Chapter 4.1 part 4

F is a field We study $F[x]$

In both rings $\mathbb{Z}$ and $F[x]$, the Fundamental Theorem of Arithmetic holds.

Th1.8 Every integer - element $\mathbb{Z}$ - except 0 and ± 1 can be written as a product of primes in an essentially unique way

Th 4.4 Every polynomial - element of $F[x]$ - except constants can be written as a product of irreducibles in an essentially unique way

Exceptions are the same: these are 0 and the units in the ring ($\mathbb{Z}$ or $F[x]$)

Euclid's Lemma (in $\mathbb{Z}$)

Th1.1 $a, b \in \mathbb{Z}$, $b > 0$

There exist unique $q, r \in \mathbb{Z}$ such that

$$a = bq + r \qquad 0 \leq r < b$$

either $r = 0$ or $0 < r < b$

Euclid's Lemma (in $F[x]$)

Th 4.6 $f, g \in F[x]$ $g \neq 0_F = 0_{F[x]}$

There exist unique $q, r \in F[x]$ such that

$$f = gq + r \qquad \text{either } r = 0_F \text{ or } \deg r < \deg g$$

Pf <u>Uniqueness</u> $f = g q_1 + r_1$ either $r_i = 0_F$ or $\deg r_i < \deg$ $i = 1,2$

$f = g q_2 + r_2$

Wanted: $\underline{r_1 = r_2}$, $\underline{q_1 = q_2}$

If $r_1 = r_2$, then

$g(q_1 - q_2) = 0_F$ implies

$q_1 = q_2$

because $F[x]$ is an integral domain by Cor 4.3

If $q_1 = q_2$, then

$r_2 - r_1 = g \cdot 0_F = 0_F$

We'll use Ex 12 p 94 $\deg(r_1 \pm r_2) \le \max(\deg r_1, \deg r_2)$

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

Assume, for the sake of a contradiction, that $q_1 \neq q_2$, $r_1 \neq r_2$.

By Th 4.2,

$$\deg g + \deg(q_1 - q_2) = \deg(r_2 - r_1)$$

$$\deg(r_2 - r_1) = \max(\deg r_1, \deg r_2) < \deg g$$

$\deg(q_1 - q_2) \geq 0$ by the definition of degree.

Thus the equality cannot hold.

<u>Existence</u>

If there exists $q \in F[x]$ such that $f = gq$, then we are done with $r = 0_F$.

Assume that such $q \in F[x]$ does not exist.

Consider the set

$S = \{ \deg(f - gt) \mid t \in F[x] \}$ - a set of non-negtive integers.

S is non-empty: If $f = 0_F$, then pick $t = 1_F$ with $f - gt = -g \neq 0_F$

If $f \neq 0_F$, then pick $t = 0_F$ with $f - gt = f \neq 0_F$

Thus S has its minimal element: for some $t = q \in F[x]$,

$\deg(f - gq)$ is the smallest possible.

Let $f - gq = r$

We need to prove that $\deg r < \deg g$.

It will follow from:

<u>If $\deg r \geq \deg g$</u>, then there is $t \in F[x]$ such that $\deg(f - gt) < \deg r$.

Let $r = a_0 + \dots + a_n x^n$ $\quad a_n \neq 0_F$

$g = b_0 + \dots + b_m x^m$ $\quad b_m \neq 0_F$ $\qquad n \geq m \quad (\deg r \geq \deg g)$

Let $t = q + a_n b_m^{-1} x^{n-m}$ $\qquad a_n b_m^{-1} \in F$

$$f - gt = f - g(q + a_n b_m^{-1} x^{n-m}) = \underbrace{f - gq}_{r} - g\, a_n b_m^{-1} x^{n-m}$$

$$= r - a_n b_m^{-1} x^{n-m} g$$

$$= a_0 + \dots + \cancel{\underline{a_n x^n}} - \left(b_0 a_n b_m^{-1} x^{n-m} + \dots + \cancel{\underline{a_n b_m^{-1} b_m x^n}} \right).$$

Thus $\deg(f - gt) < n = \deg r = \deg(f - gq)$.