Math 562/662 **Spring 2024**
Homework 4 **Drew Armstrong**

---

1. Extending Ring Homomorphisms to Polynomials. Given a ring homomorphism $\varphi : R \to S$ we define the function $\varphi : R[x] \to S[x]$ by sending $f(x) = \sum_k a_k x^k$ to

$$f^\varphi(x) := \sum_k \varphi(a_k) x^k.$$

(a) Prove that $f(x) \mapsto f^\varphi(x)$ is a ring homomorphism.

(b) Given an integer $n \geq 0$ let $\varphi : \mathbb{Z}[x] \to (\mathbb{Z}/n\mathbb{Z})[x]$ be the extension of the quotient homomorphism $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Show that

$$f^\varphi(x) = 0 \quad \iff \quad n \text{ divides every coefficient of } f(x).$$

(c) **Gauss' Lemma.** A polynomial $f(x) \in \mathbb{Z}[x]$ is called *primitive* when its coefficients have no common prime factors. If $f(x), g(x) \in \mathbb{Z}[x]$ are primitive, prove that $f(x)g(x) \in \mathbb{Z}[x]$ is also primitive. [Hint: Let $p \geq 2$ be a common prime factor of the coefficients of $f(x)g(x)$ and let $\varphi : \mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x]$ be the map from part (b). Since $\mathbb{Z}/p\mathbb{Z}$ is a field, and since $f^\varphi(x)g^\varphi(x) = \varphi(f(x)g(x)) = 0$ we must have $f^\varphi(x) = 0$ or $g^\varphi(x) = 0$.]

(a): Note that the two homomorphisms agree when restricted to the "constant polynomials" $R \subseteq R[x]$ and $S \subseteq S[x]$, hence we have $\varphi(0) = 0$ and $\varphi(1) = 1$. Furthermore, for any $f(x) = \sum a_k x^k$ and $\sum b_k x^k$ in $R[x]$ then we have

$$\begin{aligned}
(f+g)^\varphi &= \left(\sum (a_k + b_k)x^k\right)^\varphi \\
&= \sum \varphi(a_k + b_k)x^k \\
&= \sum \left[\varphi(a_k) + \varphi(b_k)\right] x^k \\
&= \sum \varphi(a_k)x^k + \sum \varphi(b_k)x^k \\
&= f^\varphi + g^\varphi
\end{aligned}$$

and

$$\begin{aligned}
(fg)^\varphi &= \left(\sum_m \left(\sum_{k+\ell=m} a_k b_\ell\right) x^m\right)^\varphi \\
&= \sum_m \varphi\left(\sum_{k+\ell=m} a_k b_\ell\right) x^m \\
&= \sum_m \left(\sum_{k+\ell=m} \varphi(a_k)\varphi(b_\ell)\right) x^m \\
&= \sum_k \varphi(a_k)x^k \sum_\ell \varphi(b_\ell)x^\ell \\
&= f^\varphi g^\varphi.
\end{aligned}$$

(b): Given an integer $n \geq 0$ we have a natural "quotient homomorphism" $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $k \mapsto [k]$. Recall that $[k] = [0]$ if and only if k is a multiple of n. Let $\varphi : \mathbb{Z}[x] \to (\mathbb{Z}/n\mathbb{Z})[x]$ be the extension to rings of polynomials. Then the kernel is

$$\ker \varphi = \{f(x) \in \mathbb{Z}[x] : f^\varphi(x) = 0\}$$

$$= \left\{ \sum a_k x^k \in \mathbb{Z}[x] : \sum [a_k] x^k = 0 \right\}$$
$$= \left\{ \sum a_k x^k \in \mathbb{Z}[x] : [a_k] = [0] \text{ for all } k \right\}$$
$$= \left\{ \sum a_k x^k \in \mathbb{Z}[x] : n | a_k \text{ for all } k \right\}.$$

(c): Let $f(x), g(x) \in \mathbb{Z}[x]$ and assume that $f(x)g(x)$ is not primitive. In this case we will show that either $f(x)$ or $g(x)$ is not primitive. Since $f(x)g(x)$ is not primitive, there exists some prime $p \geq 2$ that divides every coefficient of $f(x)g(x)$. In other words, the the ring homomorphism $\varphi : \mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x]$ satisfies $(fg)^\varphi(x) = 0$. Then since $f^\varphi(x)g^\varphi(x) = (fg)^\varphi(x) = 0$ and since $(\mathbb{Z}/p\mathbb{Z})[x]$ is a domain[1] we conclude that $f^\varphi(x) = 0$ or $g^\varphi(x) = 0$. In the first case we see that p divides every coefficient of $f(x)$, hence $f(x)$ is not primitive, and in the second case p divides every coefficient of $g(x)$, hence $g(x)$ is not primitive.

