Chapter 4 Arithmetic in $F[x]$:

We have studied the rings $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ extensively.

Now that we know what rings are, we return to another very important case of rings: polynomial rings.

Given a ring R, the polynomial ring $R[x]$ is defined by

$$R[x] = \{ a_0 + a_1 x + \cdots + a_n x^n : a_i \in R,\ n \in \mathbb{Z}_{\geq 0} \}.$$

We will see many of the nice properties of $\mathbb{Z}$ carry over to this ring.

4.1 Polynomial arithmetic and the Division Algorithm:

The first thing to note is that if R is a ring, then $R[x]$ is also a ring. The addition and multiplication are defined as follows: given $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ and $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ in R, we define

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n$$

where we set $b_k = 0$ if $k > m$ and we assume wlog $n \geq m$,

and

$$f(x) \cdot g(x) = \sum_{k=0}^{n+m} c_k x^k$$

where $c_k = \sum_{j=0}^{k} a_j b_{k-j}$.

We also require $ax = ax$ for all $a \in R$ and if

$$a_0 + a_1 x + \cdots + a_n x^n = b_0 + b_1 x + \cdots + b_m x^m,$$

then $m = n$ and

$$a_i = b_i \text{ for } 0 \le i \le m.$$

Using these properties one can check $R[x]$ is a ring. If R is commutative with 1_R, then so is $R[x]$. Also, R is a subring of $R[x]$.

Example: Let $R = \mathbb{Z}/4\mathbb{Z}$ and consider $R[x]$.

Let $f(x) = x + 2x^2 + 3x^5 = 0 + 1\cdot x + 2x^2 + 0\cdot x^3 + 0\cdot x^4 + 3x^5$

and $g(x) = 1 + 4x + 2x^2$.

Then $f(x) + g(x) = 1 + (1+4)x + (2+2)x^2 + 3x^5 = 1 + x + 3x^5$

$f(x)g(x) = (x + 2x^2 + 3x^5)(1 + 4x + 2x^2)$

$= x + 4x^2 + 2x^3 + 2x^2 + 8x^3 + 4x^4 + 3x^5 + 12x^6 + 6x^7$

$= x + 2x^2 + 2x^3 + 3x^5 + 2x^7.$

Warning: The term "x" here is an indeterminate, not a variable.

You do not replace x with numbers here like in calculus. Also, really one should not write $f(x)$ and $g(x)$ because it makes it look as if x can be substituted for, but the books denote them this way as it is customary to write $f(x)$, but I will try to remember not to do

this to help eliminate the confusion.

Def: Given $f = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ with $a_n \neq 0$, we refer to a_n as the *leading coefficient* of f and n as the *degree* of f.

Example: Let $f = 2 + 3x + 4x^2 + 10x^5 + 7x^{10}$.

be in $(\mathbb{Z}/7\mathbb{Z})[x]$. Note since $7 = 0$ here, the

leading coefficient is $10 = 3$ and the degree is 5.

We have $R \subseteq R[x]$ as a subring as mentioned earlier. If $a \in R$, $a \neq 0$ we say a has degree 0. There are generally two ways to deal with the degree of 0_R. The book says we do not give 0_R a degree, so we will follow that. The other way to do it so that things work out nicely is to say the degree of 0_R is $-\infty$.

Theorem 4.1.1: Let R be an integral domain and f, g nonzero polynomials in $R[x]$. Then

$$\deg(fg) = \deg f + \deg g.$$

If R is not assumed to be an integral domain one only has

$$\deg(fg) \leq \deg f + \deg g.$$

Before we prove this, note that if we set $\deg(0_R) = -\infty$ the result would be true without having to require the polynomials to be nonzero.

Proof: From the definition we see that if f has leading coefficient a_n and g has leading coefficient b_m, then fg has leading coefficient $a_n b_m$ as long as $a_n b_m \neq 0$. If R is an integral domain, $a_n b_m \neq 0$ because $a_n \neq 0$ and $b_m \neq 0$. Thus, $\deg(fg) = \deg f + \deg g$ if R is an integral domain. If R is not an integral domain it could be the case that $a_n b_m = 0$, in which case $\deg(fg) < m+n$. Thus, in the general case one obtains

$$\deg(fg) \leq \deg f + \deg g.$$

□

Example: Let $f = 1 + 2x \in (\mathbb{Z}/4\mathbb{Z})[x]$ and $g = 2x^2 \in (\mathbb{Z}/4\mathbb{Z})[x]$.

