

Polynomials

The Division Algorithm for polynomials

Division Algorithm for integers

Let a and b be any integers with $b > 0$. There are unique integers q and r such that

$$a = qb + r$$

where $0 \leq r < b$.

Division Algorithm for polynomials

Let F be a field, and let $p(x)$ and $g(x)$ be two polynomials in $F[x]$ with $p(x) \neq 0$. There are polynomials $q(x)$ (the quotient) and $r(x)$ (the remainder) such that $g(x) = p(x)q(x) + r(x)$ and either $r(x) = 0$, or $\deg(r(x)) < \deg(p(x))$. Furthermore, $q(x)$ and $r(x)$ are unique.

Key ideas:

- We are dividing $p(x)$ into $g(x)$ here - this statement is equivalent to the familiar

$$\frac{g(x)}{p(x)} = q(x) + \frac{r(x)}{p(x)}$$

$p(x)$ goes into $g(x)$ $q(x)$ times, with a remainder of $r(x)$.

- The coefficients of the polynomials should be elements of a field.
- There's a specific bound on the remainder - we need it to be 0, or of a lesser degree than the divisor $p(x)$.
- The statement of the Division Algorithm doesn't tell you *how* to do polynomial division.

Example:

For $g(x) = x^3 - 5x^2 + 4x + 1$, $p(x) = 2x^2 - 4$, divide $p(x)$ into $g(x)$ to get the quotient $q(x)$ and remainder $r(x)$ as in the Division Algorithm. Express $g(x)$ as

$$g(x) = p(x)q(x) + r(x)$$

Proving the Division Algorithm

The formal proof is in the Nicodemi text, pages 114-115. It's an induction proof. We'll look at some key ideas in the proof here, with illustrative examples. Much of this will be spoken, so be sure to listen.

(Room for notes / thoughts - the formal version is in your text)

The Division Algorithm in $\mathbf{Z}_m[x]$

The Division Algorithm says that division can be performed in any polynomial ring where the coefficients are elements of a field. This includes the polynomial rings $\mathbf{Z}_m[x]$ where m is prime.

- The process of division described in the proof still works, but you need to translate the notation over.
- In particular, the $\frac{a_n}{b_m}x^{n-m}$ part should be translated as $a_n(b_m^{-1})x^{n-m}$, where b_m^{-1} is the multiplicative inverse of b_m in the coefficient field $\mathbf{Z}_m$. It helps to have a Cayley table for that $\mathbf{Z}_m$ in front of you.
- If m is not prime, the Division Algorithm does not apply - it is silent on whether or not you can do the division, since $\mathbf{Z}_m$, m composite is not a field.
- The weaker condition that allows division to work is if b_m^{-1} exists; i.e. if b_m is a unit in the ring $\mathbf{Z}_m$. This depends specifically on the $p(x)$ we are trying to divide, and varies from problem to problem.
- Examples of the process of division in $\mathbf{Z}_m$ are posted live.

Consequences of the Division Algorithm

The Remainder Theorem:

Let $f(x)$ be any polynomial in $F[x]$, and let $p(x) = x - a$. Suppose $f(x) = q(x)(x - a) + r_0$ as in the Division Algorithm. Then $r_0 = f(a)$.

- This theorem says that remainder after dividing by $x - a$ is the same as the value obtained by evaluating the polynomial at a .
- Note that if you're dividing by $x - a$, the remainder has to be a constant (degree 0 or equal to 0), since the Division Algorithm guarantees that $\deg(r(x)) < \deg(p(x))$, and $p(x) = x - a$ has degree 1.

Example:

Try it. Divide $f(x) = x^3 - 4x^2 + 6x + 1$ by $x - 2$, and note the remainder. Then, evaluate $f(2)$.