Remark: This is one of many related results that go by the name "Gauss' Lemma". It is typically used to prove that polynomials $f(x) \in \mathbb{Z}[x]$ that are irreducible over $\mathbb{Z}$ are also irreducible over $\mathbb{Q}$. Here is a sketch of the proof. Let $f(x) \in \mathbb{Z}[x]$ and assume that $f(x)$ is reducible over $\mathbb{Q}$. Let's say $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{Q}[x]$. If $m, n \in \mathbb{N}$ are the least common multiples of the denominators of the coefficients of $g(x)$ and $h(x)$, respectively, then we have $mnf(x) = g'(x)h'(x)$ with $g'(x) = mg(x) \in \mathbb{Z}[x]$ and $h'(x) = nh(x) \in \mathbb{Z}[x]$. Furthermore, let $g'(x) = m'g''(x)$ and $h'(x) = n'h''(x)$ with $g''(x), h''(x) \in \mathbb{Z}[x]$ primitive, so that $mnf(x) = m'n'g''(x)h''(x)$. But we know that $f(x) = m'n'g''(x)h''(x)/mn$ has integer coefficients. Since $g''(x)h''(x)$ is primitive by part (c) this implies that $m'n'/mn$ is an integer, and hence $f(x)$ is reducible over $\mathbb{Z}$.

2. Equivalent Statements of the FTA. Consider the following statements:

- (1$\mathbb{R}$) Every non-constant $f(x) \in \mathbb{R}[x]$ has a root in $\mathbb{C}$.
- (2$\mathbb{R}$) Every non-constant $f(x) \in \mathbb{R}[x]$ is a product degree 1 and 2 polynomials in $\mathbb{R}[x]$
- (1$\mathbb{C}$) Every non-constant $f(x) \in \mathbb{C}[x]$ has a root in $\mathbb{C}$.
- (2$\mathbb{C}$) Every non-constant $f(x) \in \mathbb{C}[x]$ is a product of degree 1 polynomials in $\mathbb{C}[x]$.

I claim that these four statements are equivalent. We will prove the more difficult implications.

(a) Prove that (1$\mathbb{R}$) implies (2$\mathbb{R}$). [Hint: Let $* : \mathbb{C} \to \mathbb{C}$ be complex conjugation and let $* : \mathbb{C}[x] \to \mathbb{C}[x]$ be the extension as in Problem 1. For all $\alpha \in \mathbb{C}$ note that $f(\alpha)^* = f^*(\alpha^*)$. But if $f(x)$ has real coefficients then $f^*(x) = f(x)$. Use this to show that the non-real roots of a real polynomial come in complex conjugate pairs.]

(b) Prove that (1$\mathbb{R}$) implies (1$\mathbb{C}$). [Hint: Given $f(x) \in \mathbb{C}[x]$ we note that $(ff^*)^* = f^*(f^{**}) = f^*f = ff^*$, and hence the polynomial $f(x)f^*(x)$ has real coefficients. Assuming (1$\mathbb{R}$) we know that ff^* has a root $\alpha \in \mathbb{C}$, i.e., $f(\alpha)f^*(\alpha) = 0$. Use this to show that $f(x)$ has a root in $\mathbb{C}$.]