Then $fg = 2x^2 + 4x^3 = 2x^2$. Thus,

$$\deg(fg) = 2 < \deg f + \deg g = 3.$$

Cor 4.1.2: If R is an integral domain, so is $R[x]$.

Proof: We already stated if R is a commutative ring with identity, so is

$R[x]$. The previous theorem gives there are no zero divisors in $R[x]$ if R is an integral domain. Thus, $R[x]$ is an integral domain if R is. ■

One of the most important cases to study is $F[x]$ when F is a field. The reason for this is that one has a division algorithm on $F[x]$.

<u>Theorem 4.1.3:</u> Let F be a field and $f, g \in F[x]$. with $g \neq 0_F$. There are unique polynomials $q, r \in F[x]$ so that

$$f = gq + r$$

where $r = 0_F$ or $\deg r < \deg g$.

Before we prove this, lets work an example.

<u>Example:</u> Let $f = x^5 + x + 2 \in \mathbb{Q}[x]$ and $g = x^2 + 3x + 1 \in \mathbb{Q}[x]$.

We do polynomial long division:

[redacted]

$$\begin{array}{r} x^3 - 3x^2 + 8x - 21 \\ x^2+3x+1 \;\overline{)\; x^5 + x + 2} \\ \underline{x^5 + 3x^4 + x^3} \\ -3x^4 - x^3 + x + 2 \\ \underline{-3x^4 - 9x^3 - 3x^2} \\ 8x^3 + 3x^2 + x + 2 \\ \underline{8x^3 + 24x^2 + 8x} \end{array}$$

$$-21x^2 - 7x + 2$$
$$\underline{-21x^2 - 63x - 21}$$
$$56x + 23.$$

Thus,

$$x^5 + x + 2 = (x^2 + 3x + 1)(x^3 - 3x^2 + 8x - 21) + (56x + 23).$$

Proof: First we prove existence and then deal with uniqueness.

1) If $f = 0_F$ or $\deg f < \deg g$, then set $q = 0_F$ and $r = f$ so that $f = g \cdot 0_F + r = 0_F + r = f$.

2) Now suppose that $f \neq 0_F$ and $\deg g \leq \deg f$. We prove this by induction on the degree of f.

Base case: $n = 0$, $n = \deg f$.

This means $f = a$ for $a \in F$, $a \neq 0$ and $g = b$, $b \in F$, $b \neq 0$.

Then set $q = \frac{a}{b}$ and we are done.

Induction hypothesis: Assume that given any $h(x) \in F[x]$ of deg $\leq n$ we have $q_h(x), r_h(x) \in F[x]$ with $r_h(x) = 0$ or $r_h(x)$ with degree less than $\deg g(x)$ so that $h(x) = g(x) q_h(x) + r_h(x)$.

Let $f = a_{n+1} x^{n+1} + \cdots + a_1 x + a_0$ and $g = b_m x^m + \cdots + b_1 x + b_0$.

w/ $a_{n+1} \neq 0$, $b_m \neq 0$. Set

$$h = f - \frac{a_{n+1}}{b_m} x^{n+1-m} g.$$

Note this cancels out the x^{n+1} term so $\deg h < n+1$. Thus, we can apply the induction hypothesis to h to obtain q_h and r_h so that

$$h = g q_h + r_h.$$

$t = fu + gv = (tq + r)u + gv$

We then have

$$f - \frac{a_{n+1}}{b_m} x^{n+1-m} g = g q_h + r_h$$

i.e.,

$$f = \left(\frac{a_{n+1}}{b_m} x^{n+1-m} + q_h \right) g + r_h.$$

Thus, $q_f = \frac{a_{n+1}}{b_m} x^{n+1-m} + q_h$, $r_f = r_h$. This gives the existence by induction. It remains to prove uniqueness.

