MATH 403/503 L27

Factorization in $D[x]$

To show $\mathbb{Z}[x]$ is a UFD, we study factorization more generally in $D[x]$, where D is an integral domain, specifically a UFD.

Def Let D be a UFD and let

$$p(x) = a_0 + a_1 x + \cdots + a_d x^d \in D[x].$$

The content of $p(x)$ is the gcd of $a_0, a_1, \ldots, a_d$. We say $p(x)$ is primitive if the content of $p(x)$ is 1.

Remark The gcd exists in any UFD and is unique up to mult. by a unit.

Example $3x^2 + 2x + 5 \in \mathbb{Z}[x]$ is primitive

$9x^4 - 6x + 15$ has content 3 so is not primitive.

Theorem (Gauss Lemma for $D[x]$)
Let D be a UFD and $f(x), g(x)$ be primitive pol's in $D[x]$. Then $f(x)g(x)$ is primitive.

Proof Write $f(x)=\sum_{i=0}^{m} a_i x^i$, $g(x)=\sum_{i=0}^{n} b_i x^i$.

Suppose $p \in D$ is a prime dividing the coefficients of $f(x)g(x)$.
Let r be the smallest non-neg. integer such that $p \nmid a_r$. Such r exists since $f(x)$ is primitive. Similarly, let $s \geq 0$ be the smallest integer such that $p \nmid b_s$
Then, consider the coeff c_{r+s} of x^{r+s} in $f(x)g(x)$:

$$c_{r+s} = a_0 b_{r+s} + a_1 b_{r+s-1} + \cdots + a_{r+s} b_0 \quad (*)$$

where we put $a_i = 0$ for $i > m$ and $b_i = 0$ for $i > n$.
Since $p \mid a_0, \ldots, p \mid a_{r-1}$ and $p \mid b_0, \ldots, p \mid b_{s-1}$, p divides all terms in RHS of $(*)$ except the term $a_r b_s$. But $p \mid c_{r+s}$. Contradiction. ∎

Lemma D UFD, $p(x), q(x) \in D[x]$
The content of $p(x)q(x)$ is the product of the contents of $p(x)$, $q(x)$.

Proof $p(x) = c\,p_1(x)$, $\begin{cases} c = \text{content of } p(x) \\ p_1(x) \text{ primitive.} \end{cases}$

and $q(x) = d\,q_1(x)$.

$\Rightarrow p(x)q(x) = cd\,\underbrace{p_1(x)q_1(x)}_{\text{primitive by Thm.}}$

$\Rightarrow [\text{content of } p(x)q(x)] = cd$

Lemma 18.26 D UFD, $F = \text{Frac } D$.
If $p(x) \in D[x]$ can be factored in $F[x]$, say $p(x) = f(x)g(x)$ where $f(x), g(x) \in F[x]$, then $p(x) = f_1(x)g_1(x)$ where $f_1(x), g(x) \in D[x]$ and $\deg f_1(x) = \deg f(x)$, $\deg g_1(x) = \deg g(x)$.

Proof Let $a, b \in D$ - not 0 s.t. $af(x), bg(x) \in D[x]$.

Find $a_1, b_1 \in D$ such that

$af(x) = a_1 \underbrace{f_1(x)}_{\text{primitive}}$ $\quad a_1 = \text{content}(af(x))$

$bg(x) = b_1 \underbrace{g_1(x)}_{\text{primitive}}$ $\quad b_1 = \text{content}(bg(x))$

Then $ab f(x) g(x) = a_1 b_1 \underbrace{f_1(x) g_1(x)}_{\text{primitive by Thm}}$

$\Rightarrow ab \mid a_1 b_1$ say $abc = a_1 b_1$

$\Rightarrow p(x) = c f_1(x) g_1(x)$ ∎

Cor 18.27A primitive pol in $D[x]$ (D UFD) is irr in $D[x]$ iff it is irr in $F[x]$, $F = \text{Frac } D$.

Th 18.29 If D is a UFD, then $D[x]$ is a UFD.

Proof Let $p(x) \in D[x]$ be nonzero nonunit. If $p(x)$ is a constant then it can be factored uniquely into irreducibles since D is a UFD. Suppose $\deg p(x) > 0$. Let $F = \text{Frac } D$. Since $F[x]$ is a ED, it is a PID, hence a UFD. Let

$$p(x) = f_1(x) f_2(x) \cdots f_n(x)$$

be a factorization into irr $f_i(x) \in F[x]$. Choose $a_i \in D \setminus \{0\}$ s.t. $a_i f_i(x) \in D[x]$. Let $b_i = \text{content}(a_i f(x))$ so that $a_i f_i(x) = b_i g_i(x)$, where $g_i(x)$ primitive. By Cor 18.27, each $g_i(x)$ is irr in $D[x]$. We have

$$a_1 \cdots a_n p(x) = b_1 \cdots b_n \underbrace{g_1(x) \cdots g_n(x)}_{\text{primitive by Thm.}}$$

So $a_1 \cdots a_n \mid \text{content}(\text{LHS}) = b_1 \cdots b_n$

$a_1 \cdots a_n \cdot a = b_1 \cdots b_n$ some $a \in D$

$\Rightarrow p(x) = a \cdot g_1(x) \cdots g_n(x)$.

Since D is a UFD, can factor

$a = c_1 c_2 \cdots c_k$, c_i irr in D

$\Rightarrow p(x) = c_1 c_2 \cdots c_k g_1(x) \cdots g_n(x)$.

Shows existence

Uniqueness Suppose

$p(x) = a_1 \cdots a_m f_1(x) \cdots f_n(x)$

$= b_1 \cdots b_r g_1(x) \cdots g_s(x)$

By Cor 18.27 $f_i(x)$, $g_i(x)$ irr in $F[x]$ and a_i, b_i units in F. So can rearrange $g_i(x)$'s so that $f_i(x)$, $g_i(x)$ associates and $n = s$ (since $F[x]$ is a UFD),

$\Rightarrow c_i f_i(x) = d_i g_i(x)$, some $c_i, d_i \in D$.

f_i, g_i primitive $\Rightarrow c_i, d_i$ associates in D.

$\Rightarrow a_1 \cdots a_m = u b_1 \cdots b_n$ in D, u unit

Since D is a UFD, $m=s$.
After relabeling, a_i and b_i are associates $\forall i$.

∎