2.2 Lecture 7: Division in the polynomial ring $\mathbb{F}[X]$

Recall the division algorithm in $\mathbb{Z}$: if m is a positive integer and n is any integer, then there exist unique integers q and r (respectively called the quotient and remainder on dividing n by m) with $0 \leqslant r < m$ and

$$n = mq + r.$$

This can be proved by observing that there is exactly one integer multiple of m in the interval $[n - m + 1, n]$.

For a field $\mathbb{F}$, the polynomial ring $\mathbb{F}[X]$ has many properties in common with the ring $\mathbb{Z}$ of integers. The first of these is a version of the division algorithm.

Definition 17. *Let* $f(X)$, $g(X)$ *be polynomials in* $\mathbb{F}[X]$*. We say that* $g(X)$ divides $f(X)$ *in* $\mathbb{F}[X]$ *if* $f(X) = g(X)q(X)$ *for some* $q(X) \in \mathbb{F}[X]$ *(i.e. if* $f(X)$ *is a multiple of* $g(X)$ *in* $\mathbb{F}[X]$*).*

We write $g(X)|f(X)$ as a shorthand notation for the statement that $g(X)$ divides $f(X)$. This symbol is a vertical bar - not a dash or a forward or back slash.

Theorem 18. (Division Algorithm in $\mathbb{F}[x]$). *Let* $\mathbb{F}$ *be a field and let* $f(X)$ *and* $g(X)$ *be polynomials in* $\mathbb{F}[X]$ *with* $g(X) \neq 0$*. Then there exist* unique *polynomials* $q(X)$ *and* $r(X)$ *in* $\mathbb{F}[X]$

$$f(X) = g(X)q(X) + r(X).$$

with $r(X) = 0$ *or* $\deg(r(X)) < \deg(g(X))$.

Notes

1. In this situation $q(x)$ and $r(x)$ are called the quotient and remainder upon dividing $f(x)$ by $g(x)$.
2. There are two separate assertions to be proved - the existence of such a $q(x)$ and $r(x)$, and their uniqueness.

Proof: (Existence) Define S to be the set of all polynomials in $\mathbb{F}[x]$ of the form $f(x) - g(x)h(x)$ where $s(x) \in \mathbb{F}[x]$. So S is the set of all those polynomials in $\mathbb{F}[x]$ *that differ from* $f(x)$ *by a multiple of* $g(x)$. Our goal for the existence part of the proof is show that either the zero polynomial belongs to S, or S contains some element whose degree is less than that of $g(x)$.

1. If $0 \in S$ then $f(x) - g(x)h(x) = 0$ for some $h(x) \in \mathbb{F}[x]$, so $f(x) = g(x)h(x)$ and we can take $q(x) = h(x)$ and $r(x) = 0$.
2. If $0 \notin S$, let $r(x)$ be an element of minimal degree in S.

Let m denote the degree of $g(x)$ and write

$$g(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0,\ a_m \neq 0.$$

Let $t = \deg(r(x))$ and write

$$r(x) = b_t x^t + b_{t-1}x^{t-1} + \cdots + b_1 x + b_0,\ b_t \neq 0.$$

We claim that $t < m$. We know since $r(x) \in S$ that there exists a polynomial $h(x) \in \mathbb{F}[x]$ for which

$$r(x) = f(x) - g(x)h(x).$$

Thus

$$b_t X^t + b_{t-1}X^{t-1} + \cdots + b_1 X + b_0 = f(X) - g(X)h(X).$$

If $t \geqslant m$ then $t - m \geqslant 0$. Also $a_m \neq 0$ in $\mathbb{F}$, so a_m has an inverse $1/a_m$ in $\mathbb{F}$ and the element b_t/a_m belongs to $\mathbb{F}$. Now subtract the polynomial $g(X)(b_t/a_m)X^{t-m}$ (which has leading term $b_t X^t$) from both sides of the above equation to get

$$b_t X^t + \cdots + b_1 X + b_0 - g(X)(b_t/a_m)X^{t-m} = f(X) - g(X)h(X) - g(X)(b_t/a_m)X^{t-m}.$$

The left side of the above equation is $r_1(X)$, a polynomial of degree less than t in $\mathbb{F}[X]$. The right hand side is $f(X) - g(X)h_1(X)$ where $h_1(X) = h(X) + (b_t/a_m)X^{t-m}$. Thus $r_1(X)$ belongs to S, contrary to the choice of $r(X)$ as an element of minimal degree in S. We conclude that $t < m$ and

$$f(X) = g(X)h(X) + r(X)$$

is a description of $f(X)$ of the required type. This proves the existence.

Things to think about in this fussy proof:

1. How do we know that $r_1(X)$ above has degree less than t?
2. Why can we conclude that $t < m$ at the third last line above?
3. Where does the proof use the fact that $\mathbb{F}$ is a field?

Uniqueness (this is easier to write down): Suppose that

$$\begin{aligned} f(X) &= g(X)q_1(X) + r_1(X),\ \deg(r_1(X)) < m \text{ or } r_1(X) = 0 \\ \text{and } f(X) &= g(X)q_2(X) + r_2(X),\ \deg(r_2(X)) < m \text{ or } r_2(X) = 0. \end{aligned}$$

Then

$$0 = g(X)(q_1(X) - q_2(X)) + (r_1(X) - r_2(X)) \Longrightarrow g(X)(q_1(X) - q_2(X)) = r_2(X) - r_1(X).$$

Now $g(X)(q_1(X) - q_2(X))$ is either zero or a polynomial of degree at least m, and $r_2(X) - r_1(X)$ is either zero or a polynomial of degree less than m. Hence these two can be equal only if they are both zero, which means $q_1(X) = q_2(X)$ (since $g(X) \neq 0$) and $r_1(X) = r_2(X)$. This completes the proof. □

Let $f(X) \in R[X]$ for some ring R; suppose

$$f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0.$$

If $\alpha \in R$ then we let $f(\alpha)$ denote the element

$$a_n \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$$

of R. Thus associated to the polynomial $f(X)$ we have a function from R to R sending α to $f(\alpha)$. Forming the element $f(\alpha)$ is called *evaluating* the polynomial $f(X)$ at α.

Definition 19. *In the above context,* $\alpha \in R$ *is a* root *of* $f(X)$ *if* $f(\alpha) = 0$.

Theorem 20. *(The Factor Theorem) Let* $f(X)$ *be a polynomial of degree* $n \geqslant 1$ *in* $\mathbb{F}[X]$ *and let* $\alpha \in \mathbb{F}$. *Then* α *is a root of* $f(X)$ *if and only if* $X - \alpha$ *divides* $f(X)$ *in* $\mathbb{F}[X]$.

Proof: By the division algorithm (Theorem 18), we can write

$$f(X) = q(X)(X - \alpha) + r(X),$$

where $q(X) \in \mathbb{F}[X]$ and either $r(X) = 0$ or $r(X)$ has degree zero and is thus a non-zero element of $\mathbb{F}$. So $r(X) \in \mathbb{F}$; we can write $r(X) = \beta$. Now

$$\begin{aligned} f(\alpha) &= q(\alpha)(\alpha - \alpha) + \beta \\ &= 0 + \beta \\ &= \beta. \end{aligned}$$

Thus $f(\alpha) = 0$ if and only if $\beta = 0$, i.e. if and only if $r(X) = 0$ and $f(X) = q(X)(X - \alpha)$ which means $X - \alpha$ divides $f(X)$. □

Remark: This proves more than the statement of the theorem, it proves that $f(\alpha)$ is the remainder on dividing $f(X)$ by $X - \alpha$ in $\mathbb{F}[X]$.