Suppose we have

$$f = g q_1 + r_1 \quad \text{and} \quad f = g q_2 + r_2$$

with $r_i = 0$ or $\deg r_i < \deg g$. As before, in the case of integers, we subtract:

$$0 = g(q_1 - q_2) + (r_1 - r_2).$$

Thus,

$$r_1 - r_2 = g(q_2 - q_1).$$

Since $\deg g > \deg (r_1 - r_2)$, we cannot have $g \mid r_1 - r_2$ unless $r_1 = r_2$. Thus, we must have $r_1 = r_2$ and so $q_1 = q_2$. ∎

4.2 Divisibility in $F[x]$:

We now study divisibility of polynomials in $F[x]$. A surprising amount of the results from divisibility in $\mathbb{Z}$ have analogous results

here; in fact, many of the proofs are completely analogous! Throughout F is a field.

Def: Let $f, g \in F[x]$ with $g \neq 0_F$. We say g <u>divides</u> f and write $g \mid f$ if there exists $h \in F[x]$ so that $f = gh$.

Example: We have $(x-1)(x+2)$ divides $(x-1)^2(x+2)(x+3)$ in $\mathbb{Q}[x]$. Here $h = (x-1)(x+3)$. Moreover, we have $a(x-1)(x+2)$ divides $(x-1)^2(x+2)(x+3)$ for any nonzero $a \in \mathbb{Q}$ as then we can take $h = \frac{1}{a}(x-1)(x+3)$.

Note the example shows a polynomial can have infinitely many divisors!

We can define the greatest common divisor as in the case of integers, but the ability to scale by a constant would ruin uniqueness. To remedy this, we require our gcd to be monic, i.e., the leading coefficient must be 1_F.

Def: Let $f, g \in F[x]$ with f and g not both 0_F. The <u>greatest common divisor of f and g</u>, denoted $\gcd(f,g)$, is the monic polynomial of highest degree which that divides f and g. In particular, d is the gcd of f and g provided d is monic

and satisfies

1) $d \mid f$ and $d \mid g$

2) if $c \mid f$ and $c \mid g$, then $\deg c \leq \deg d$.

As in the case of integers, our first example makes use of factorization; this is in general not the most efficient way to calculate the gcd of two polynomials.

Example: Let $f = 2(x-1)^2(x+2)^3(x-1/2)^4(x+10)$ and $g = 7(x+2)^2(x-1/2)^6(x-10)^2(x-15)$. Then

$$\gcd(f,g) = (x+2)^2(x-1/2)^4.$$

As with $\mathbb{Z}$, we want a more efficient method. We again have a Euclidean algorithm here as well, which we know work up to.

Theorem 4.2.1: Let $f, g \in F[x]$ not both 0. There is a unique greatest common divisor d of f and g. Moreover there exist polynomials $u, v \in F[x]$ so that $d = fu + gv$.

Proof: Consider the set

$$S = \{ fm + gn : m, n \in F[x] \}.$$

Let $t \in S$ be the element with minimal degree. This exist because the collection of degrees is a collection of non-negative integers,

so by well-ordering has a minimal element. By definition, there exists $u, v \in F[x]$ so that $t = fu + gv$. We now must argue that $t = \gcd(f,g)$ after we scale it to make it monic. If necessary, scale u, v so that t is monic. Suppose $e \in F[x]$ is a common divisor of f and g. Then e necessarily divides $fu + gv$ (same proof as for integers), so $e \mid t$. Thus, $\deg e \leq \deg t$. It only remains to show that $t \mid f$ and $t \mid g$. Suppose $t \nmid f$. Then write $f = tq + r$ with $0 \leq \deg r < \deg t$.

This gives

$$\begin{aligned} r &= f - tq \\ &= f - (fu+gv)q \\ &= (1 - uq)f + (-vq)g. \end{aligned}$$

Thus, $r \in S$. But $\deg r < \deg t$, which is a contradiction. Thus, it must be the case that $t \mid f$. The same argument shows $t \mid g$.

Thus, t is a monic polynomial dividing f and g and any other common divisor must have smaller degree. Thus, t is a greatest common divisor.

It remains to show t is unique. Suppose t and t' are both gcds of f and g. By property (2) of the definition we have $\deg t \leq \deg t'$ and $\deg t' \leq \deg t$ so we must have $\deg t = \deg t'$. ~~By [illegible]~~

Since t' is a gcd of f and g we have there exist $a, b \in F[x]$ so that $f = t'a$ and $g = t'b$. Thus,

$$t = fu + gv = t'au + t'bv$$
$$= t'(au + bv).$$

Thus, $t' \mid t$. Since $\deg t = \deg t'$ and

$$\deg t = \deg t' + \deg(au + bv),$$

we must have $\deg(au + bv) = 0$, ie, $au + bv = c \in F$.

