Math 562/662 **Spring 2022**
Homework 1 **Drew Armstrong**

---

1. Lexicographic Degree. Given $\mathbf{k} = (k_1, \ldots, k_n), \boldsymbol{\ell} = (\ell_1, \ldots, \ell_n) \in \mathbb{N}^n$ we say that

$$\mathbf{k} < \boldsymbol{\ell} \quad \Leftrightarrow \quad \text{there exists } j \text{ such that } k_i = \ell_i \text{ for all } i < j, \text{ but } k_j < \ell_j.$$

Given $f(x_1, \ldots, x_n) = \sum_{\mathbf{k} \in \mathbb{N}^n} a_{\mathbf{k}} \mathbf{x}^{\mathbf{k}} \in \mathbb{F}[\mathbf{x}]$ we define $\deg(f)$ as the lexicographically biggest element $\mathbf{k} \in \mathbb{N}^d$ such that $a_{\mathbf{k}} \neq 0$. The degree of the zero polynomial is not defined.

(a) For all $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{N}^n$ prove that $\mathbf{a} \leq \mathbf{b}$ and $\mathbf{b} \leq \mathbf{c}$ imply $\mathbf{a} \leq \mathbf{c}$. [Hint: If $\mathbf{a} = \mathbf{b}$ or $\mathbf{b} = \mathbf{c}$ then there is nothing to show, so we can assume that $\mathbf{a} < \mathbf{b}$ and $\mathbf{b} < \mathbf{c}$.]

(b) For all $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{N}^n$, show that $\mathbf{a} \leq \mathbf{b}$ implies $\mathbf{a} + \mathbf{c} \leq \mathbf{b} + \mathbf{c}$. [Hint: It is easier to prove that $\mathbf{a} + \mathbf{c} > \mathbf{b} + \mathbf{c}$ implies $\mathbf{a} > \mathbf{b}$.]

(c) For all nonzero $f(\mathbf{x}), g(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$, prove that $\deg(fg) = \deg(f) + \deg(g)$. [Hint: If $a_{\mathbf{k}}, b_{\boldsymbol{\ell}} \in \mathbb{F}$ are the coefficients of $f(\mathbf{x}), g(\mathbf{x})$ then $c_{\mathbf{m}} = \sum_{\mathbf{k} + \boldsymbol{\ell} = \mathbf{m}} a_{\mathbf{k}} b_{\boldsymbol{\ell}}$ are the coefficients of $f(\mathbf{x})g(\mathbf{x})$. Let $\mathbf{d} = \deg(f)$ and $\mathbf{e} = \deg(g)$ so that $\mathbf{k} > \mathbf{d}$ implies $a_{\mathbf{k}} = 0$ and $\boldsymbol{\ell} > \mathbf{e}$ implies $b_{\boldsymbol{\ell}} = 0$. Use parts (a) and (b) to show that $\mathbf{m} > \mathbf{d} + \mathbf{e}$ implies $c_{\mathbf{m}} = 0$.]

2. Introduction to Permutations. Let S_3 be the set of invertible functions from the set $\{1, 2, 3\}$ to itself. These are called *permutations of* $\{1, 2, 3\}$.

(a) List all 6 elements of this set. [I recommend using cycle notation.]

(b) We can think of $(S_3, \circ, \mathrm{id})$ as a group, where $\circ$ is functional composition and id is the identity function defined by $\mathrm{id}(1) = 1$, $\mathrm{id}(2) = 2$ and $\mathrm{id}(3) = 3$. Write out the full 6×6 group table. Observe that this group is not abelian.

3. The Alternating Group. Let $(ij) \in S_n$ denote the permutation of $\{1, \ldots, n\}$ that switches $i \leftrightarrow j$ and sends every other number to itself. Such elements are called *transpositions*. Observe that each transposition is equal to its own inverse.

(a) Prove that every element of S_n can be expressed as a composition of transpositions. [Hint: Prove that every cycle is a composition of transpositions. By convention, the identity permutation is the composition of zero transpositions.]

(b) Let $A_n \subseteq S_n$ denote the subset of permutations that can be expressed as a composition of an **even number** of transpositions. Prove the following properties:

- $\mathrm{id} \in A_n$,
- $\sigma, \tau \in A_n \Rightarrow \sigma \circ \tau \in A_n$,
- $\sigma \in A_n \Rightarrow \sigma^{-1} \in A_n$.

These properties say that A_n is a *subgroup* of S_n. We call it the *alternating subgroup of* S_n, or just the *alternating group*.

4. Waring's Algorithm. Let $\mathbb{E} \supseteq \mathbb{F}$ be a field extension. Suppose that the polynomial $f(x) = x^3 + ax^2 + bx + c \in \mathbb{F}[x]$ has roots $\alpha, \beta, \gamma \in \mathbb{E}$, so that

$$x^3 + ax^2 + bx + c = (x - \alpha)(x - \beta)(x - \gamma).$$

Use Waring's algorithm to find a polynomial in $\mathbb{F}[x]$ whose roots are $\alpha^2, \beta^2, \gamma^2$. [Hint: The coefficients of $(x - \alpha^2)(x - \beta^2)(x - \gamma^2)$ are symmetric combinations of α, β, γ, hence we can express them in terms of the coefficients a, b, c, which are in $\mathbb{F}$.]