3.6 Factorization in Polynimial Rings

We assume R is commutative UFD.

Def: For $f(x) = a_0 + a_1x + ... + a_nx^n \epsilon R[x]$, $c(f) = gcd(a_0, a_1, ..., a_n)$ is called the *content* of $f(x)$.

Ex: $f(x) = 3x^2 + 6x + 3\epsilon\mathbb{Z}[x]$, then $c(f) = 3$ in $\mathbb{Z}[x]$ and $c(f) = 1$ in $\mathbb{R}[x]$.

Note: (1)$3x^2 + 6x + 3 = 3(x + 1)(x + 1)$ where 3, x+1 are irreducible element in $\mathbb{Z}[x]$. (2)$3x^2 + 6x + 3 = (3x + 3)(x + 1)$ where 3x+3, x+1 are irreducible element in $\mathbb{Q}[x]$.

Def: (1)$f(x)\epsilon R[x]$ is *primitive* if $c(f) = 1$. (2)$f(x)\epsilon R[x]$ is *monic* if the leading coefficient is 1.

Note:An irreducible polynomial is primitive.

Lemma: (*Gauss Lemma*) $c(f(x)g(x)) = c(f(x))c(g(x))$ for $f(x), g(x)\epsilon R[x]$.

Prove: Suppose $f(x) = c(f)f_1(x)$ and $g(x) = c(g)g_1(x)$ where $f_1(x), g_1(x)$ are primitive, then $c(fg) = c(c(f)f_1c(g)g_1) = c(f)c(g)c(f_1g_1)$. It remains to show $c(f_1, g_1) = 1$. Suppose

$$f_1(x) = \sum_{i=0}^{n} a_ix^i \text{ and } g_1(x) = \sum_{i=0}^{m} b_ix^i$$

Suppose P is an irreducible element in R such that $P|c(f_1g_1)$. Let s be smallest integer such that $P|a_i$ for $i < s$ and P can not be divided by a_s. Let t be the smallest integer such that $P|b_j$ for $j < t$ and P can not be divided by b_t. Then $P|\sum_{i+j=s+t} a_ib_j$ and

$$\sum_{i+j=s+t} a_ib_j = a_0b_{s+t} + a_1b_{s+t-1} + ... + a_{s-1}b_{t+1} + a_sb_t + a_{s+1}b_{t-1} + ... + a_{s+t}b_0.$$

Hence $P|a_sb_t, thusP|a_s$ or $P|b_t$ a contradiction.

Lemma: Let F be the quotient field of R,and $f(x), g(x)\epsilon R[x]$ are primitive, then f, g are associate in R[x] if and only if f, g are associate in F[x].

Prove:(necessary)clear. (sufficient)Suppose $f = \frac{b}{a}g$ where $a, b \epsilon R$,then $af = bg$ and $a = c(af) = c(bg)$. Hence $f = g$.

Lemma: Let R be UFD and F be the quotient field of R. Pick primitive polynomial $f(x) \epsilon R[x]$ with degree$\geq$1, then $f(x)$ is irreducible in R[x] if and only if $f(x)$ is irreducible in F[x].

Prove:(necessary)Suppose $f(x) = g(x)h(x)$ for some $g(x), h(x) \epsilon F[x]$ with degree $\geq$1, then $f(x) = cg_1(x)h_1(x)$ for $c \epsilon F$ and $g_1(x), h_1(x) \epsilon R[x]$ are primitive polynomials with degree $\geq$1. Note $g_1(x)h_1(x)$ is primitive. Since $f(x)$ and $g_1(x)h_1(x)$ are associates in F[x],they are also associates in R[x]. Hence $f(x)$ is not irreducible in R[x]. (sufficient)Suppose $f(x) = g(x)h(x)$ where $g(x), h(x) \epsilon R[x]$ are not units in $\mathbb{R}[x]$. Note $1 = c(f)c(gh) = c(g)c(h)$, hence $c(g) = c(h) = 1$ in R. Hence the degree of $g(x), h(x)$ are $\geq$1. Thus $g(x), h(x)$ are not unit in F[x]. Hence $f(x)$ is not irreducible in F[x].