Definition: (degree, monic polynomial)

Let $p(x) \in K[x]$. The **degree** of $p(x)$ is the largest power of x in the expression for $p(x)$ that has a nonzero coefficient in K.

This term in $p(x)$ is called the **leading term**, and $p(x)$ is said to be **monic** if the coefficient of the leading term is 1.

Proposition: (degree properties) Let $p(x)$ and $q(x) \in \mathbb{R}[x]$. Then

1) The degree of $p(x) \cdot q(x)$ is the sum of the degrees of $p(x)$ and $q(x)$.

2) The degree of $p(x) + q(x)$ is less than or equal to the maximum of the degrees of $p(x)$ and $q(x)$.

proof: Immediate from the definitions of polynomial multiplication and division. However, there is one convention worth noting!

If $p(x) = 0$, then $p(x) \cdot q(x) = 0$. How does this fit with (1)? In order for this to work we declare the degree of the zero polynomial to be $-\infty$, and enforce the special rules that $-\infty + n = -\infty \quad \forall\, n \in \mathbb{N} \cup \{0\}$ and $-\infty < n \quad \forall\, n \in \mathbb{N} \cup \{0\}$ □

Definition: (polynomial divisibility)

Let $p(x), q(x) \in K[x]$.

We say that $q(x)$ **divides** $p(x)$ if $\exists\ r(x) \in K[x]$ with

$$p(x) = q(x) \cdot r(x)$$

Proposition: (divisibility properties)

Let $f(x), g(x), p(x), q(x), r(x)$ be polynomials in $K[x]$.

1) If $p(x) \cdot q(x) = 1$ then $p(x), q(x)$ have degree zero, i.e., are constant.

2) If $p(x)$ divides $q(x)$ and $q(x)$ divides $p(x)$, then $\exists\ a \in K$ with $a \cdot q(x) = p(x)$.

3) If $q(x)$ divides $p(x)$

and $r(x)$ divides $q(x)$,

then $r(x)$ divides $p(x)$.

4) If $q(x)$ divides $p(x)$

and $q(x)$ divides $r(x)$,

then

$q(x)$ divides

$p(x) \cdot f(x) + r(x) \cdot g(x)$.

proof: 1) If $p(x) \cdot q(x) = 1$, then

neither $p(x)$ nor $q(x)$ is

the zero polynomial.

If either $p(x)$ or $q(x)$ were nonconstant, then one of them would have positive degree, and hence, $p(x) \cdot q(x)$ would have positive degree. Therefore, both $p(x)$ and $q(x)$ are constant.

2) Suppose

$p(x) = f(x)\, q(x)$ and

$q(x) = g(x)\, p(x)$.

Then substituting,

$$p(x) = f(x) \cdot g(x) \cdot p(x),$$

and so

$$0 = f(x) \cdot g(x) \cdot p(x) - p(x)$$

$$0 = (f(x) \cdot g(x) - 1) \cdot p(x).$$

Either $p(x)$ is the zero polynomial,

in which case choosing $a = 0$

will give us $a \cdot g(x) = p(x)$, or

$$f(x) \cdot g(x) - 1 = 0$$

$$\Rightarrow \quad f(x) \cdot g(x) = 1$$

By the previous result,

we must have that $f(x)$

and $g(x)$ are nonzero

constant polynomials,

and so in particular

choosing $a = f(x)$ yields

the result.

3) and 4) maybe later...

□

Definition: (irreducibility) A polynomial $p(x) \in K[x]$ is said to be *irreducible* if $p(x)$ cannot be expressed as the product of two polynomials with strictly positive lower degrees.

Example 1: (irreducibility over different fields)

Consider $p(x) = x^3 + x + 1$.

Assuming K is one of $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$, we can use the quadratic formula to obtain the zeros of $p(x)$ as

$$x = \frac{-1 \pm \sqrt{1 - 4}}{2}$$

$$x = \frac{-1 \pm \sqrt{3}\, i}{2} \in \mathbb{C}$$

If we could factor $p(x)$ over $\mathbb{R}$ or $\mathbb{Q}$, then the factors would have to be linear and of the form

$$x - \left(\frac{-1 \pm \sqrt{3}\, i}{2}\right).$$

This means that $p(x)$ is irreducible in $\mathbb{Q}[x]$ or $\mathbb{R}[x]$, but not irreducible (reducible) in $\mathbb{C}[x]$.

What about $p(x) \in \mathbb{Z}_2[x]$?

Note that if $p(x)$ were reducible, we could write

$p(x) = q(x) \cdot r(x)$ and each of $q(x), r(x)$ must have degree one. Since the constant coefficient of $p(x)$ is one, we'd need

$q(x) = r(x) = x+1$ or

$q(x) = r(x) = x-1 = x+1$

in $\mathbb{Z}_2[x]$.

$$(x+1)(x+1)$$

$$= x^2 + \underbrace{2x}_{0 \text{ in } \mathbb{Z}_2[x]} + 1 = x^2 + 1 .$$

Therefore, x^2+x+1 is irreducible in $\mathbb{Z}_2[x]$.

What about $\mathbb{Z}_3[x]$?

Note that

$$(x+2)(x+2)$$

$$= x^2 + 4x + 4$$

$$= x^2 + x + 1 \quad (\text{in } \mathbb{Z}_3[x])$$

$$= p(x), \quad \text{reducible in } \mathbb{Z}_3[x].$$

Proposition: (irreducible decomposition)

Let $p(x) \in k[x]$. If the degree of $p(x)$ is greater than 0, $p(x)$ may be expressed as either a product of irreducible polynomials in $k[x]$ or $p(x)$ is irreducible.

proof: Induct on the degree of $p(x)$.

If the degree is one, $p(x)$ is irreducible. Now suppose the degree of $p(x)$ is $n > 1$ and that

any polynomial of smaller degree factors into irreducibles.

If $p(x)$ is not irreducible, $\exists\ q(x), r(x) \in k[x]$ of smaller degree such that

$$p(x) = q(x) \cdot r(x).$$

But then by induction, $q(x)$ and $r(x)$ factor into irreducibles, so $p(x)$ factors into irreducibles.

□

Proposition: (division) Let $p(x), q(x)$ be polynomials in $K[x]$.

If the degree of $q(x)$ is not $-\infty$, then $\exists$ polynomials $f(x), r(x)$ in $K[x]$ such that

$$p(x) = q(x) \cdot f(x) + r(x)$$

and the degree of $r(x)$ is smaller than the degree of $q(x)$.

proof: more or less just like the proof for $\mathbb{N}$. $\square$

Proposition: (divisibility and roots)

Let $p(x) \in K[x]$ and let $a \in K$. Then $\exists\, q(x) \in K[x]$ such that $p(x) = q(x)(x-a) + p(a)$.

It follows that $p(a) = 0$ if and only if $x-a$ divides p.

proof: By the previous proposition,

$\exists\ q(x), r(x)$ with

$$p(x) = q(x)(x-a) + r(x).$$

But degree of $r(x)$ must be smaller than that of $x-a$, so $r(x)$ is constant. Setting $x = a$ gives $r(x) = p(a)$ □