(a): Suppose that (1$\mathbb{R}$) is true, so every non-constant $f(x) \in \mathbb{R}[x]$ has a root in $\mathbb{C}$. In this case we will show by induction that (2$\mathbb{R}$) is true. So consider any non-constant $f(x) \in \mathbb{R}[x]$. If $\deg(f) = 1$ of $\deg(f) = 2$ then we are done. Otherwise, let $\alpha \in \mathbb{C}$ be any root of $f(x)$, which exists by (1$\mathbb{R}$). If $\alpha \in \mathbb{R}$ then we have $f(x) = (x - \alpha)g(x)$ with $g(x) \in \mathbb{R}[x]$ and we may assume by induction on degree that $g(x)$ is a product of degree 1 and 2 real polynomials,

[1] If p is prime then $\mathbb{Z}/p\mathbb{Z}$ is a field. In particular, it is a domain.

hence so is $f(x)$. Otherwise we have $\alpha \in \mathbb{C} \setminus \mathbb{R}$. In this case we note that α^* is also a root of $f(x)$ because $f^*(x) = f(x)$ and hence

$$f(\alpha^*) = f^*(\alpha^*) = [f(\alpha)]^* = 0^* = 0.$$

Applying Descartes once gives $f(x) = (x - \alpha)g(x)$ for some $g(x) \in \mathbb{C}[x]$. Then substituting $x = \alpha^*$ gives $0 = (\alpha - \alpha^*)g(\alpha^*)$. Since $\alpha \neq \alpha^*$ (because α is not real) this implies that $g(\alpha^*) = 0$. Then applying Descartes again gives $g(x) = (x - \alpha^*)h(x)$ for some $h(x) \in \mathbb{C}[x]$. Putting this together gives

$$\begin{aligned} f(x) &= (x - \alpha)(x - \alpha^*)h(x) \\ &= [x^2 - (\alpha + \alpha^*)x + (\alpha\alpha^*)]h(x), \qquad\qquad = q(x)h(x), \end{aligned}$$

where the polynomial $q(x)$ has real coefficients because $\alpha + \alpha^*$ and $\alpha\alpha^*$ are always real. Since $f(x)$ and $q(x)$ have real coefficients it follows from the uniqueness of quotients in the ring $\mathbb{C}[x]$ that $h(x)$ has real coefficients. Finally, we may assume by induction that $h(x)$ is a product of degree 1 and 2 real polynomials. Hence so is $f(x)$.

(b): Suppose that (1$\mathbb{R}$) is true, so every non-constant $f(x) \in \mathbb{R}[x]$ has a root in $\mathbb{C}$. To prove that (1$\mathbb{C}$) we must show that every non-constant $f(x) \in \mathbb{C}[x]$ has a root in $\mathbb{C}$. So consider any non-constant $f(x) \in \mathbb{C}[x]$. Define the polynomial $g(x) = f(x)f^*(x)$. From Problem 1 we have $(ff^*)^* = f^*f^{**} = f^*f = ff^*$, which says that $g(x)$ has real coefficients. From (1$\mathbb{R}$) there exists $\alpha \in \mathbb{C}$ with $g(\alpha) = 0$. Then since

$$0 = g(\alpha) = f(\alpha)f^*(\alpha)$$

we must have $f(\alpha) = 0$ or $f^*(\alpha)$. If $f(\alpha) = 0$ then we are done. And if $f^*(\alpha) = 0$ then

$$f(\alpha^*) = [f^*(\alpha)]^* = 0^* = 0,$$

so we are still done.

3. Freshman's Binomial Theorem. Let $p \geq 2$ be prime and let R be any ring of characteristic p. For any elements $a, b \in R$, prove that

$$(a + b)^p = a^p + b^p.$$

[Hint: For any $a \in R$ and $n \in \mathbb{Z}$ recall that we have an element $n \cdot a \in R$ defined by induction. If R has characteristic p then $p \cdot a = 0$ for any $a \in R$. For any $a, b \in R$, the usual binomial theorem for integers tells us that

$$(a + b)^p = a^p + \binom{p}{1} \cdot a^{p-1}b + \cdots + \binom{p}{p-1} \cdot ab^{p-1} + b^p.$$

Your job is to show that the integer $\binom{p}{k}$ is divisible by p whenever $1 \leq k \leq p - 1$.]

