3.6 Factorization in Polynomial Rings

In this section, let \( R \) be an integral domain.

The polynomial ring \( R[x_1, \cdots, x_n] \) consists of elements of a finite sum of monomials \( ax_1^{k_1} \cdots x_n^{k_n} \) with \( a \in R \) and \( k_1, \cdots, k_n \in \mathbb{N} \).

Define \( \deg 0 := -\infty \) for \( 0 \in R[x] \).

Thm 3.29. Let \( f, g \in R[x_1, \cdots, x_n] \).

1. \( \deg(f + g) \leq \max(\deg f, \deg g) \).
2. \( \deg(fg) = \deg f + \deg g \).

Thm 3.30 (The Division Algorithm). Suppose \( f, g \in R[x] \) where the leading coefficient of \( g \) is a unit in \( R \). Then there exist unique polynomials \( q, r \in R[x] \) such that

\[
f = qg + r \quad \text{and} \quad \deg r < \deg g.
\]

It can be proved by induction on \( \deg f \).

Cor 3.31. If \( F \) is a field, then \( F[x] \) is a Euclidean domain, whence \( F[x] \) is a PID and a UFD.

Proof. Define \( \varphi : F[x] - \{0\} \to \mathbb{N} \) by \( \varphi(f) = \deg f \). Verify that \( F[x] \) with \( \varphi \) is a Euclidean domain. □

Cor 3.32 (Remainder Theorem). For any \( f(x) \in R[x] \) and \( c \in R \), there exists a unique \( q(x) \in R[x] \) such that

\[
f(x) = (x - c)q(x) + f(c).
\]

An \( n \)-tuple \( (c_1, \cdots, c_n) \in R^n \) is called a root of \( f \in R[x_1, \cdots, x_n] \) if \( f(c_1, \cdots, c_n) = 0 \).

Cor 3.33. An element \( c \in R \) is a root of \( f \in R[x] \) iff \( x - c \) divides \( f \).

Thm 3.34. If \( f \in R[x] \) has degree \( n \), then \( f \) has at most \( n \) distinct roots in \( R \).

If \( f(x) = (x - c)^mg(x) \) where \( m \in \mathbb{N}^* \) and \( (x - c) \nmid g(x) \), then \( m \) is called the multiplicity of the root \( c \) of \( f \). When \( m > 1 \), \( c \) is called a multiple root.

The formal derivative of \( f = \sum_{i=0}^{n} a_ix^i \in R[x] \) is \( f' = \sum_{k=1}^{n} ka_kx^{k-1} \).

Thm 3.35. Let \( f \in R[x] \) and \( c \in R \).

1. \( c \) is a multiple root of \( f \) iff \( f(c) = 0 \) and \( f'(c) = 0 \).
2. if \( R \) is a field and \( f' \) is relatively prime to \( f \), then \( f \) has no multiple roots in \( R \).
Def. The quotient field of an integral domain $R$ is:

$$F := \{(a,b) \mid a \in R, b \in R - \{0\}\}/\sim,$$

where $(a_1,b_1) \sim (a_2,b_2)$ iff $a_1b_2 = a_2b_1$. Denote $(a,b)$ by $\frac{a}{b}$ for convenience. $F$ is a field under the operations:

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1b_2 + a_2b_1}{b_1b_2}, \quad \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1a_2}{b_1b_2}.$$

From now on, let $R$ be a UFD and $F$ the quotient field of $R$ unless otherwise specified.

Prop 3.36. Let $R$ be a UFD with quotient field $F$. Let $f = \sum_{i=0}^{n} a_i x^i \in R[x]$. If $u = c/d$ is a root of $f$, where gcd$(c,d) = 1$ in $R$, then $c | a_0$ and $d | a_n$ in $R$.

Proof. $f(u) = 0$ implies that $a_0 d^n = c \left( \sum_{i=1}^{n} (-a_i) c^{i-1} d^{n-i} \right)$ and $-a_n c^n = \left( \sum_{i=0}^{n-1} c^i d^{n-i-1} \right) d$. Consequently, if gcd$(c,d) = 1$, then $c | a_0$ and $d | a_n$. \qed

Ex. If $R = \mathbb{Z}$, then $F = \mathbb{Q}$. The proposition may be used to find the possible rational roots of a polynomial in $\mathbb{Z}[x]$ or $\mathbb{Q}[x]$.

Def. A **content** of $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ is defined by: $C(f) := \gcd(a_0, \ldots, a_n)$.

$C(f)$ is unique up to associate.

$f$ is called **primitive** if $a_0, \ldots, a_n$ are relatively prime, i.e. $C(f) = 1_R$.

Every irreducible $f \in R[x]$ is primitive.

Lem 3.37. Let $R$ be a UFD with quotient field $F$. Let $f, g \in R[x]$.

1. $f = C(f)f_1$ where $f_1$ is primitive in $R[x]$.
2. $C(fg) = C(f)C(g)$.
3. $f$ and $g$ are associates in $R[x]$ iff they are associates in $F[x]$.
4. $f$ is irreducible in $R[x]$ iff $f$ is irreducible in $F[x]$.

Check [Hungerford, Algebra] for the short proofs.

Thm 3.38. If $R$ is a UFD, then so is $R[x_1, \ldots, x_n]$.
3.6. FACTORIZATION IN POLYNOMIAL RINGS

Proof. We prove that $R[x]$ is a UFD and then apply induction. Let $F$ be the quotient field of $R$. Let $f \in R[x]$. If $f \in R$, then $f$ obviously has unique factorization. Otherwise, deg $f \geq 1$. Write $f = C(f)f_1$ where $f_1$ is primitive. Either $C(f)$ is a unit or $C(f) = c_1 \cdots c_m$ with each $c_i$ irreducible in $R$ and hence in $R[x]$. The field $F[x]$ is a UFD, so $f_1 = p_1^{e_1} \cdots p_n^{e_n}$ with each $p_i^{e_i}$ irreducible in $F[x]$. Write $p_i^{e_i} = (a_i/b_i)p_i$ where $a_i/b_i \in F$ and $p_i$ is primitive in $R[x]$. Then $p_i$ is irreducible in $F[x]$ and hence in $R[x]$. Let $a = a_1 \cdots a_n$, $b = b_1 \cdots b_n$. Then $bf_1 = ap_1 \cdots p_n$. Hence $C(b) = C(bf_1) = C(ap_1 \cdots p_n) = C(a)$. Thus $u := a/b$ is a unit in $R$. So $f = uc_1 \cdots c_mp_1 \cdots p_n$ is a product of irreducibles in $R[x]$. The uniqueness of factorization in $R[x]$ is implied by the uniqueness of factorization in $F[x]$. □

Thm 3.39 (Eisenstein’s Criterion). Let $R$ be a UFD with $F$ its quotient field. Let $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ with deg $f \geq 1$. If there is an irreducible $p \in R$ such that

\[
p \nmid a_n; \quad p \mid a_i \text{ for } i = 0, \ldots, n-1; \quad p^2 \nmid a_0,
\]

then $f$ is irreducible in $F[x]$. If $f$ is primitive, then $f$ is irreducible in $R[x]$.

The proof is omitted.

Ex. Use Eisenstein’s Criterion to show that:

1. $f = 2x^5 - 6x^3 + 9x^2 - 15 \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$.

2. Suppose $R$ is a UFD. Then $f = y^3 + x^2y^2 + x^3y + x \in R[x,y]$ is irreducible in $R[x,y]$. 