date: monday, march 4, 2024

Division Algorithm in $F[x]$

Theorem: (Division Algorithm) Let $a,b \in \mathbb{Z}$ with $b \neq 0$. Then, there exists unique q and r such that
$$a = bq + r \text{ with } r=0 \text{ or } 0 \leq r < |b|.$$

Theorem: Given any two $a,b \in \mathbb{Z}$, there exists s and t such that $\gcd(a,b) = as+bt$.

We prove similar results about $F[x]$.

Theorem: (Division Algorithm of $F[x]$) Let $a(x), b(x) \in F[x]$ where F is a field and $b \neq 0$. Then, there exists unique $q(x), r(x) \in F[x]$ such that
$$a(x) = b(x)q(x) + r(x)$$
with $r(x)=0$ or $\deg r(x) < \deg b(x)$.

Proof

(Existence) If $a(x)=0$, then $q(x)=r(x)=0$ and $a(x) = 0 = b(x)\cdot 0 + 0$. If $\deg a(x) < \deg b(x)$, let $q(x)=0$ and $r(x)=a(x)$. Then $a(x) = b(x)\cdot 0 + a(x)$. If $\deg a(x) \geq \deg b(x)$, we proceed by strong induction, ie. assume the statement is true for all $a'(x)$ with $\deg a'(x) < \deg a(x)$. Note
$$a(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0$$
and
$$b(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$$
with $a_m \neq 0$, $b_n \neq 0$ and $m \geq n$.
Since $b_n \in F$, $\frac{1}{b_n} \in F$, and so is $\frac{a_m}{b_n} \in F$ (since F is a field). So $\frac{a_m}{b_n}x^{m-n} \in F[x]$.
Then,
$$\begin{aligned} a(x) - \frac{a_m}{b_n}x^{m-n}b(x) &= a_m x^m + \cdots + a_0 - \frac{a_m}{b_n}x^{m-n}(b_n x^n + \cdots + b_0) \\ &= a_m x^m + (\text{lower order terms}) - a_m x^m + (\text{lower order terms}) \\ &= a'(x) \end{aligned}$$
with $\deg a'(x) < \deg a(x)$.
By strong induction, exists $q'(x)$ and $r'(x)$ with
$$a'(x) = b(x)q'(x) + r'(x).$$

So, $[a(x) - \frac{a_m}{b_n}x^{m-n}b(x)] = b(x)q'(x) + r'(x)$.
Thus,

$$\begin{aligned} a(x) &= b(x)q'(x) + \frac{a_m}{b_n}x^{m-n}b(x) + r'(x) \\ &= b(x)[q'(x) + \frac{a_m}{b_n}x^{m-n}] + r'(x). \end{aligned}$$

So let $q(x) = q'(x) + \frac{a_m}{b_n}x^{m-n}$ and $r(x) = r'(x)$.
Note $r(x) = r'(x) = 0$ or $\deg r(x) = \deg r'(x) < \deg b(x)$.

(Uniqueness) Suppose $a(x) = b(x)q(x) + r(x) = b(x)q'(x) + r'(x)$. So $b(x)[q(x) - q'(x)] = r'(x) - r(x)$. If $q(x) \neq q'(x)$, $b(x)[q(x) - q'(x)] \neq 0$. So $\deg(b(x)[q(x) - q'(x)]) \geq \deg b(x)$. But $\deg(r'(x) - r(x)) \leq \max\{\deg r(x), \deg r'(x)\} < \deg b(x)$. This can't happen. So $q'(x) = q(x)$ and $r'(x) = r(x)$.

$\square$

Def$^{\underline{n}}$: A monic polynomial $d(x)$ is a greatest common divisor of $p(x)$ and $q(x)$ if $d(x) | p(x)$ and $d(x) | q(x)$, and if $d'(x) | p(x)$ and $d'(x) | q(x)$, then $d'(x) | d(x)$. Write $d(x) = \gcd(p(x), q(x))$.

Theorem: Let $p(x), q(x) \in F[x]$. Then there exists $a(x)$ and $b(x)$ such that

$$\gcd(p(x), q(x)) = a(x)p(x) + b(x)q(x)$$

(assuming not both $p(x), q(x)$ are 0).

<u>Proof</u>

Let $S = \{a(x)p(x) + b(x)q(x) \mid a(x), b(x) \in F[x]\}$. Let $d(x) \in S$ be the element such that $\deg d(x) \leq \deg t(x)$ for all $t(x) \in S$. Also, by rescaling, can assume $d(x)$ is monic.
Claim: $\gcd(p(x), q(x)) = d(x)$.
Show $d(x) | p(x)$. Apply the division algorithm,

$$p(x) = d(x)\tilde{q}(x) + r(x)$$

with $r(x) = 0$ or $\deg r(x) < \deg d(x)$.
If $\deg r(x) < \deg d(x)$,

$$\begin{aligned} r(x) &= p(x) - d(x)\tilde{q}(x) \\ &= p(x) - [a(x)p(x) + b(x)q(x)]\tilde{q}(x) \\ &= (1 - a(x)\tilde{q}(x))p(x) + q(x)[(-1)b(x)\tilde{q}(x)] \in S \end{aligned}$$

But then S has an element of smaller degree, than $d(x)$. A contradiction.

So $r(x)=0$.
Same proof shows $d(x) \mid q(x)$.
Suppose $d'(x) \mid p(x)$ and $d'(x) \mid q(x)$. So $p(x)=d'(x)p'(x)$ and $q(x)=d'(x)q'(x)$.
Thus, $d(x)=p(x)a(x)+q(x)b(x)=d'(x)p'(x)a(x)+d'(x)q'(x)b(x)$.
So $d'(x) \mid d(x)$.

$\square$

Note: Division Algorithm gives a Euclidean algorithm to find $\gcd(a(x), b(x))$.

$$\begin{aligned}
a(x) &= b(x)q_1(x) + r_1(x) \\
b(x) &= r_1(x)q_2(x) + r_2(x) \\
r_1(x) &= r_2(x)q_3(x) + r_3(x) \\
&\vdots \\
r_{n-2} &= r_{n-1}(x)q_n(x) + \overbrace{r_n(x)}^{\neq 0} \\
r_{n-1} &= r_n(x)q_n(x) + 0
\end{aligned}$$

the monic version of $r_n(x)$ is the gcd of $a(x)$ and $b(x)$

Take-Away: $\mathbb{Z}$ and $F[x]$ are very similar!