Let $k, p \in \mathbb{Z}$ with $p \geq 2$ prime and $1 \leq k \leq p - 1$. Let $N = \binom{p}{k} \in \mathbb{N}$, so that

$$p(p-1)\cdots 2 \cdot 1 = N \cdot k(k-1)\cdots 2 \cdot 1 \cdot (p-k)(p-k-1)\cdots 2 \cdot 1.$$

Since p divides the left hand side it also divides the right side, hence by Euclid's lemma it divides some factor on the right hand side. But every factor on the right hand side other than N is smaller than p, hence p must divide N. In other words, we can write $N = pN'$ for some $N' \in \mathbb{N}$. If $c \in R$ is any element of a ring of characteristic p it follows that

$$\binom{p}{k} \cdot c = (pN') \cdot c = N' \cdot (p \cdot c) = N' \cdot 0 = 0.$$

Finally, if $a, b \in R$ are any two elements in a ring of characteristic p then we have

$$\begin{aligned}(a+b)^p &= a^p + \binom{p}{1} \cdot a^{p-1}b + \cdots + \binom{p}{p-1} \cdot ab^{p-1} + b^p \\ &= a^p + 0 + \cdots + 0 + b^p \\ &= a^p + b^p.\end{aligned}$$

4. Eisenstein's Criterion. Let $p \geq 2$ be prime.

(a) Given a polynomial $f(x) = a_0 + \cdots + a_n x^n \in \mathbb{Z}[x]$ with $p | a_i$ for $0 \leq i \leq n-1$, $p \nmid a_n$ and $p^2 \nmid a_0$, prove that $f(x)$ is irreducible over $\mathbb{Z}$. [Hint: Suppose that $f(x) = g(x)h(x)$ with $\deg(g) = k \geq 1$ and $\deg(h) = \ell \geq 1$. Consider the ring homomorphism $\varphi : \mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x]$ from 1(b), so that $g^\varphi(x)h^\varphi(x) = f^\varphi(x) = [a_n]x^n$ with $[a_n] \neq [0]$. Since p is prime this implies that $g^\varphi(x) = [b]x^k$ and $h^\varphi(x) = [c]x^\ell$ for some $[c], [d] \neq [0]$. But then the constant terms of $g(x)$ and $h(x)$ are divisible by p, so the constant term of $f(x) = g(x)h(x)$ is divisible by p^2.]

(b) The p-th cyclotomic polynomial is $\Phi_p(x) = 1 + x + \cdots + x^{p-1} = (x^p - 1)/(x - 1)$, so

$$\Phi_p(1+x) = \frac{(1+x)^p - 1}{x} = \binom{p}{1} + \binom{p}{2}x + \cdots + \binom{p}{p}x^{p-1}.$$

Use part (a) and the proof of Problem 3 to show that $\Phi_p(1+x)$ is irreducible over $\mathbb{Z}$. Use this to conclude that $\Phi_p(x)$ is irreducible over $\mathbb{Z}$.

(a): Let $p \geq 2$ be prime. Consider a polynomial $f(x) = a_0 + \cdots + a_n x^n \in \mathbb{Z}[x]$ with $p | a_i$ for all $0 \leq i \leq n-1$, $p \nmid a_n$ and $p^2 \nmid a_0$. Assume for contradiction that we can write $f(x) = g(x)h(x)$ for some non-constant $g(x), h(x) \in \mathbb{Z}[x]$. Say $\deg(g) = k \geq 1$ and $\deg(h) = \ell \geq 1$. Let $\varphi : \mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x]$ be the ring homomorphism from Problem 1. By the assumptions on $f(x)$ we have

$$g^\varphi(x)h^\varphi(x) = f^\varphi(x) = [a_n]x^n + [0]x^{n-1} + \cdots + [0].$$

But note that $(\mathbb{Z}/p\mathbb{Z})[x]$ is a unique factorization domain because p is prime. This implies that any divisor of $[a_n]x^n$ must have the form $[b]x^m$ for some $b, m \in \mathbb{Z}$. In particular, we must have $g^\varphi(x) = [b]x^k$ and $h^\varphi(x) = [c]x^\ell$ for some $b, c \in \mathbb{Z}$ not divisible by p. Since the constant terms of $g^\varphi(x)$ and $h^\varphi(0)$ are $[0]$, the constant terms of $g(x)$ and $h(x)$ are divisible by p. But then the constant term of $f(x) = g(x)h(x)$ is divisible by p^2. Contradiction.

