Chapter 4.3

Section 4.3 Irreducibles and unique factorization F - a field

Th 4.14 Every polynomial (element of $F[x]$ except elements of F) can be presented as a product of irreducibles in an essentially unique way

(The Fundamental Theorem of Arithmetic for $F[x]$)

Recall $p \in \mathbb{Z}$, $p \neq 0, \pm 1$ is called a prime if it is divisible by nothing but $\underbrace{1, -1}$, p, $-p$

$\{1, -1\}$ - units in $\mathbb{Z}$

$-p = \underset{\text{unit}}{(-1)} p$

A prime is divisible by nothing except units and itself times a unit

Def f and $g \in F[x]$ are associates if $f = cg$ with $c \in F$, $c \neq 0_F$

(f is an associate of g, or g is an associate of f: $g = c^{-1} f$)

Clearly, every polynomial is divisible by itself, units, its associates

Def $p \in F[x]$, $p \notin F$ is said to be irreducible if its only divisors are units and associates of p

Th4.11 $f \in F[x]$ is <u>reducible</u> (not irreducible) iff
$f \notin F$
f can be written as a product of two polynomials
of <u>lower degree</u>

Analog: $m \in \mathbb{Z}$ is <u>not</u> a prime iff $m = ab$ with $|a| < |m|$
$m \neq 0, \pm 1$ $|b| < |m|$

As we derived Th1.5 from 1.4, let us derive from Th4.10 the following

<u>Prop</u> Let $p \in F[x]$ be an irreducible polynomial.
If $p \mid bc$, then $p \mid b$ or $p \mid c$ (or both)

<u>Pf</u> To prove: "if $p \nmid b$, then $p \mid c$"
It suffices to prove the following:
"if $p \nmid b$, then $(p, b) = 1_F$"

Th4.10: If $p \mid bc$ and $(p, b) = 1_F$, then $p \mid c$

$p \nmid b$ implies that associates of p also don't divide b:
if $(up) \mid b$ then $b = upr = p(ur)$, therefore $p \mid b$

Thus, since p is irreducible and $p \nmid b$, the only common divisors of p and b are units - non-zero polynomials of <u>degree zero</u>.
The only monic polynomial of degree 0 is 1_F. Thus $(p, b) = 1_F$ as required.

Cor 4.13 (parallel to Cor 1.6 for $\mathbb{Z}$)

Let $p \in F[x]$ be an irreducible polynomial.

If $p \mid a_1 \dots a_n$ then $p \mid a_i$ for some i (p must divide at least one of them)

The preparations for the proof of The Fundamental Theorem of Arithmetic are finished.

The proof consists of two parts:

Existence of a presentation - parallel to the proof of Th 1.7

Uniqueness of the presentation - the proof is based on Cor 4.13

"If we have Euclid's Lemma in a ring, then we have the uniquenes clause of the Fundamental Theorem of Arithmetic in the ring"

Examples: $\mathbb{Z}$, $F[x]$ (F - a field)