2.10 Proof of existence and uniqueness of primitive representatives

Proposition 2.11. *Let R be a UFD. Let $\mathbb{F}$ be the field of fractions of R and let $f(x) \in \mathbb{F}[x]$. Then*

(a) *There exists an element $c \in \mathbb{F}$ and a primitive polynomial $g(x) \in R[x]$ such that*

$$f(x) = cg(x).$$

(b) *The factors c and $g(x)$ are unique up to multiplication by a unit in R, i.e. If*

$$f(x) = CG(x)$$

with $C \in \mathbb{F}$ and $G(x) \in R[x]$ primitve then

$$\text{there exists } u \in R^\times \text{ such that} \qquad C = u^{-1}c \qquad \text{and} \quad G(x) = ug(x).$$

(c) *$f(x)$ is irreducible in $\mathbb{F}[x]$ if and only if $g(x)$ is irreducible in $R[x]$.*

Proof.

(a) Let
$$f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_k}{b_k}x^k \in \mathbb{F}[x].$$
Making a common denominator,
$$f(x) = \frac{1}{b_0 b_1 \cdots b_k}(c_0 + c_1 x + \cdots + c_k x^k), \quad \text{where } c_i = a_i b_1 \cdots \hat{b}_i \cdots b_k$$
(the $\hat{b}_i$ denotes omission of the factor b_i in the product).
Let $d = \gcd(c_0, c_1, \ldots, c_k)$.
Letting $c = \frac{d}{b_0 b_1 \cdots b_k} \in \mathbb{F}$ and $g(x) = c_0' + c_1' x + \cdots + c_k' x^k \in R[x]$ where $c_i' = \frac{c_i}{d}$ then
$$f(x) = \frac{d}{b_0 \cdots b_k}(c_0' + c_1' x + \cdots + c_k' x^k) = cg(x)$$
Since d divides c_i then $c_i' \in R$.
Since $\gcd(c_0', c_1', \ldots, c_k') = 1$ then $c_0' + c_1' x + \cdots + c_k' x^k = g(x)$ is primitive.

(b) Suppose $f(x) = cg(x)$ and $f(x) = CG(x)$ where $c, C \in \mathbb{F}$ and $g(x), G(x) \in R[x]$ are primitive polynomials.
Let
$$\begin{matrix} g(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k, \\ G(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_k x^k \end{matrix} \qquad \text{and} \qquad c = \frac{a}{b} \quad \text{and} \quad C = \frac{A}{B},$$
with $a_0, \ldots, a_k, b_0, \ldots, b_k, a, b, A, B \in R$.
Since $f(x) = \frac{a}{b}g(x) = \frac{A}{B}G(x)$ then $aBg(x) = bAG(x)$.
So $aBa_0 = bAb_0, aBa_1 = bAb_1, \ldots, aBa_k = bAb_k$.
Since $g(x)$ is primitive then $\gcd(aBa_0, aBa_1, \ldots, aBa_k) = aB$.
Since $G(x)$ is primitive then $\gcd(bAb_0, bAb_1, \ldots, bAb_k) = bA$.
Thus, by Proposition 16.8,
$$\text{there exists } u \in R^\times \text{ such that} \qquad aB = ubA.$$

So $c = uC$ and $CG(x) = cg(x) = uCg(x) = C(ug(x))$.
By the cancellation law, Proposition 4.46, $G(x) = ug(x)$.
So c and $g(x)$ are unique up to multiplication by a unit.

(c) $\Longrightarrow$: Proof by contrapositive.
Assume $g(x)$ is not irreducible in $R[x]$. To show: $f(x)$ is not irreducible in $\mathbb{F}[x]$.
Then there exist $g_1(x)$ and $g_2(x)$ in $R[x]$ such that $g(x) = g_1(x)g_2(x)$.
So $f(x) = cg(x) = cg_1(x)g_2(x)$.
Since $R[x] \subseteq \mathbb{F}[x]$ then $g_1(x), g_2(x) \in \mathbb{F}[x]$.
So $f(x)$ is not irreducible in $\mathbb{F}[x]$.

(c) $\Longleftarrow$: Proof by contrapositive.
Assume $f(x)$ is not irreducible in $\mathbb{F}[x]$. To show: $g(x)$ is not irreducible in $R[x]$.
Then there are $f_1(x)$ and $f_2(x)$ in $\mathbb{F}[x]$ such that $f(x) = f_1(x)f_2(x)$.
So, by (a), there exist $c_1, c_2 \in \mathbb{F}$ and primitive polynomials $g_1(x), g_2(x) \in R[x]$ such that

$$f_1(x) = c_1 g_1(x) \quad \text{and} \quad f_2(x) = c_2 g_2(x).$$

Let $c = c_1 c_2$.
Then $f(x) = (c_1c_2)g_1(x)g_2(x)$.
By Gauss' lemma, Lemma 2.14, $g_1(x)g_2(x)$ is a primitive polynomial in $R[x]$.
So, by part (b), there exists $u \in R^\times$ such that $g(x) = ug_1(x)g_2(x)$.
So $g(x)$ is not irreducible in $R[x]$.

□