Moreover, since t and t' are monic, we must have $c = 1$ and so $t = t'$ as desired. ∎

Cor 4.2.2: Let F be a field, $f, g \in F[x]$ not both zero. A monic polynomial $d \in F[x]$ is the gcd of f and g iff it satisfies

1) $d \mid f$ and $d \mid g$
2) if $c \mid f$ and $c \mid g$, then $c \mid d$.

Proof: Exercise. This should follow very much like the analogous result for integers. ∎

Reason

We say f and g are relatively prime if $\gcd(f, g) = 1_F$.

Theorem 4.2.3: Let F be a field and $f, g, h \in F[x]$. If $f \mid gh$ and $\gcd(f, g) = 1_F$, then $f \mid h$.

Proof: This is exactly like the proof for the analogous result for $\mathbb{Z}$. You should write out the details to help you recall how the proof goes. ☒

4.3 Irreducible and Unique Factorization:

Recall that when working in $\mathbb{Z}$ the only units were ± 1. For $F[x]$ there are many more units: every element of F is a unit! That means if we want to factor we can't just consider "positive" elements now as there is no notion of positive and negative.

Def: Let $f \in F[x]$. We say $g \in F[x]$ is an <u>associate</u> of f if $f = ug$ for some unit $u \in F[x]$. (Note in this case unit is the same as element of F.)

Def: We say a nonconstant $f \in F[x]$ is <u>irreducible</u> if its only divisors are associates and ~~nonconstant~~ nonzero constant polynomials. A nonconstant polynomial that is not irreducible is said to be <u>reducible</u>.

Example: Let $f = x \in \mathbb{Q}[x]$. Suppose $g \in \mathbb{Q}[x]$ divides f and $g \notin \mathbb{Q}$. Then there exists $h \in \mathbb{Q}[x]$ s.t. $f = gh$. Since $\deg f = 1 = \deg g + \deg h$ and $\deg g > 0$, we have $\deg g = 1$ and $\deg h = 0$. Thus, $h \in \mathbb{Q}$ and $g = ax + b$ for some $a, b \in \mathbb{Q}$. But then $x = ahx + bh$, i.e., $b = 0$ and $ah = 1$. Thus, g is an associate of f and so f is irreducible.

Theorem 4.3.1: Let F be a field. A nonzero polynomial f is ~~irreducible~~ reducible in $F[x]$ iff f can be written as the product of two polynomials of lower degree.

Proof: Suppose f is reducible, i.e. f has a divisor $g \in F[x]$ where g is nonconstant and not an associate. Thus, there exists $h \in F[x]$ so that $f = gh$. Since we assumed g is not an associate of f or a constant, we have $h \notin F$ so $\deg g < \deg f$. and $\deg h < \deg f$.

Now suppose f is the product of two polynomials of lower degree, say $f = gh$. The only units of $F[x]$ are the elements of F, so g, h are nonconstant and not units, thus f is not reducible. ∎

The field F makes a big difference on whether $f \in F[x]$ is reducible or irreducible. For instance, $f = x^2 - 2$ is irreducible in $\mathbb{Q}[x]$ because $\sqrt{2} \notin \mathbb{Q}$, but if we think of f as an element of $\mathbb{R}[x]$ then

$f = (x-\sqrt{2})(x+\sqrt{2})$.

so it is reducible in $\mathbb{R}[x]$.

Exercise: 1) Let $F \subseteq K$ be fields. Show if $f \in K[x]$ is irreducible, then f is irreducible in $F[x]$ as well.

2) Let $F \subseteq K$ be fields. Show if $f \in F[x]$ is reducible, then f is reducible in $K[x]$ as well.

Theorem 4.3.2: Let F be a field and $p \in F[x]$ a nonconstant polynomial. The following are equivalent:

1) p is irreducible
2) if $b, c \in F[x]$ satisfy $p \mid bc$, then $p \mid b$ or $p \mid c$
3) if $r, s \in F[x]$ with $p = rs$, then r or s is a nonzero element of F.