(b): Let $\Phi_p(x)$ be the pth cyclotomic polynomial and let $f(x) = \Phi_p(1+x) \in \mathbb{Z}[x]$. The hint shows that

$$f(x) = \binom{p}{1} + \binom{p}{2}x + \cdots + \binom{p}{p-1}x^{p-2} + x^{p-1}.$$

In Problem 3 we showed that $\binom{p}{k}$ is divisible by p when $1 \leq k \leq p-1$. Furthermore, since $\binom{p}{1} = p$ we have $p^2 \nmid \binom{p}{1}$. Then since $f(x)$ satisfies the hypotheses of Eisenstein's criterion we conclude that $f(x)$ is irreducible over $\mathbb{Z}$. Finally, suppose for contradiction that $\Phi_p(x) = g(x)h(x)$ for some $g(x), h(x) \in \mathbb{Z}[x]$. Then

$$f(x) = \Phi_p(1+x) = g(1+x)h(1+x) = g'(x)h'(x)$$

with $g'(x), h'(x) \in \mathbb{Z}[x]$ which contradicts the fact that $f(x)$ is irreducible over $\mathbb{Z}$. Hence $\Phi_p(x)$ is irreducible over $\mathbb{Z}$.

Remark: By the remark after Problem 1 we conclude that $\Phi_p(x)$ is also irreducible over $\mathbb{Q}$. It is also true that the cyclotomic polynomial $\Phi_n(x)$ is irreducible over $\mathbb{Q}$ for non-prime $n \in \mathbb{N}$ but this is much more difficult to prove.

5. Fundamental Theorem of Symmetric Polynomials. For any field $\mathbb{F}$, the symmetric group S_n acts on the set of polynomials $\mathbb{F}[x_1, \ldots, x_n]$ by permuting the variables:

$$\sigma \cdot f(x_1, \ldots, x_n) := f(x_{\sigma(1)}, \cdots, x_{\sigma(n)}).$$

We say that f is a *symmetric polynomial* when $\sigma \cdot f = f$ for all $\sigma \in S_n$.

(a) Let $\mathbf{x} = (x_1, \ldots, x_n)$. Then for any $\mathbf{k} = (k_1, \ldots, k_n) \in \mathbb{N}^n$ we define the notation

$$\mathbf{x}^{\mathbf{k}} := x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}.$$

Every $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ has a unique expression $f(\mathbf{x}) = \sum_{\mathbf{k} \in \mathbb{N}^n} a_{\mathbf{k}} \mathbf{x}^{\mathbf{k}}$ with $a_{\mathbf{k}} \in \mathbb{F}$ for all $\mathbf{k} \in \mathbb{N}^n$. Check that this notation satisfies $\mathbf{x}^{\mathbf{k}} \mathbf{x}^{\boldsymbol{\ell}} = \mathbf{x}^{\mathbf{k}+\boldsymbol{\ell}}$ for all $\mathbf{k}, \boldsymbol{\ell} \in \mathbb{N}^n$. It follows from this (but you don't need to prove it) that

$$\left(\sum_{\mathbf{k} \in \mathbb{N}^n} a_{\mathbf{k}} \mathbf{x}^{\mathbf{k}} \right) \left(\sum_{\boldsymbol{\ell} \in \mathbb{N}^n} b_{\boldsymbol{\ell}} \mathbf{x}^{\ell} \right) = \sum_{\mathbf{m} \in \mathbb{N}^n} \left(\sum_{\mathbf{k}+\boldsymbol{\ell}=\mathbf{m}} a_{\mathbf{k}} b_{\boldsymbol{\ell}} \right) \mathbf{x}^{\mathbf{m}}.$$

(b) We define the *lexicographic order* on $\mathbb{N}^n$ as follows:

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

One can check (don't do this) that this defines a total order on $\mathbb{N}^n$ which satisfies the well-ordering property and for all $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{N}^n$ we have $\mathbf{a} \leq \mathbf{b} \Rightarrow \mathbf{a} + \mathbf{c} \leq \mathbf{b} + \mathbf{c}$. Based on this, we define the *lexicographic degree* function $\deg : \mathbb{F}[\mathbf{x}] \to \mathbb{N}^n$ by

$$\deg \left(\sum_{\mathbf{k} \in \mathbb{N}^n} a_{\mathbf{k}} \mathbf{x}^{\mathbf{k}} \right) := \max_{\text{lex}} \{ \mathbf{k} \in \mathbb{N}^n : a_{\mathbf{k}} \neq 0 \}.$$

Use part (a) and the given properties to show that $\deg(fg) = \deg(f) + \deg(g)$ for all nonzero polynomials $f(\mathbf{x}), g(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$.

