MATH146 - 2025-01-27

GEORGE MCNINCH

Contents

1. Polynomials over a field and the division algorithm

1.1. Some general notions for commutative rings.

Definition 1.1.1. If R is a commutative ring with 1 and if $u \in R$ we say that u is a *unit* - or that u is *invertible* - provided that there is $v \in R$ with $uv = 1$; then $v = u^{-1}$.

We write $R^\times$ for the units in R.

A commutative ring R is a *field* provided that every non-zero element is invertible. Thus R is a field if $R^\times = R \setminus \{0\}$.

Proposition 1.1.2. *If R is a commutative, then $R^\times$ is an abelian group (with operation the multiplication in R).*

For any commutative ring R and elements $a, b \in R$ we say that a **divides** b – written $a \mid b$ – if $\exists x \in R$ with $ax = b$.

Proposition 1.1.3. *For $a, b \in R$ we have $a \mid b$ if and only if $b \in \langle a \rangle$.*

Recall that we introduced the principal ideal $\langle a \rangle = aR$ for any commutative ring R and any $a \in R$. In fact, given $a_1, \cdots, a_n \in R$ we can consider the ideal

$$\langle a_1, \cdots, a_n \rangle = \sum_{i=1}^{n} a_i R$$

defined as

$$\langle a_1, \cdots, a_n \rangle = \left\{ \sum_{i=1}^{n} r_i a_i | r_i \in R \right\}.$$

It is straightforward to check that $\langle a_1, \cdots, a_n \rangle$ is indeed an ideal of R.

Date: 2025-01-28 09:54:50 EST (george@valhalla).

1.2. **The degree of a polynomial.** Let F be a field and consider the ring of polynomials $F[T]$.

Definition 1.2.1. The *degree* of a polynomial $f = f(T) \in F[T]$ is define to be $\deg(f) = -\infty$ if $f = 0$, and otherwise $\deg(f) = n$ where

$$f = \sum_{i=0}^{n} a_i T^i \quad \text{with each } a_i \in F \text{ and } a_n \neq 0.$$

We have some easy and familiar properties of the degree function:

Proposition 1.2.2. *Let $f, g \in F[T]$.*

(a) $\deg(fg) = \deg(f) + \deg(g)$.
(b) $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$ *and equality holds if* $\deg(f) \neq \deg(g)$.
(c) $f \in F[T]^\times$ *if and only if* $\deg(f) = 0$. *In particular,* $F[T]^\times = F^\times$.

Proposition 1.2.3. *Let $f, g \in F[T]$. If $g \neq 0$ and $\deg g < \deg f$ then $[g] = g + \langle f \rangle$ is a non-zero element of $F[T]/\langle f \rangle$.*

1.3. **The division algorithm.**

Theorem 1.3.1. *Let F be a field, and let $f, g \in F[T]$ with $0 \neq g$. Then there are polynomials $q, r \in F[T]$ for which*

$$f = qg + r$$

and $\deg r < \deg g$.

Proof. First note that we may suppose f to be non-zero. Indeed, if $f = 0$, we just take $q = r = 0$. Clearly $f = qg + r$, and $\deg(r) = -\infty < \deg(g)$ since g is non-zero.

We now proceed by induction on $\deg(f) \geq 0$.

For the base case in which $\deg(f) = 0$, we note that $f = c$ is a constant polynomial; here $c \in F^\times$.

If $\deg(g) = 0$ as well, then $g = d \in F^\times$ and then $c = (c/d)d + 0$ so we may take $q = c/d$ and $r = 0$. Now $\deg(r) = -\infty < \deg(g)$ as required.

If $\deg(g) > 0$, we simply take $q = 0$ and $r = f$: we then have $f = 0 \cdot g + f$ and $\deg(f) = 0 < \deg(g)$ as required.

We have now confirmed the Theorem holds when $\deg(f) = 0$.

Proceeding with the induction, we now suppose $n > 0$ and that the Theorem holds whenever f has degree $< n$. We must prove the Theorem holds when f has degree n.

Since f has degree n, we may write $f = a_n T^n + f_0$ where $a_n \in F^\times$ and $f_0 \in F[T]$ has $\deg(f_0) < n$.

Let us write $g = \deg(g)$; we may write $g = b_m T^m + g_0$ where $b_m \in F^\times$ and $g_0 \in F[T]$ has $\deg(g_0) < m$.

If $n < m$ we take $q = 0$ and $r = f$ to find that $f = qg + r$ and $\deg(r) < \deg(g)$.

Finally, if $m \leq n$ we set

$$f_1 = f - (a_n/b_m)T^{n-m}g = a_n T^n + f_0 - \left(\frac{a_n}{b_m} b_m T^n + \frac{a_n}{b_m} T^{n-m} g_0\right) = f_0 - \frac{a_n}{b_m} T^{n-m} g_0.$$

We have $\deg(f_0) < n$ by assumption, and $\deg\left(\frac{a_n}{b_m} T^{n-m} g_0\right) < n$ by the Proposition together with the fact that $\deg(g_0) < m$.

Thus $\deg(f_1) < n$. Now we apply the induction hypothesis to write

$$f_1 = q_1 g + r_1 \quad \text{with } \deg(r_1) < \deg(g).$$

Finally, we have

$$f = f_1 + (a_n/b_m)T^{n-m}g = q_1 g + r_1 + (a_n/b_m)T^{n-m}g = \left(q_1 + (a_n/b_m)T^{n-m}\right) g + r_1$$

so we have indeed written $f = qg + r$ in the required form. $\square$

Corollary 1.3.2. *Let F be a field and let $f \in F[T]$. For $a \in F$, there is a polynomial $q \in F[T]$ for which*

$$f = q(T-a) + f(a).$$

Corollary 1.3.3. *For $f \in F[T]$ an element $a \in F$ is a **root** of the polynomial f if and only if $T - a \mid f$ in $F[T]$.*