Proof: 1) $\Rightarrow$ 2) Suppose p is irreducible and $p \mid bc$. If $p \mid b$ we are done, so assume $p \nmid b$. Since p is irreducible this means $\gcd(p, b) = 1$. Thus, there exists s, t with $s, t \in F[x]$ so that $1 = ps + bt$. Multiplying this by c we obtain

$$c = psc + bct.$$

Since $p \mid psc$ and $p \mid bct$, we have $p \mid c$.

2) $\Rightarrow$ 3) Suppose $p = rs$ for some $r, s \in F[x]$. By property 2) we have $p \mid r$ or $p \mid s$. Without loss of generality assume $p \mid r$ so there exists $a \in F[x]$ with $r = pa$. Then we have

$p = rs = pas$.

This gives $\deg p = \deg p + \deg(as)$, i.e. $\deg(as) = 0$. This gives $s \in F$ as desired.

3) $\Rightarrow$ 1) Let $c \in F[x]$ be a divisor of p. Then we can write $p = cb$ for some $b \in F[x]$. Property 3) then gives c or b is a nonzero constant. Thus, the only divisors of p are constants and associates so p is irreducible. ∎

Cor 4.3.3: Let $p \in F[x]$ be irreducible. If $p \mid a_1 \cdots a_n$ for $a_i \in F[x]$, Then $p \mid a_j$ for some j with $1 \le j \le n$.

Proof: Exercise. ∎

Theorem 4.3.4: Let F be a field. Every nonconstant polynomial $f \in F[x]$ is a product of irreducible polynomials in $F[x]$. The factorization is unique: i.e.

$$f = p_1 \cdots p_r$$

and

$$f = q_1 \cdots q_s$$

with each p_j, q_j irreducible, then $r = s$ and after possible reordering and relabelling each p_i is an associate of q_i.

Proof: Exercise. See the same proof for $\mathbb{Z}$. ∎

4.4 Polynomial functions, roots, and reducibility:

We have been very careful thus far to make sure polynomials $f \in F[x]$ are viewed as elements of the polynomial ring $F[x]$ and not as functions. However, each polynomial $f \in F[x]$ induces a function from $F \to F$ as follows. Let $f = \sum_{j=0}^{n} a_j x^j \in F[x]$. This induces the function $f: F \to F$ by $r \mapsto f(r) := \sum_{j=0}^{n} a_j r^j$. This function is referred to as a _Polynomial function_.

It is not the case that different polynomials always induce different functions.

Example: Let $f = x^4 + x + 1 \in (\mathbb{Z}/3\mathbb{Z})[x]$ and $g = x^3 + x^2 + 1 \in (\mathbb{Z}/3\mathbb{Z})[x]$.

These are different polynomials clearly. First, consider the polynomial function induced by $f: \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$:

$$f(0) = 1$$
$$f(1) = 0$$
$$f(2) = 2^4 + 2 + 1 = 1.$$

The polynomial function induced by $g: \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$:

$$g(0) = 1$$
$$g(1) = 0$$
$$g(2) = 2^3 + 2^2 + 1 = 1.$$

Since the functions agree on all values of $\mathbb{Z}/3\mathbb{Z}$ they are the same

function even though they are induced by different polynomials.

The point here is since $\mathbb{Z}/3\mathbb{Z}$ is a finite set there are only finitely many possible functions from $\mathbb{Z}/3\mathbb{Z}$ to $\mathbb{Z}/3\mathbb{Z}$, but there are infinitely many polynomials in $(\mathbb{Z}/3\mathbb{Z})[x]$ so they cannot all induce different functions.

We need some care when making statements. We are used to evaluating polynomials from calculus, but you must keep in mind you don't evaluate polynomials; you evaluate the induced polynomial function.

Def: Let R be a commutative ring and $f \in R[x]$. An element $a \in R$ is said to be a <u>root</u> (or <u>zero</u>) of f if $f(a) = 0_R$

(Note f is a polynomial, $f(a)$ means the polynomial function associated to f evaluated at a.)

<u>Example</u>: Let $f = (x-2)(x+\pi)(x-2i) \in \mathbb{C}[x]$. It is easy to see the roots of the polynomial function associated to f are $2, -\pi$, and $2i$.

