Polynomial.hs - Proofs

Joel Richardson

August 22, 2023

1 Division

```
polyDivMod :: ED r => Polynomial r -> Polynomial r -> (Polynomial r, Polynomial r)
polyDivMod a@(Monomial c d) (Monomial c' d')
    | d >= d' = (Monomial (c // c') (d - d'), Monomial (c % c') d)
    | otherwise = (0, a)
polyDivMod a b
    | degree a < degree b = (0, a)
    | isZero q = (0, r)
    | otherwise = (\(q', r') -> (q + q', r')) $ polyDivMod r (expand b)
    where
        q = Monomial (leadingCoeff a // leadingCoeff b) (degree a - degree b)
        r = expand $ a - (q * b)
```

Definition

Suppose R is some ring, then $divmod : R[x] \times R[x] \to R[x] \times R[x]$ is a function such that if $divmod : (a, b) \mapsto (q, r)$ then:

1. $a = q \cdot b + r$
2. If there exists q' such that $a = q' \cdot b$ then $r = 0$
3. If R is a field, then no $r' \in R[x]$ exists such that $degree(r') < degree(r)$ and $a = q \cdot b + r'$

Proof

$$divmod\left(a_n x^n + a_{n-1}x^{n-1} + \ldots,\ b_m x^m + b_{m-1}x^{m-1} + \ldots\right)$$
$$= \begin{cases} qx^{n-m} + rx^n : (q, r) = divmod(a, b) & (a_n x^n + \\ 0 & \text{if } x \in \mathbb{R} \end{cases}$$

Let us consider the monomial case first - take $a = c_a x^{d_a}$ and $b = c_b x^{d_b}$. In this case

$$divide : (a, b) \mapsto \left(\frac{c_a}{c_b} x^{d_a - d_b}, (c_a \mod c_b) x^{d_a - d_b} \right)$$

and,

$$c_b x^{d_b} \cdot \frac{c_a}{c_b} x^{d_a - d_b} + (c_a \mod c_b) x^{d_a} = c_b \cdot (c_a // c_b) x^{d_a} + (c_a \mod c_b) x^{d_a - d_b}$$