(c) The *elementary symmetric polynomials* $e_1(\mathbf{x}), \ldots, e_n(\mathbf{x})$ are defined by

$$(y - x_1) \cdots (y - x_n) = y^n - e_1(\mathbf{x}) y^{n-1} + e_2(\mathbf{x}) y^{n-2} + \cdots + (-1)^n e_n(\mathbf{x}).$$

One can check that each $e_i(\mathbf{x})$ is monic (i.e., has lex-leading coefficient 1) and has $\deg(e_j) = (1, \ldots, 1, 0, \ldots, 0)$, with j ones followed by $n - j$ zeroes. For any symmetric polynomial $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$, prove that we can find a (possibly non-symmetric) polynomial $g(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ such that

$$f(\mathbf{x}) = g(e_1(\mathbf{x}), \ldots, e_n(\mathbf{x})).$$

[Hint: Use induction on lexicographic degree. Suppose that $f(\mathbf{x}) = c\mathbf{x}^{\mathbf{k}} + \text{lower terms}$. Use the fact that $f(\mathbf{x})$ is symmetric to show that $k_1 \geq k_2 \geq \cdots \geq k_n$. Define

$$g(\mathbf{x}) := c e_1(\mathbf{x})^{k_1 - k_2} e_2(\mathbf{x})^{k_2 - k_3} \cdots e_{n-1}(\mathbf{x})^{k_{n-1} - k_n} e_n(\mathbf{x})^{k_n}$$

and use (b) to check that $g(\mathbf{x}) = c\mathbf{x}^{\mathbf{k}} + \text{lower terms}$. Then since $\deg(f - g) < \deg(f)$ we may assume that $f(\mathbf{x}) - g(\mathbf{x}) = h(e_1(\mathbf{x}), \ldots, e_n(\mathbf{x}))$ for some $h(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$.]

(d) Let $f(x) \in \mathbb{F}[x]$ be a polynomial in one variable and let $\mathbb{E} \supseteq \mathbb{F}$ be a splitting field for $f(x)$ over $\mathbb{F}$. That is, suppose that there exist $\alpha_1, \ldots, \alpha_n \in \mathbb{E}$ such that

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n).$$

For any multivariable polynomial $F(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$ we have the evaluation $F(\alpha_1, \ldots, \alpha_n) \in \mathbb{E}$. If F is symmetric, use part (c) to show that $F(\alpha_1, \ldots, \alpha_n) \in \mathbb{F}$.

(a): This is easy:

$$\begin{aligned}\mathbf{x}^{\mathbf{k}}\mathbf{x}^{\ell} &= x_1^{k_1}\cdots x_n^{k_n}x_1^{\ell_1}\cdots x_n^{\ell_n}\\ &= x_1^{k_1+\ell_1}\cdots x_n^{k_n+\ell_n}\\ &= \mathbf{x}^{\mathbf{k}+\ell}.\end{aligned}$$

(b): 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

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

and then since $\mathbf{k}+\boldsymbol{\ell} \leq \mathbf{d}+\boldsymbol{\ell} \leq \mathbf{d}+\mathbf{e}$ we conclude that $\mathbf{k}+\boldsymbol{\ell} \leq \mathbf{d}+\mathbf{e}$.

Remark: This is **exactly the same proof** you would use to rigorously prove the identity $\deg(fg) = \deg(f)+\deg(g)$ for polynomials in one variable. It's just that no one ever bothers to write that proof down.

(c): If $f(\mathbf{x})$ has degree $\mathbf{0}$ then $f(\mathbf{x}) = c$ for some constant $c \in \mathbb{F}$ and we can write $f(\mathbf{x}) = g(e_1(\mathbf{x}), \ldots, e_n(\mathbf{x}))$ with $g(\mathbf{x}) = c$. Now let $f(\mathbf{x})$ be symmetric with $\deg(f) = \mathbf{k} > \mathbf{0}$ and

assume for induction that all symmetric polynomials of smaller lexicographic degree satisfy the desired property. By assumption we have

