Unique Factorization for Polynomials

Recall: If F is a field and $f \in F[x]$, where $\deg(f) > 0$, then f is reducible over $F \Leftrightarrow$ there exists $g \in F[x]$ with $0 < \deg(g) < \deg(f)$ such that $g|f$.

Theorem 9 (Unique Factorization Theorem) Let $f \in F[x]$, $f \neq 0$. Then there exists $c \in F$ and distinct monic irreducible polynomials $p_1, p_2, \ldots, p_r \in F[x]$ and positive integers $n_1, n_2, \ldots, n_r$ such that

$$(1) \qquad f(x) = c \cdot p_1(x)^{n_1} p_2(x)^{n_2} \cdots p_r(x)^{n_r}.$$

Moreover, c, the polynomials $p_1, \ldots, p_r$ and the integers $n_1, \ldots, n_r$ are uniquely determined by f (up to order).

Notation For a monic irreducible polynomial $p \in F[x]$ put

$$\mathrm{expt}_p(f) = \begin{cases} n_i & \text{if } p = p_i \\ 0 & \text{if } p \neq p_i \text{ for any } i \end{cases}$$

Corollary (GCD-formula) If $f, g \in F[x]$, then $f|g \Leftrightarrow \mathrm{expt}_p(f) \leq \mathrm{expt}_p(g)$, for all monic irreducible polynomials $p \in F[x]$. Thus:

$$\mathrm{expt}_p(\gcd(f,g)) = \min(\mathrm{expt}_p(f), \mathrm{expt}_p(g)).$$