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 $c_{\mathbf{m}} = 0$.]

(a): If $\mathbf{a} = \mathbf{b}$ or $\mathbf{b} = \mathbf{c}$ then there is nothing to show. So let us assume that $\mathbf{a} < \mathbf{b}$ and $\mathbf{b} < \mathbf{c}$. By definition, this means that there exist some j and k satisfying

- $a_j < b_j$ and $a_i = b_i$ for all $i < j$,
- $b_k < c_k$ and $b_i = c_i$ for all $i < k$.

Now let $m = \min\{j, k\}$, so that $a_i = b_i = c_i$ for all $i < m$. If $m = j = k$ then we have $a_m < b_m < c_m$. If $m = j < k$ then we have $a_m < b_m = c_m$. If $m = k < j$ then we have $a_m = b_m < c_m$. In any case, we have $a_m < c_m$. Since $a_m < c_m$ and $a_i = c_i$ for all $i < m$ we conclude that $\mathbf{a} < \mathbf{c}$ (and hence $\mathbf{a} \leq \mathbf{c}$) as desired.

(b): Suppose that $\mathbf{a} + \mathbf{c} > \mathbf{b} + \mathbf{c}$. By definition, this means that there exists some j such that $a_j + c_j > b_j + c_j$ and $a_i + c_i = b_i + c_i$ for all $i < j$. The first condition implies $a_j > b_j$ and the second condition implies $a_i = b_i$ for all i. Hence $\mathbf{a} > \mathbf{b}$ as desired.

(c): Let us write $f(\mathbf{x}) = \sum_{\mathbf{k} \in \mathbb{N}^n} a_{\mathbf{k}} \mathbf{x}^{\mathbf{k}}$ and $g(\mathbf{x}) = \sum_{\boldsymbol{\ell} \in \mathbb{N}^n} b_{\boldsymbol{\ell}} \mathbf{x}^{\boldsymbol{\ell}}$, with $\deg(f) = \mathbf{d} \in \mathbb{N}^n$ and $\deg(g) = \mathbf{e} \in \mathbb{N}^n$. By definition, this means that

- $a_{\mathbf{d}} \neq 0$ and $a_{\mathbf{k}} = 0$ for all $\mathbf{k} > \mathbf{d}$,
- $b_{\boldsymbol{\ell}} \neq 0$ and $b_{\boldsymbol{\ell}} = 0$ for all $\boldsymbol{\ell} > \mathbf{e}$.

The product is given by $f(\mathbf{x})g(\mathbf{x}) = \sum_{\mathbf{m} \in \mathbb{N}^n} c_{\mathbf{m}} \mathbf{x}^{\mathbf{m}}$, with coefficients

$$c_{\mathbf{m}} = \sum_{\mathbf{k}+\boldsymbol{\ell}=\mathbf{m}} a_{\mathbf{k}} b_{\boldsymbol{\ell}} \in \mathbb{F}.$$

Our goal is to show that $\deg(fg) = \mathbf{d} + \mathbf{e}$. In other words, we want to show that $c_{\mathbf{d}+\mathbf{e}} \neq 0$ and that $\mathbf{m} > \mathbf{d} + \mathbf{e}$ implies $c_{\mathbf{m}} = 0$.

For the first condition, we observe that

$$c_{\mathbf{d}+\mathbf{e}} = \sum_{\mathbf{k}+\boldsymbol{\ell}=\mathbf{d}+\mathbf{e}} a_{\mathbf{k}} b_{\boldsymbol{\ell}} \in \mathbb{F}.$$

Since $a_{\mathbf{d}} \neq 0$ and $b_{\mathbf{e}} \neq 0$, the summand $a_{\mathbf{d}} b_{\mathbf{e}}$ is nonzero. But I claim that every other summand is zero. Indeed, suppose that $\mathbf{k} + \boldsymbol{\ell} = \mathbf{d} + \mathbf{e}$ with $\mathbf{k} \neq \mathbf{d}$ or $\boldsymbol{\ell} \neq \mathbf{e}$, which implies that $\mathbf{k} \neq \mathbf{d}$

and $\boldsymbol{\ell} \neq \mathbf{e}$. If $\mathbf{k} > \mathbf{d}$ then by definition of $\deg(f)$ we have $a_{\mathbf{k}} = 0$, hence the summand $a_{\mathbf{k}} b_{\boldsymbol{\ell}}$ is zero. And if $\mathbf{k} < \mathbf{d}$ then from (b) we must have $\boldsymbol{\ell} > \mathbf{e}$ because

$$\begin{aligned} \mathbf{k} &< \mathbf{d} \\ \mathbf{k} + \boldsymbol{\ell} &< \mathbf{d} + \boldsymbol{\ell} && \text{add } \boldsymbol{\ell} \text{ to both sides} \\ \mathbf{d} + \mathbf{e} &< \mathbf{d} + \boldsymbol{\ell} && \text{because } \mathbf{k} + \boldsymbol{\ell} = \mathbf{d} + \mathbf{e} \\ \mathbf{e} &< \boldsymbol{\ell}. && \text{add } -\mathbf{d} \text{ to both sides} \end{aligned}$$