$$f(\mathbf{x}) = cx_1^{k_1}x_2^{k_2}\cdots x_n^{k_n} + \text{ lower terms.}$$

I claim that $k_1 \geq k_2 \geq \cdots \geq k_n$. To prove this, suppose for contradiction that $k_i < k_{i+1}$ and let $\mathbf{k}' = \sigma(\mathbf{k})$ where σ is the permutation that swaps the ith and jth coordinates. Note that $\mathbf{k}' > \mathbf{k}$ in lexicographic order. Since $f(\mathbf{x})$ is symmetric, the coefficients of $\mathbf{x}^{\mathbf{k}}$ and $\mathbf{x}^{\mathbf{k}'}$ in $f(\mathbf{x})$ must be equal; in particular, both coefficients are non-zero. But then $f(\mathbf{x})$ contains the term $c\mathbf{x}^{\mathbf{k}'}$, where $\mathbf{k}' > \mathbf{k}$. This contradicts the assumption that $\mathbf{k}$ is the highest exponent in $f(\mathbf{x})$.

Thus we may consider the (symmetric) polynomial

$$g(\mathbf{x}) := ce_1(\mathbf{x})^{k_1-k_2}e_2(\mathbf{x})^{k_2-k_3}\cdots e_{n-1}(\mathbf{x})^{k_{n-1}-k_n}e_n(\mathbf{x})^{k_n}$$

According to part (b) this polynomial is monic and satisfies

$$\begin{aligned}
\deg(g) &= (k_1-k_2)\deg(e_1) + (k_2-k_3)\deg(e_2) + \cdots + k_n\deg(e_n) \\
&= (k_1-k_2)(1,0,\ldots,0) \\
&\quad + (k_2-k_3)(1,1,0\ldots,0) \\
&\quad\ \vdots \\
&\quad + k_n(1,1,\ldots,1) \\
&= (k_1,k_2,\ldots,k_n) \\
&= \mathbf{k}.
\end{aligned}$$

Since $f(\mathbf{x})$ and $g(\mathbf{x})$ are symmetric polynomials with the same leading term it follows that $f(\mathbf{x}) - g(\mathbf{x})$ is a symmetric polynomial of strictly smaller degree, hence by induction there exists a (possibly non-symmetric) polynomial $h(\mathbf{x})$ satisfying

$$f(\mathbf{x}) - g(\mathbf{x}) = h(e_1(\mathbf{x}),\ldots,e_n(\mathbf{x})).$$

Finally, we have

$$f(\mathbf{x}) = g(\mathbf{x}) + h(e_1(\mathbf{x}),\ldots,e_n(\mathbf{x})) = g'(e_1(\mathbf{x}),\ldots,e_n(\mathbf{x})),$$

where

$$g'(\mathbf{x}) = cx_1^{k_1-k_2}x_2^{k_2-k_3}\cdots x_n^{k_n} + h(\mathbf{x}).$$

(d): Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ with $a_0,\ldots,a_n \in \mathbb{F}$ and let $\mathbb{E} \supseteq \mathbb{F}$ be a field containing elements $\alpha_1,\ldots,\alpha_n \in \mathbb{E}$ such that

$$f(x) = (x-\alpha_1)\cdots(x-\alpha_n).$$

Expanding the right hand side and comparing coefficients shows that $a_k = (-1)^k e_k(\alpha_1,\ldots,\alpha_n)$, which shows that $e_k(\alpha_1,\ldots,\alpha_n) \in \mathbb{F}$ for all k. More generally, let $F(\mathbf{x})$ be any symmetric polynomial in n coordinates. By part (c) we can write

$$F(\mathbf{x}) = g(e_1(\mathbf{x}),e_2(\mathbf{x}),\ldots,e_n(\mathbf{x}))$$

for some polynomial $g(\mathbf{x})$ with coefficients in $\mathbb{F}$. Then substituting $x_k = \alpha_k$ gives

$$F(\alpha_1,\ldots,\alpha_n) = g(e_1(\alpha_1,\ldots,\alpha_n),\ldots,e_n(\alpha_1,\ldots,\alpha_n)) \in \mathbb{F}.$$

Remark: This theorem is extremely old[2] but a rigorous proof is almost never written down. Most authors just mention that it's "well-known". The first rigorous proof, using lexicographic degree, was given by Gauss as part of his second proof of the Fundamental Theorem of Algebra. The computational theory of multivariable polynomials was studied more rigorously after the invention of computers. The foundations were laid by Bruno Buchberger in his 1965 thesis.

[2]Apart from Descartes' theorem on long division of polynomials it is the oldest theorem in this class. It is sometimes attributed to Newton.