Division Algorithm for Polynomials

A - a commutative ring and $A[x]$ is the polynomial rings. The units in the polynomial ring are

$$A[x]^\times = A^\times \text{ if } A \text{ is an integral domain.}$$

Remark: Integral domain is necessary. ~~Counter Example~~

Example: In $\mathbb{Z}_4[x]$, $(1+2x)(1-2x) = 1$.

Let $f \in A[x]$. If the leading coefficient of f is a non-zero divisor of A, then f is a non-zero divisor in $A[x]$.

Monic polynomial: $f = a_d x^d + a_{d-1} x^{d-1} \cdots a_1 x + a_0$ is called monic if $a_d \in A^\times$.

Divison Algorithm: Let $f, g \in A[x]$, A is any commutative ring. If $g \neq 0$, $g = bx^d +$ lower degree terms

b is the leading coefficient in g $b = lc(g)$ ~~deg~~

then $\exists$ polynomials q and $r \in A[x]$ such that

$$b^s f = qg + r \quad \text{where } s \text{ is } \mathrm{Max}(0, \deg f - \deg g + 1)$$

and degree $r < \deg g$. Moreover, if b is a non-zero divisor in A, then q and r are uniquely defined.

Proof: Proof by induction on s.

When $s = 0$, $\Longrightarrow$ $\deg f - \deg + 1 \leq 0 \Rightarrow \deg f < \deg g$

Choose, $q = 0$, and $r = f$.

Assume the hypothesis to be true ~~for s~~ till less than s.

If $s > 0$, then $\deg f - \deg + 1 \geq 0 \Rightarrow \deg f \geq \deg g$.

$$\left.\begin{aligned} f &= ax^e + \text{lower degree terms} \\ g &= bx^d + \text{lower degree terms} \end{aligned}\right\} \Longrightarrow e \geq d.$$

$bf = bax^e + $ lower degree terms

$ax^{e-d}g = abx^e + $ lower degree terms.

Let $f_1 = bf - ax^{e-d}g. \implies \deg f_1 < e$

Therefore $s_1 = \text{Max}(0, \deg f_1 - \deg g + 1) < s. \implies s_1 \leq s-1$

By applying the induction hypothesis to f_1 and s_1, $\exists\ q_1, r_1$ such that

$$b^{s_1} f_1 = q_1 g + r_1 \text{ where } \deg r_1 < \deg g$$

~~$b^s f_1 \neq$~~ ~~Now substituting~~ From the expression for f_1, we get

$$b^s f = b^{s-1} f_1 + b^{s-1} a x^{e-d} g$$

$$= b^{s-1-s_1} b^{s_1} f_1 + b^{s-1} a x^{e-d} g$$

$$b^s f = b^{s-1-s_1}(q_1 g + r_1) + b^{s-1} a x^{e-d} g$$

$$= (b^{s-1-s_1} q_1 + b^{s-1} a x^{e-d}) g + b^{s-1-s_1} r_1$$

$$\implies b^s f = b^{s-1-s_1}(q_1 + b^{s_1} a x^{e-d}) g + b^{s-1-s_1} r_1$$

$$q = (q_1 + b^{s_1} a x^{e-d}) b^{s-1-s_1}, \quad r = b^{s-1-s_1} r_1$$

Note that $\deg r \leq \deg r_1 < \deg g$. First part proved.

~~First~~ Uniqueness of q and r: Assume that b is a non-zero divisor (NZD) in A, and

$$b^s f = qg + r \quad \& \quad b^s f = q'g + r'$$

$$\implies (q - q')g = (r' - r)$$

Note that $\deg(r' - r) < \deg g$. But b is a NZD which implies $\deg(q - q')g \geq \deg g$. By this contradiction $q - q' = 0$, and $r - r' = 0$.

Corollary: $f, g \in A[X]$, $g \neq 0$, g is monic. Then $\exists$ a unique q and $r \in A[X]$ such that $f = qg + r$ and $\deg r < \deg g$.

26·1 Theorem: K is a field $\Rightarrow K[X]$ is a principal ideal domain (PID).