In this case we have $b_{\boldsymbol{\ell}} = 0$, hence the summand $a_{\mathbf{k}} b_{\boldsymbol{\ell}}$ is still zero. Since all but one summand in $c_{\mathbf{d}+\mathbf{e}}$ is zero and the last is nonzero, we conclude that $c_{\mathbf{d}+\mathbf{e}} \neq 0$ as desired.

For the second condition we want to show that $\mathbf{m} > \mathbf{d} + \mathbf{e}$ implies $c_{\mathbf{m}} = 0$. In this case, every summand in $c_{\mathbf{m}}$ has the form $a_{\mathbf{k}} b_{\boldsymbol{\ell}}$ for some $\mathbf{k}, \boldsymbol{\ell}$ with $\mathbf{k} + \boldsymbol{\ell} = \mathbf{m} > \mathbf{d} + \mathbf{e}$. We will be done if we can show that $\mathbf{k} + \boldsymbol{\ell} > \mathbf{d} + \mathbf{e}$ implies $\mathbf{k} > \mathbf{d}$ or $\boldsymbol{\ell} > \mathbf{e}$ since this implies that at least one of $a_{\mathbf{k}}$ and $b_{\boldsymbol{\ell}}$ is zero, hence $a_{\mathbf{k}} b_{\boldsymbol{\ell}} = 0$. In this case every summand $a_{\mathbf{k}} b_{\boldsymbol{\ell}}$ of $c_{\mathbf{m}}$ is zero, hence $c_{\mathbf{m}} = 0$. It is equivalent to prove the contrapositive statement: that $\mathbf{k} \leq \mathbf{d}$ and $\boldsymbol{\ell} \leq \mathbf{e}$ imply $\mathbf{k} + \boldsymbol{\ell} \leq \mathbf{d} + \mathbf{e}$. So let us suppose that $\mathbf{k} \leq \mathbf{d}$ and $\boldsymbol{\ell} \leq \mathbf{e}$. In this case, (b) implies that

$$\left\{ \begin{array}{ccc} \mathbf{k} & \leq & \mathbf{d} \\ \mathbf{k} + \boldsymbol{\ell} & \leq & \mathbf{d} + \boldsymbol{\ell} \end{array} \right\} \quad \text{and} \quad \left\{ \begin{array}{ccc} \boldsymbol{\ell} & \leq & \mathbf{e} \\ \mathbf{d} + \boldsymbol{\ell} & \leq & \mathbf{d} + \mathbf{e} \end{array} \right\},$$

and then since $\mathbf{k} + \boldsymbol{\ell} \leq \mathbf{d} + \boldsymbol{\ell} \leq \mathbf{d} + \mathbf{e}$, part (a) implies that $\mathbf{k} + \boldsymbol{\ell} \leq \mathbf{d} + \mathbf{e}$. □

I think that was a wholesome exercise.

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 $3! = 6$ 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.

(a): I will list the permutations in one-line notation and in cycle notation:

one-line	123	213	132	321	231	312
cycle	id	(12)	(23)	(13)	(123)	(132)

(b): Here is the group table, where the entry in row σ and column τ is $\sigma \circ \tau$:

$\circ$	id	(12)	(13)	(23)	(123)	(132)
id	id	(12)	(13)	(23)	(123)	(132)
(12)	(12)	id	(132)	(123)	(23)	(13)
(13)	(13)	(123)	id	(132)	(12)	(23)
(23)	(23)	(132)	(123)	id	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	id
(132)	(132)	(23)	(12)	(13)	id	(123)

The group is not abelian since, for example, we have $(12) \circ (23) = (132)$ and $(23) \circ (12) = (123)$, but $(123) \neq (132)$.

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:

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

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*.

