9.4 Let K be a field and suppose that $f(x)$ is a polynomial of degree $n > 0$ in $K[x]$. Recall from Exercise 9.3 that if $f(x)$ is not irreducible, then $f(x)$ factors as the product of two polynomials of lower degree. Prove Theorem 9.2 by induction on degree n of $f(x)$. First show that for $n = 1$ the degree n polynomial $f(x)$ is irreducible. Then perform the inductive step.

Base case: $n = 1$

The polynomial $f(x)$ has degree $n = 1$

Suppose $f(x) = g(x)h(x)$

We know the sum of degrees will be 1, by theorem 9.1

So one of $g(x), h(x)$ must be a unit with degree 0, and the other must be degree 1

So by exercise 9.3, since one of $g(x), h(x)$ is the same degree as $f(x)$, then $f(x)$ must be irreducible.

Inductive Step:

Inductive Hypothesis: If $f(x)$ is a polynomial of degree n, it is either irreducible or a product of irreducible polynomials

Show that if $f(x)$ is a polynomial of degree $n + 1$, it is either irreducible or a product of irreducible polynomials.

Case: $f(x)$ cannot be factored into polynomials of smaller degree.

Then $f(x)$ is irreducible.

Case: $f(x)$ can be factored into polynomials of smaller degree.

Then $f(x) = g(x)h(x)$, for $g(x), h(x)$ with degrees each less than $n + 1$, sum degrees $n + 1$

So by inductive hypothesis, $g(x)$ is either irreducible or a product of irreducible polynomials.

And similarly, $h(x)$ is either irreducible or a product of irreducible polynomials.

We know $f(x)$ is the product of these polynomials.

So $f(x)$ is a product of irreducible polynomials.

9.8 Prove the division theorem. Proceed as follows.

1. Begin by reviewing how we proved in the integer case that q and r exist. We did an induction on the size of b, with a fixed. If $b = 1$, the desired result is easy to verify. Assume, then, that $b > 1$ and that the division theorem for integers holds for $b - 1$. Then we obtain nonnegative integers q', r' with $b - 1 = aq' + r'$ and $r' < a$. Adding 1 to both sides yields $b = aq' + (r' + 1)$. If $r' + 1 < a$, we are done. Otherwise $r' + 1 = a$, in which case $b = a(q' + 1) + 0$, we again we are done.

Nothing to show, just review.

2. In the polynomial case, we want to mimic this approach as best we can. The size of a polynomial is measured in terms of its degree. Thus we can try to do an induction on the degree of $b(x)$, with $a(x)$ held fixed. It may be best to do this in three stages. First, deal with the case in which $b(x)$ has degree less than the degree of $a(x)$. This should be easy. Then deal with the case in which $b(x)$ and $a(x)$ have the same degree. This is a little trickier, but it is still entirely elementary. You are now ready for the general induction step.

Assume degree $b(x) < a(x)$, then let $q(x) = 0, r(x) = b(x)$. Then division works.

Assume degree $b(x) = a(x)$.

We want $r(x)$ such that degree $r(x) < a(x)$

Then we can pick a polynomial $q(x)$ such that $a(x)q(x) = b(x) - r(x)$, where degree $r(x) < a(x)$

A is the coefficient of the highest term of $a(x)$, and B is the coefficient of the highest term of $b(x)$,

Then let $q(x) = \frac{B}{A}$, then $b(x) - r(x) = \frac{B}{A}a(x)$, so $r(x) = b(x) - \frac{B}{A}a(x)$

Since the highest degree term of $a(x)$ has coefficient A, and $b(x)$ has coefficient of highest degree term B, then the result $b(x) - a(x)q(x)$ does not contain the highest term, so $r(x)$ is less than degree of $a(x)$

So these choices for $q(x), r(x)$ work for the division theorem when degree $a(x) = b(x)$