Proof: Let $\mathfrak{A}$ be an ideal. $\mathfrak{A} \subseteq K[X]$. WMA $\mathfrak{A} \neq 0$ and $\mathfrak{A} \neq K[X]$. Choose a non-zero $g \in A$ with the minimum degree. Note that this is possible. Consider the set

$$M = \{ \deg g \mid g \neq 0, g \in \mathfrak{A} \} \subseteq \mathbb{N}.$$

The well ordered set $\mathbb{N}$ has an minimal element.
It is clear that $K[X]g \subseteq A$. Let $f \in A$. By the division algorithm $\exists$ q and r in ~~$K[X]$~~ $\mathfrak{A}$ such that $f - qr = r$.
However, $\deg r < \deg g$ which violates the minimal degree of g. ~~Thre~~ Therefore, $r = 0$.
Hence any ideal of $K[X]$ must be a principal ideal.

Illustrative Example: $\mathbb{Z}[X]$. Consider the ideal $\mathfrak{A}$ generated by $\{2, X\} = 2\mathbb{Z}[X] + X\mathbb{Z}[X]$. We will show that this ideal is not principal. Suppose it were principle, then $\mathfrak{A} = \mathbb{Z}[X]g$. $g \in \mathfrak{A}$. Also $2 \in g\mathfrak{A}$.
$\Rightarrow 2 = fg \Rightarrow g$ is a constant. Then $g = \pm 1. \Rightarrow 1 \in \mathfrak{A}$.
Now $1 = 2f_1 + Xf_2$. Substitute $X = 0$. Then $1 = 2f_1$ implies $2 \in \mathbb{Z}^\times$ which is a contradiction. Therefore $\mathfrak{A}$ cannot be a principal ideal.

Verify that for a field K, $K[X, Y]$ cannot be a principal ideal. In general, a polynomial ring in one variable, over a PID <u>is not</u> a PID.

We will show later that if K is a field, then every ideal in $K[x_1, x_2 \dots x_n]$ is finitely generated?

Theorem: Let $g \in A[X]$, $g \neq 0$, $\deg g = n$ and g is monic.
i.e, $g = x^n + \dots$ lower degree terms

Let $\mathfrak{a}$ be the ideal $A[X]g$ (ideal generated by g), and B be the quotient ring.

$B = A[X] / A[X]g$. Then B is a free-module with basis $1, \bar{X}, \bar{X}^2, \bar{X}^3 \dots \bar{X}^{n-1}$, where $\bar{X}$ denotes the equivalence class for the element X.

Proof: Consider the ring homomorphism π

$$A[X] \xrightarrow{\pi} B = A[X] / A[X]g$$
$$X \longmapsto \bar{X} \quad \text{Denote } \bar{X} = x \in B.$$
$$f \longmapsto \bar{f}$$

To show $1, x, x^2, \dots x^{n-1}$ is linearly independent.
Note that π is a ring homomorphism because the equivalence relation is also congruent.

Consider $\bar{f} = a_0 + a_1 x + a_1 x^2 \dots \quad a_{n-1} x^{n-1} = 0$
$\Rightarrow \pi(a_0 + a_1 X + a_1 X^2 \dots a_{n-1} X^{n-1}) = \bar{f}$

$$\Rightarrow \underbrace{a_0 + a_1 X + a_2 X^2 \dots a_{n-1} X^{n-1}}_{< \deg g} = \underbrace{q\, g}_{\text{degree} > g}$$

~~Contradict~~ $\Rightarrow a_0 = a_1 = a_2 \dots a_{n-1} = 0$. Therefore LI

Let $b \in B$. Then $b = \pi(f) = \pi(a_0 + a_1 X + \dots \quad a_d X^d)$
$= a_0 + a_1 x + \dots \quad a_d x^d \quad$ (π is A-linear)

Note $g(x) = 0 \Rightarrow x^n = a_0 + a_1 x \dots \quad a_n x^{n-1}$.

Now we can use induction to show that $1, x, \dots x^{n-1}$ is a G.S.