(a): The cycle notation is has the property that it can be viewed as a composition of commuting cycles. For example, we have

$$(137)(256)(48) = (137) \circ (256) \circ (48) = (48) \circ (137) \circ (256) = (562) \circ (84) \circ (712) = \text{etc.}$$

We will show that each cycle can be viewed as a composition of (non-commuting) transpositions. For example, we have seen that $(123) = (12) \circ (23)$. One can similarly check that

$$\begin{aligned} (1234) &= (12) \circ (23) \circ (34), \\ (12335) &= (12) \circ (23) \circ (34) \circ (45), \end{aligned}$$

and, indeed, for any numbers $i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, n\}$ we have

$$(i_1 i_2 i_3 \cdots i_{k-1} i_k) = (i_1 i_2) \circ (i_2 i_3) \circ \cdots \circ (i_{k-1} i_k).$$

By combining these two observations, we see that any permutation can be expressed as a composition of (generally non-commuting) cycles. This composition is not unique.[1]

(c): By definition we say that id is a composition of zero transpositions. Since zero is an even number this says that $\text{id} \in A_n$. If you don't like that, observe that for any transposition (ij) we have $(ij)^{-1} = (ji) = (ij)$. Hence $\text{id} = (ij) \circ (ij)$ can be expressed as a composition of two transpositions, and two is even.

Next, suppose that $\sigma, \tau \in A_n$ so we can write

$$\begin{aligned} \sigma &= s_1 \circ s_2 \circ \cdots \circ s_k, \\ \tau &= t_1 \circ t_2 \cdots \circ t_\ell, \end{aligned}$$

for some transpositions $s_1, \ldots, s_k, t_1, \ldots, t_\ell$, where k and ℓ are even. But then we can write $\sigma \circ \tau$ as a composition of $k + \ell$ transpositions:

$$\sigma \circ \tau = s_1 \circ s_2 \circ \cdots \circ s_k \circ t_1 \circ t_2 \cdots \circ t_\ell.$$

Since $k + \ell$ is even this implies that $\sigma \circ \tau \in A_n$.

---

[1] For example, we could also write

$$(i_1 i_2 i_3 \cdots i_{k-1} i_k) = (i_1 i_k) \circ (i_1 i_{k-1}) \circ \cdots \circ (i_1 i_2).$$

Finally, for any $\sigma \in A_n$ we will show that $\sigma^{-1} \in A_n$.[2] If $\sigma \in A_n$ then by definition we can write

$$\sigma = s_1 \circ s_2 \circ \cdots \circ s_k,$$

where $s_1, \ldots, s_k$ are transpositions and k is even. But observe that for any transposition $s = (ij)$ we have $s^{-1} = (ij) = s$, which is also a transposition (in fact, the same transposition). Combining this with the formula $(\rho \circ \tau)^{-1} = \tau^{-1} \circ \rho^{-1}$ gives

$$\sigma^{-1} = s_k^{-1} \circ \cdots \circ s_2^{-1} \circ s_1^{-1} = s_k \circ \cdots \circ s_2 \circ s_1,$$

so σ^{-1} can also be expressed as a composition of k transpositions. Hence $\sigma^{-1} \in A_n$.

Remark: It is harder to prove that a given permutation can **not** be expressed as a product of evenly many transpositions. For example, I will show that the permutation $(12) \in S_3$ is not in A_3. Suppose for contradiction that we can write

$$(*) \qquad (12) = (t_1 \circ t_2) \circ (t_3 \circ t_4) \circ \cdots \circ (t_{2k-1} \circ t_k)$$

for some k. From the group table in Problem 2 we see that any two transpositions compose to give (123) or $(132) = (123)^{-1}$, thus the condition $(*)$ implies that (12) is a power of (123). But the power of (123) are

$$(123)^0 = \text{id}, \quad (123)^1 = (123), \quad (123)^2 = (132), \quad (123)^3 = \text{id}, \qquad \text{and then it repeats.}$$

Since (12) is a not a power of (123) we obtain a contradiction to $(*)$, hence (12) is not in A_3. The same argument shows that (13) and (23) are not in A_3. Hence we find that

$$A_3 = \{\text{id}, (123), (132)\},$$

with group table

$\circ$	id	(123)	(132)
id	id	(123)	(132)
(123)	(123)	(132)	id
(132)	(132)	id	(123)

By accident, it happens that this group **is abelian**, and in fact it is isomorphic to the additive group $(\mathbb{Z}/3\mathbb{Z}, +, 0)$. This can be seen by observing that the group tables are "the same" up to renaming of the elements:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

We will show later that **any** two groups of size 3 must be isomorphic.

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 $\mathbb{F}$.]

---

[2] Of course we already know that $\sigma^{-1} \in S_n$ exists, and from part (a) we know that σ^{-1} can be expressed as a composition of transpositions. We just want to show that the number of these transpositions is even.

