Math 510B Notes

Peter Kagey

January 17, 2019

Theorem. (recall from 2019-01-11)
If D is a UFD then $D[x]$ is also a UFD.

Lemma. If f factors in $K[x]$ then it factors in $D[x]$. Namely, suppose D is a UFD with field of fractions K, and assume $f(x) \in D[X]$ is primitive. If $f(x) = g(x)h(x) \in K[x]$ then there exists a factorization $f(x) = g_2(x)h_2(x)$ with $g_2, h_2 \in D[x]$, where $g(x) = \alpha g_2(x)$ and $h(x) = \beta h_2(x)$ with $\alpha, \beta \in K$.

Proof of lemma. The polynomials g and h can be written as

$$g(x) = \sum_{i=0}^{n} \left(\frac{a_i}{b_i}\right) x^i, \qquad h(x) = \sum_{i=0}^{m} \left(\frac{c_i}{d_i}\right) x^i$$

with $a_i, b_i, c_i, d_i \in D$. Then let $b = \prod_{i=0}^{n} b_i$ and $d = \prod_{i=0}^{m} d_i$ so that $b \cdot g(x) = g_1(x) \in D[x]$, and $bd \cdot f(x) = g_1(x)h_1(x)$. Since f is primitive, taking the content of both sides, $C(bd \cdot f) = bd \approx C(g_1) \cdot C(h_1)$. Thus

$$\begin{aligned}
bd \cdot f(x) &= g_1(x)h_1(x) \\
&= C(g_1)g_2(x) \cdot C(h_1)h_2(x) && \text{where } g_2 \text{ and } h_2 \text{ are primitive} \\
&\approx bdg_2(x)h_2(x) && \text{where } g_2h_2 \text{ is primitive by Gauss}
\end{aligned}$$

so by the cancellation property, $f(x) = ug_2(x)h_2(x)$ where u is a unit. □

Proof of theorem. Choose $f(x) \in D[x]$.
Existence.
Write $f(x) = C(f)f_1(x)$ where f_1 is primitive with $\deg(f_1) \geq 1$, so that $f(x) \notin D$. Since D is a UFD, $C(f)$ can be factored in D, $C(f) = p_1 \cdots p_k$.

If f_1 is irreducible, then $f(x)$ factors as $p_1 \cdots p_k f_1(x)$.

If f_1 is not irreducible, then $f_1(x) = g(x)h(x)$ with the degree of g and h strictly less than f_1, so by induction on the degree of polynomials, g_1 and h_1 are products of irreducibles, so f factors as $f(x) = p_1 \cdots p_k h_1(x) \cdots h_n(x) g_1(x) \cdots g_m(x)$

Uniqueness.
Assume that f can be factored as both

$$\begin{aligned}
f(x) &= c_1 \cdots c_m p_1(x) \cdots p_n(x) \\
&= d_1 \cdots d_r q_1(x) \cdots q_s(x),
\end{aligned}$$

where c_i, d_i are prime and $p_i(x), q_i(x)$ are irreducible. Further, without loss of generality, move the content of each irreducible polynomial to the coefficient. Then $p_1(x) \cdots p_n(x)$ and $q_1(x) \cdots q_s(x)$ are primitive so $c_1 \cdots c_m \approx d_1 \cdots d_r$ and $c_i \approx d_i$ after relabeling. Therefore $p_1(x) \cdots p_n(x) \approx q_1(x) \cdots q_s(x) \in D[x]$. Consider these terms over the field of fractions $K[x]$, then $p_i(x), q_i(x)$ are irreducible in $K[x]$ since they're irreducible in $D[x]$ (by the lemma.) Then the uniqueness of factorizations in $K[x]$ implies $n = s$ and $p_i(x) \approx q_i(x)$ in $K[x]$.

So for all i, $p_i(x) = \frac{a_i}{b_i}q_i(x)$, so $b_ip_i(x) = a_iq_i(x)$ and thus $C(b_ip_i(x)) = C(a_iq_i(x))$ and $b_i \approx a_i$. Thus $\frac{a_i}{b_i} = \frac{a_i}{ua_i} = u^{-1}$, which is a unit in D. Therefore polynomial parts are unique. $\square$

Theorem. (Eisenstein's irreducibility criteria for UFDs)
Let D be a UFD then $f(x) = a_0 + \ldots + a_nx^n \in D[x]$ is irreducible in $K[x]$ if there exists some prime $p \in D$ such that

1. the prime divides all but the leading coefficient, $p \mid a_0, \ldots p \mid a_{n-1}$, but $p \nmid a_n$, and
2. the prime divides the constant term only once, $p^2 \nmid a_0$.

Proof. By Gauss's lemma, if f factors in $K[x]$ it factors in $D[x]$, so assume that

$$f(x) = g(x)h(x) = (b_0 + \ldots + b_kx^k)(c_0 + \ldots + c_\ell x^\ell).$$

Since $a_0 = b_0c_0$ and $p^2 \nmid a_0$, either $p \nmid b_0$ or $p \nmid c_0$, so assume without loss of generality that $p \nmid b_0$.
Next consider the map $\phi\colon D[x] \to D/\langle p\rangle[x]$ which reduces all coefficients mod p

$$\phi(f(x)) = \overline{f}(x) = \overline{a}_nx^n = (\overline{b}_0 + \ldots + \overline{b}_kx^k)(\overline{c}_0 + \ldots + \overline{c}_\ell x^\ell)$$

where $b_0 \neq 0$, so $x \nmid \overline{g}(x)$. This means $x^n \mid h(x)$, so $l = n$ and $k = 0$, and thus $\overline{g}$ is constant. Therefore $f(x)$ has only trivial factorizations. $\square$