Proof logic:

- For polynomials in $F[x]$, the Division Algorithm guarantees we can write $f(x) = q(x)(x - a) + r(x)$ with $\deg(r(x)) < \deg(x - a)$.
- Since $\deg(x - a) = 1$, $r(x) = r_0$ must be a constant.
- And since $f(x) = q(x)(x - a) + r_0$, $f(a) = q(a)(a - a) + r_0 = 0 + r_0 = 0$

The Root Theorem:

For any polynomial $f(x)$ in $F(x)$ and any $a \in F$, $f(a) = 0$ if and only if $x - a$ is a factor of $f(x)$.

Example:

Show that $x + 3$ is a factor of $f(x) = 2x^3 + 3x^2 - 11x - 6$.

The Remainder Theorem and Root Theorem are the basis for the PreCalc technique of factoring polynomials of degree higher than 2 by guess-and-check. A typical PreCalc problem would be to factor (for example) $f(x) = x^3 + 2x^2 - 5x - 6$ by observing that the potential roots must be factors of 6 (so $\pm 1, \pm 2, \pm 3, \pm 6$), and start throwing values at it, using synthetic division to evaluate/divide quickly:

$x = 1$ (not a root):

$$\begin{array}{r|rrrr} 1 & 1 & 2 & -5 & -6 \\ & & 1 & 3 & -2 \\ \hline & 1 & 3 & -2 & -8 \end{array} \quad f(1) = -8$$

$x = -1$ (root):

$$\begin{array}{r|rrrr} -1 & 1x^3 & 2 & -5 & -6 \\ & & -1 & -1 & 6 \\ \hline & 1x^2 & 1x & -6 & 0 \end{array} \quad f(-1) = 0$$

$\underbrace{\hspace{1.5cm}}_{g(x)}$

Since $x = -1$ is a root, $x + 1$ is a factor. As an added benefit, synthetic division also produces the quotient resulting from division by $x + 1$:

$$f(x) = (x + 1)(x^2 + x - 6)$$

At that point, it's possible to finish factoring:

$$f(x) = (x + 1)(x + 3)(x - 2)$$

Proof logic:

- Suppose $x - a$ is a factor of $f(x)$. Then $f(x) = p(x)(x - a)$ and $r(x) = r_0 = 0$. By the Remainder Theorem, $f(a) = r_0 = 0$.
- Suppose $f(a) = 0$, and $f(x) = p(x)(x - a) + r_0$ as in the Division Algorithm. By the Remainder Theorem, $r_0 = f(a) = 0$, and so $f(x) = p(x)(x - a)$, and $x - a$ is a factor.

Definition:

If $f(x)$ has a factorization $f(x) = p(x)(x - a)^m$, but $(x - a)^{m+1}$ is not a factor, we say that $x = a$ is a root of **multiplicity** m .

For example, $f(x) = x^4 - x^3 - x + 1$ factors as

$$f(x) = (x - 1)^2(x^2 + x + 1)$$

The real root $x = 1$ has multiplicity 2, and if we were counting the number of real roots, we'd count it twice and say that $f(x)$ has two real roots.

Corollary:

Let F be a field. A polynomial $g(x) \in F[x]$ of degree $n \geq 1$ has at most n roots in F , counting multiplicities.

Proof logic:

- The key idea is that if $g(x)$ has a root $x = a_1$, then it can be factored as

$$g(x) = p_1(x)(x - a_1)$$

and the degree of $p_1(x)$ is $n - 1$.

- If $p_1(x)$ has a root $x = a_2$, then it can be factored as $p_2(x)(x - a_2)$, and we get

$$g(x) = p_2(x)(x - a_1)(x - a_2)$$

so a_2 is also a root of $g(x)$, and $\deg(p_2(x)) = n - 2$.

- This process can be repeated no more than n times - at that point, $\deg(p_n(x)) = n - n = 0$, $p_n(x) = C$ is constant, and the factorization of g would be

$$g(x) = C(x - a_1)(x - a_2)\dots(x - a_n)$$

- This is not a guarantee that you always *can* keep factoring down to all linear factors, just that you can't go any further down than this. There are at most n roots.