3. Assume that $b(x)$ has degree n, and that n is larger than the degree of $a(x)$. Make the appropriate induction assumption about polynomials of degree $n - 1$. Taking a hint form the integer case, in which we wrote b as the sum of the smaller integer $b - 1$ and 1, we want to write $b(x)$ in terms of a polynomial of degree $n-1$ and a polynomial of degree 1. Can we write $b(x)$ as $xg(x)$ for some polynomial $g(x)$ of degree $n - 1$? Not necessarily, but we can come close. Observe that you can rewrite $b(x)$ in the form $xg(x) + c$ for some constant c. Use the induction assumption to rewrite $g(x)$ as $a(x)q'(x) + r'(x)$ for suitable polynomials $q'(x), r'(x)$. What do you know about the degree of $r'(x)$? Plug the expression for $g(x)$ back into $xg(x) + c$ and look at what you have. The argument at this point is reminiscent of the argument for the divsion theorem for the integers. You have two cases, depending on the degree of $r'(x)$. In one case, it will be obvious what $q(x)$ and $r(x)$ should be; in the other case, some more work will need to be done.

Assume $b(x)$ is of degree n, where n is large than the degree of $a(x)$

Assume that the theorem holds for all polynomials of degree less than n.

Let $b(x) = b_n x^n + ...b_2 x + b_1$

Then if we say $b(x) = xg(x) + c$,

Then we can choose $g(x) = b_n x^{n-1} + ..b_2$, and let $c = b_1$

Since $g(x)$ has degree less than n, there must exist $q'(x), r'(x)$, and degree $r'(x) < a(x)$

So $g(x) = a(x)q'(x) + r'(x)$

So $b(x) = x[a(x)q'(x) + r'(x)] + b_1$

This is equal to $a(x)(xq'(x)) + (xr'(x) + b_1)$

If degree $(xr'(x) + b_1) < a(x)$, we are done with choices for $q(x), r(x)$

Otherwise, $xr'(x) + b_1$ must be the same degree as $a(x)$

So by part 2, we can find $q''(x), r''(x)$ such that $xr'(x) + b_1 = a(x)q''(x) + r''(x)$

Where degree $r''(x) < a(x)$

So $b(x) = a(x)(xq'(x) + q''(x)) + r''(x)$

4. To prove the uniqueness portion of the theorem, suppose there is another pair of polynomials $s(x), t(x)$ with

$$b(x) = a(x)s(x) + t(x)$$

and with degree of $t(x)$ less than the degree of $a(x)$. Use the degree formula of theorem 9.1 to show that $r(x) - t(x) = 0 = q(x) - s(x)$

Assume $b(x) = a(x)s(x) + t(x)$ and $b(x) = a(x)q(x) + r(x)$

So $a(x)s(x) + t(x) = a(x)q(x) + r(x)$

So $a(x)[s(x) - q(x)] = r(x) - t(x)$

But $r(x), t(x)$ are lower degree than $a(x)$, so $s(x) - q(x)$ must be negative degree

This is only possible if $s(x) - q(x) = 0$

So $0 = t(x) - r(x)$. So $q(x) = s(x), r(x) = t(x)$

9.12 Theorem 9.10: Let K be a field and let $f(x)$ be a nonzero polynomial of degree n. Then $f(x)$ has at most n distinct roots in K.

Prove 9.10 (Hint: if $f(x)$ has $n+1$ distinct roots, what can you say about the degree of $f(x)$?)

Let $f(x)$ be a nonzero polynomial of degree n

Show that there are at most n distinct roots in K

By contradiction: assume that there are more than n distinct roots of $f(x)$ in K

Then the distinct roots of $f(x)$ are $(x-r_1), (x-r_2), ..., (x-r_m)$ for $m > n$

So the product $(x-r_1)(x-r_2)...(x-r_m)$ with degree m divides $f(x)$, by 9.9

But $m > n$, so $f(x)$ must be 0

But this contradicts that $f(x)$ is a nonzero polynomial of degree n