Expanding the right hand side gives

$$\begin{aligned} x^3 + ax^2 + bx + c &= (x-\alpha)(x-\beta)(x-\gamma) \\ &= x^3 - e_1x^2 + e_2x - e_3, \end{aligned}$$

where

$$\begin{aligned} e_1 &= \alpha+\beta+\gamma, \\ e_2 &= \alpha\beta+\alpha\gamma+\beta\gamma, \\ e_3 &= \alpha\beta\gamma. \end{aligned}$$

And then comparing coefficients gives

$$\begin{aligned} e_1 &= -a, \\ e_2 &= b, \\ e_3 &= -c. \end{aligned}$$

Now consider the polynomial with roots $\alpha^2, \beta^2, \gamma^2$:

$$x^3 + a'x^2 + b'x + c' = (x-\alpha^2)(x-\beta^2)(x-\gamma^2),$$

where a', b', c' are some elements of $\mathbb{E}$. We will show that a', b', c' can be expressed in terms of a, b, c, hence are actually in $\mathbb{F}$. To do this we expand the right hand side to get

$$x^3 + a'x^2 + b'x + c' = x^3 - (\alpha^2+\beta^2+\gamma^2)x^2 + (\alpha^2\beta^2+\alpha^2\gamma^2+\beta^2\gamma^2)x - (\alpha^2\beta^2\gamma^2),$$

and then compare coefficients to get

$$\begin{aligned} a' &= -(\alpha^2+\beta^2+\gamma^2), \\ b' &= \alpha^2\beta^2+\alpha^2\gamma^2+\beta^2\gamma^2, \\ c' &= -\alpha^2\beta^2\gamma^2. \end{aligned}$$

Since each of these is a symmetric combination of α, β, γ we know that each can be expressed in terms of the elementary symmetric combinations e_1, e_2, e_3 by Waring's algorithm.

We begin with a'. Note that a' and $-e_1^2$ have the same leading term $-\alpha^2$. Expand $-e_1^2$ to get

$$-(\alpha+\beta+\gamma)^2 = -\alpha^2-\beta^2-\gamma^2-2(\alpha\beta+\alpha\gamma+\beta\gamma).$$

Then subtract to get

$$\begin{aligned} a' + e_1^2 &= 2(\alpha\beta+\alpha\gamma+\beta\gamma) \\ a' + e_1^2 &= 2e_2 \\ a' &= -e_1^2 + 2e_2 \\ &= -(-a)^2 + 2(b) \\ &= 2b - a^2. \end{aligned}$$

Now we compute b'. Observe that b' and e_2^2 have the same leading term $\alpha^2\beta^2$. Expand to get

$$\begin{aligned} e_2^2 &= (\alpha\beta+\alpha\gamma+\beta\gamma)^2 \\ &= \alpha^2\beta^2+\alpha^2\gamma^2+\beta^2\gamma^2+2\alpha^2\beta\gamma+2\alpha\beta^2\gamma+2\alpha\beta\gamma^2. \end{aligned}$$

Then subtract to get

$$\begin{aligned}
b' - e_2^2 &= -2(\alpha^2\beta\gamma + \alpha\beta^2\gamma + \alpha\beta\gamma^2) \\
b' - e_2^2 &= -2(\alpha + \beta + \gamma)(\alpha\beta\gamma) \\
b' - e_2^2 &= -2e_1e_3 \\
b' &= e_2^2 - 2e_1e_3 \\
&= (b)^2 - 2(-a)(-c) \\
&= b^2 - 2ac.
\end{aligned}$$

Finally, we observe that

$$\begin{aligned}
c' &= -\alpha^2\beta^2\gamma^2 \\
&= -(\alpha\beta\gamma)^2 \\
&= -e_3^2 \\
&= -(-c)^2 \\
&= -c^2.
\end{aligned}$$

In conclusion, we have

$$x^3 + (2b - a^2)x^2 + (b^2 - 2ac)x - c^2 = (x - \alpha^2)(x - \beta^2)(x - \gamma^2).$$

Example: Consider the polynomial x^3+x^2+x+1 with coefficients $(a, b, c) = (1, 1, 1)$. Consider the factorization

$$x^4 - 1 = (x - 1)(x^3 + x^2 + x + 1).$$

Since $x^4 - 1$ has roots $\pm 1, \pm i$ and $x - 1$ has root $+1$, we see that $x^3 + x^2 + x + 1$ has roots $-1, \pm i$. According to the result of Problem 4, the polynomial $x^3 + a'x^2 + b'x + c'$ with

$$(a', b', c') = (2b - a^2, b^2 - 2ac, -c^2) = (2 - 1, 1 - 2, -1) = (1, -1, -1)$$

should have roots $(-1)^2, i^2, (-i)^2$, i.e., $1, -1, -1$. And, indeed, we have

$$x^3 + x^2 - x - 1 = (x - 1)(x + 1)^2,$$

which has the desired roots and multiplicities.