<u>Theorem 4.4.1</u>: Let F be a field and $f \in F[x]$. For $a \in F$, the remainder when f is divided by $x-a$ is the value $f(a)$.

Proof: Write $f = (x-a)q + r$ for $q, r \in F[x]$, $r = 0_F$ or $\deg r < \deg(x-a) = 1$. Thus, $r \in F$. Viewing f as a polynomial function, we have

$$f(a) = (a-a)q(a) + r(a)$$
$$= r(0_F)$$

Thus, $r(a) = f(a)$. However, since $r \in F$ we have $r = f(a)$ as claimed. ∎

Example: Find the remainder of $f = x^{50} - x^2 + x + 10$ when divided by $x + 2$ in $(\mathbb{Z}/3\mathbb{Z})[x]$. We have $x + 2 = x - (-2) = x - 1$ in $(\mathbb{Z}/3\mathbb{Z})[x]$. Thus, the remainder is $f(1) = 1^{50} - 1^2 + 1 + 10 = 11 = 2$ in $(\mathbb{Z}/3\mathbb{Z})[x]$.

Theorem 4.4.2: Let F be a field, $f \in F[x]$, and $a \in F$. Then a is a root of f iff $x - a$ is a factor of f in $F[x]$.

Proof: Suppose a is a root of f, ie, $f(a) = 0_F$. Then we have $r = 0_F$ by from above, so $f = (x-a)q$ for some $q \in F[x]$, ie, $(x-a)$ is a factor of f.

Now suppose $(x-a)$ is a factor of f. Then $f = (x-a)q$ for some $q \in F[x]$. Then $f(a) = (a-a)q(a) = 0_F$. Thus, a is a root

of f. ∎

Cor. 4.4.3: Let $f \in F[x]$ be nonzero of degree n. Then f has at most n roots.

Proof: We prove this by induction on n. If $n=1$, then we have $f = ax+b$ for some $a, b \in F$. Then $\alpha = -\frac{b}{a}$ is a root, and the only root so f has at most 1 root. This is our base case. Now for some $k \in \mathbb{Z}_{\geq 1}$ assume any polynomial of degree k has at most k roots.

Let f be a polynomial of degree $k+1$. If f has no roots we are done. Assume f has a root $a \in F$. Then

$$f = (x-a)q$$

for $q \in F[x]$ with degree $q = \deg f - 1 = k$. We apply the induction hypothesis to q to conclude q has at most k roots. Thus, f has at most $k+1$ roots. ∎

Cor. 4.4.4: Let $f \in F[x]$ with $\deg f \geq 2$. If f is irreducible in $F[x]$ then f has no roots in F.

Proof: If f has a root a, then $(x-a)$ is a factor of f. Since $\deg f \geq 2$ we have $q\ (x-a) \mid f$ then f is not irreducible. ∎

Cor 4.4.5: Let $f \in F[x]$ have degree 2 or 3. Then f is irreducible in $F[x]$ iff f has no roots in F.

Proof: We just saw if f is irreducible it has no roots, so it only remains to prove if f has no roots it is irreducible. Suppose f is reducible, so $f = gh$ for $g, h \in F[x]$ with $0 < \deg g, h < \deg f$. If $\deg f = 2$, Then $\deg g = \deg h = 1$. If $\deg f = 3$, Then $\deg g = 2$ and $\deg h = 1$ (or vice versa). In either case, f has a factor of degree 1. However, every polynomial of degree 1 has a root, so f has a root as well. Thus, if f has no root then f is irreducible. ∎

Example: It is key that $\deg f$ is 2 or 3 in the above Cor. For example, $f = (x^2+1)^2 \in \mathbb{R}[x]$ has no roots but is not irreducible!

Cor 4.4.6: Let $f, g \in F[x]$ with F an infinite field. Then f and g induce the same function $F \to F$ iff $f = g$ in $F[x]$.

Proof: Suppose f and g induce the same function $F \to F$. Then $f(a) = g(a)$ for every $a \in F$. Thus, $f(a) - g(a) = 0_F$ for every $a \in F$, i.e., $f(x) - g(x)$ has $a \in F$ as a root for every $a \in F$. However, we know this cannot happen because the number of roots of $f - g$ is bounded by $\deg(f-g)$. Thus, $f = g$.

If $f = g$ in $F[x]$ clearly the same polynomial function is induced. ∎