a subgroup (a subset that is also a group under composition) and T contains both (12) and $(12 \cdots n)$ then $T = S_n$.

   Hint. If $\sigma \in S_n$ then what is the relation between the cycle decomposition of π and that of $\sigma^{-1}\pi\sigma$?

7. (From Hoffman-Kunze) Let $\mathbb{F}$ be a field and $f : \mathbb{F}^2 \to \mathbb{F}$ be a 2-linear alternating function. Show that

$$f\left(\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix}\right) = (ad - bc) f(e_1, e_2) \ ,$$

   where e_i is the vector with a 1 in the i-th spot and a zero in the other. Find an analogous formula for a 3-linear alternating function from $\mathbb{F}^3$ to $\mathbb{F}$.

8. Let $\mathbb{F}$ be a field and write $\mathbb{F}[x]$ for the set of polynomials with coefficients in $\mathbb{F}$. Define $\deg(p)$ for the degree of $p \in \mathbb{F}[x]$: the largest k such that the coefficient of x^k in p is nonzero. The degree of the zero polynomial is defined to be $-\infty$.

   (a) Show that for $p, q \in \mathbb{F}[x]$, the product pq has degree $\deg(pq) = \deg(p) + \deg(q)$.

   (b) Show that for $p, d \in \mathbb{F}[x]$ such that d is nonzero, there exist $q, r \in \mathbb{F}[x]$ such that $p = qd + r$ and $\deg(r) < \deg(d)$. (This result is called the *division algorithm.*)

   Hint. We may assume that $\deg(p) \geq 0$, for otherwise we can choose $r = q = 0$. Also we can assume $\deg(d) \leq \deg(p)$, or else we choose $q = 0$ and $r = p$. So use induction on $\deg(p)$, starting with $\deg(p) = 0$, meaning that $p(x) = c$ for some nonzero $c \in \mathbb{F}$. For the inductive step, if $\deg(p) > 0$, find some $q_1 \in \mathbb{F}[x]$ such that $\deg(p - q_1 d) < \deg(p)$ and continue.

9. Show that if $p \in \mathbb{F}[x]$ and $c \in \mathbb{F}$ then $p(c) = 0$ if and only if the polynomial $x - c$ divides p (that is, we can find $d \in \mathbb{F}[x]$ such that $(x - c)d = p$).

10. Let $p, q \in \mathbb{F}[x]$ be nonzero and define the subset $\mathcal{S}$ of $\mathbb{F}[x]$ as

$$\mathcal{S} = \{ap + bq : a, b \in \mathbb{F}[x]\} .$$

(a) Let $d \in \mathcal{S}$ be nonzero of minimal degree. Show that d divides both p and q (see the definition of "divides" in exercise 9).

(b) Show that if $s \in \mathbb{F}[x]$ divides both p and q then s divides d.

(c) Conclude that there exists a unique monic polynomial (that is, with leading coefficient 1) $d \in \mathbb{F}[x]$ satisfying:

i. d divides both p and q and

ii. if $s \in \mathbb{F}[x]$ divides both p and q then s divides d.

(This d is called the *greatest common divisor* of p and q.)