Long Division and Roots

Proposition 1. *Let R be a commutative unital ring, and let $a(x), b(x) \in R[x]$ be polynomials such that $b(x) \neq 0$ and the leading coefficient of b is a unit in R. Then there exist polynomials $q(x), r(x) \in R[x]$ such that $a(x) = q(x)b(x) + r(x)$ and either $r(x) = 0$ or $\deg r < \deg b$.*

Proof. If $a(x) = 0$, set $q(x) = r(x) = 0$. Suppose now that $a(x) \neq 0$; we proceed by strong induction on $\deg a$.

- **Base case.** If $\deg a = 0$, then $a(x) = a_0$ is a constant. If $\deg b = 0$, then $b(x) = b_0$ is also a constant, and in this case b_0 is the leading coefficient of b, hence a unit. Let $q(x) = a_0 b_0^{-1}$ and $r(x) = 0$. If $\deg b > 0$, let $q(x) = 0$ and $r(x) = a_0$. Then $a(x) = q(x)b(x) + r(x)$ and we have $\deg b \geq 1 > 0 = \deg r$.
- **Inductive Step.** Suppose the result holds for all polynomials $\overline{a}(x)$ of degree strictly less than n, where $n > 0$, and suppose that $a(x)$ has degree n. If $\deg a < \deg b$, let $q(x) = 0$ and $r(x) = a(x)$. Now suppose instead that $\deg a \geq \deg b$. Let $m = \deg b$ and let a_n be the leading coefficient of $a(x)$ and b_m the leading coefficient of $b(x)$ (which is a unit). Define $\overline{a}(x) = a(x) - a_n b_m^{-1} x^{n-m} b(x)$. Note that $\deg \overline{a} < \deg a$. By the inductive hypothesis, we have $\overline{q}(x), r(x) \in R[x]$ such that $\overline{a}(x) = \overline{q}(x)b(x) + r(x)$ and either $r(x) = 0$ or $\deg r < \deg b$. Define $q(x) = \overline{q}(x) + a_n b_m^{-1} x^{n-m}$. Now

$$\begin{aligned} a(x) - q(x)b(x) &= a(x) - \overline{q}(x)b(x) - a_n b_m^{-1} x^{n-m} b(x) \\ &= \overline{a}(x) - \overline{q}(x)b(x) \\ &= r(x) \end{aligned}$$

  as needed.

By induction, the result holds for all n. □

Corollary 2. *Suppose F is a field.*

1. *$F[x]$ is a Euclidean domain with norm $N(a) = 2^{\deg a}$. In particular, $F[x]$ is also a UFD and a GCD domain.*
2. *$p(x) \in F[x]$ is irreducible iff $p(x)$ cannot be factored as a product of non-constants.*
3. *If $p(x)$ has degree 1, then $p(x)$ is irreducible in $R[x]$.*

The Evaluation Map

So far, we've been thinking of polynomials as objects in their own right. But we can also treat them like functions in the usual sense by "plugging in" ring elements for the variable. Given a polynomial $p(x) = \sum_{i=0}^{n} a_n x^n$ in $R[x]$, R a commutative unital ring, we define the *evaluation map* $\varepsilon_p : R \to R$ by $\varepsilon_p(r) = \sum_{i=0}^{n} a_i r^i$.

Proposition 3 (Factor Theorem)**.** *Let R be a commutative unital ring, with $p(x) \in R[x]$ and $a \in R$. Then a is a root of $p(x)$ if and only if $x - a$ divides $p(x)$ in $R[x]$.*

Proof. Certainly if $x - a$ divides $p(x)$ then a is a root of p. Conversely, suppose a is a root of $p(x)$. Now $b(x) = x - a$ is monic, so by the polynomial long division algorithm we have $q(x), r(x) \in R[x]$ such that $p(x) = q(x)(x-a)+r(x)$ and either $r(x) = 0$ or $\deg r < 1$. If $r(x) \neq 0$, then $r(x) = r_0$ is a constant. Evaluating at a we have $p(a) = r_0$, a contradiction. So $r(x) = 0$ and $x - a$ divides $p(x)$. □

Proposition 4. *Let R be a domain and $p(x) \in R[x]$ a polynomial of degree 2 or 3. Then $p(x)$ cannot be written as a product of nonconstants in $R[x]$ if and only if $p(x)$ does not have a root in R.*

Proof. Note that if $p(x) = a(x)b(x)$, then $\deg a + \deg b$ is either 2 or 3. Thus $p(x)$ is a product of nonconstants iff it has a factor of degree 1. But $p(x)$ has a factor of degree 1 iff it has a root in R. □

Example

- Show that $p(x) = x^2 + 1$ is irreducible over $\mathbb{Z}/(3)$.

1 Eisenstein's Irreducibility Criterion

Proposition 5. *Let R be a domain and $q(x) = \sum_{i=0}^{n} \in R[x]$. Suppose $p \in R$ is prime such that $p \not| a_n$, $p|a_i$ for each $0 \leq i < n$, and $p^2 \not| a_0$. Then $q(x)$ cannot be factored as a product of nonconstants.*

Proof. Suppose we have

$$q(x) = b(x)c(x) = \left(\sum_i b_i x^i\right)\left(\sum_j c_j x^j\right) = \sum_k \left(\sum_{i+j=k} b_i c_j\right) x^k.$$

Note that $q_0 = b_0 c_0$. Since $p|b_0c_0$ and $p^2 \not| b_0c_0$, p divides exactly one of b_0 and c_0; suppose WLOG that $p|b_0$, so $p \not| c_0$. Letting $n = \deg q$, $h = \deg b$, and $k = \deg c$, we have $q_n = b_h c_k$, and since $p \not| q_n$, $p \not| b_h$. Let i be minimal such that $p \not| b_i$. (Note that $0 < i \leq \deg b \leq n$.)

We now have

$$q_i = b_i c_0 + b_{i-1} c_1 + \cdots + b_{i-t} c_t$$

for some t. If $i < n$, then $p|q_i$, and by construction, $p|b_j$ for $j < i$. Thus $p|b_i c_0$, and since $p \not| c_0$ we have $p|b_i$ – a contradiction. So $i = n$ and thus $\deg b = n = \deg q$. But $\deg q = \deg b + \deg c$, so that $\deg c = 0$; hence c is a constant. □