Polynomial.hs - Proofs

Joel Richardson

August 21, 2023

1 divide

```
divide :: Ring r => Polynomial r -> Polynomial r -> (Polynomial r, Polynomial r)
divide a@(Monomial c d) (Monomial c' d')
        | d >= d' = (Monomial (c // c') (d - d'), Monomial (c `remainder` c') (d - d'))
        | otherwise = (0, a)
divide a b
        | degree a < degree b = (0, a)
        | isZero q = (0, r)
        | otherwise = (\(q', r') -> (q + q', r')) $ divide 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 $divide : R[x] \times R[x] \to R[x] \times R[x]$ is a function such that if $divide : (a, b) \mapsto (q, r)$ then:

1. $a = q \cdot b + r$
2. If there exists q' such that $a = q' \cdot b$ then $q = q'$
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

First suppose $a = c_a x^{d_a}$ and $b = c_b x^{d_b}$. Then we have

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

and,

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