Theorem 16.2 (Division Algorithm for $F[x]$). *Let F be a field and $f(x)$ $g(x) \in F[x]$ where $g(x) \neq 0$. Then there are unique $q(x)$ $r(x) \in F[x]$ such that $f(x) = g(x)q(x) + r(x)$ and either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.*

Proof. If $\deg f(x) < \deg g(x)$, then $q(x) = 0$ and $r(x) = f(x)$, otherwise, we induction/recursion on the degree of $f(x)$: Let $m = \deg f(x)$ and $n = \deg g(x)$,

- Base: For any $g(x)$, if $0 \geq n$ which implies $n = 0$, then there is q such that $f(x) = g(x) \times q + 0$ and $0 = 0$.

- Induction: For any $f(x)$ with degree belows m, and any $g(x)$, there are $q(x)$ and $r(x)$ such that $f(x) = g(x)q(x) + r(x)$, then there are q such that $f_m = g_n \times q$, also, by induction hypothesis, we know there are $q'(x)$ and $r(x)$ such that $f(x) - g(x)qx^{m-n} = g(x)q'(x) + r(x)$, which is in fact $f(x) = g(x)q'(x) + r(x) + g(x)qx^{m-n} = g(x)(q'(x) + qx^{m-n}) + r(x)$.

The result is unique by comparing the degree. □

Corollary 16.1 (Remainder Theorem). *Let F be a field, $a \in F$ and $f(x) \in F[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$.*

Proof. Induction on the degree of $f(x)$ with hypothesis: Let $n = \deg F[x]$, $m \in F$, then $f(a) + ma^{n+1}$ is the remainder in the division of $f(x) + max^n$ by $x - a$.

- Base: Let $n = 0$, $m \in F$, then the remainder in the divison of $f(x) + max^0 = f_0 + ma$ by $x - a$ is obviously $f_0 + ma = f(a) + ma^{0+1} = f(a) + ma$.

- Induction: Let $n = \deg f(a)$, $m \in F$, the remainder in the division of $f(x) + max^n$ by $x - a$ is the divison of $f(x) + max^n - (f_n + ma)x^{n-1}(x - a) = f'(x) + (f_n + ma)x^{n-1}a$ by $x - a$ where $f'(x) = f(x) - f_n x^n$. By induction hypothesis, we know the remainder in the divison of $f'(x) + (f_n + ma)x^{n-1}$ by $x - a$ is $f'(a) + (f_n + ma)a^{n-1+1} = f'(a) + (f_n + ma)a^n = f(a) + ma^{n+1}$.

Then, choose $m = 0$, we get $f(a)$ is the remainder is the divison of $f(a)$ by $x - a$.

The Path: It doesn't work that we induction on the origin proposition, we need to prove that $f(x) - f_n x^{n-1}(x - a) = f'(x) + f_n x^{n-1}a$ divided by $x - a$ produces the remainder we want. Therefore, we need a weaker induction hypothesis. By comparing with the origin proposition, we find that we can prove the origin proposition by replacing f_n with 0 if the new induction hypothesis is true. □

Corollary 16.2 (Factor Theorem)**.** *Let F be a field, $a \in F$ and $f(x) \in F[x]$, then a is a zero of $f(x)$ (i.e. $f(a) = 0$) iff $x - a$ is a factor of $f(x)$.*

Proof.

- ($\Rightarrow$) If $f(a) = 0$, then by Corollary 16.1.
- ($\Leftarrow$) If $x - a$ is a factor of $f(x)$, then the remainder is 0. By Corollary 16.1, we know $f(a)$ is the remainder in the division of $f(x)$ by $x - a$, then $f(a) = 0$, which implies a is a zero of $f(x)$.

□

Theorem 16.3 (Polynomials of Degree n Have at Most n Zeros)**.** *A polynomials of degree n over a field has at most n zeros.*

Proof. We induction on n.

- Base: A polynomials with degree 0 has 0 zero (recall that $f(x) = 0$ has no degree).
- Induction: For any $f(x) \in F[x]$, if $f(x)$ has no zero, then trivial. Suppose $f(a) = 0$ for some $a \in F$, then $f(x) = (x - a)q(x)$. By induction hypothesis, we know $q(x)$ has at most $n - 1$ (1 comes from $\deg(x - a)$) zeros (note that a can be the zero of $q(x)$), then $f(x)$ has at most $n - 1 + 1$ zeros: $q(x)$ has at most $n - 1$ zeros, $(x - a)$ has only one zero (a).

We may count duplicate zeros at once, by replacing $(x - a)$ with $(x - a)^k$, so that $q(a)$ won't be 0. □

Theorem 16.4 ($F[x]$ is a principal integral domain)**.** *Let F be a field, then $F[x]$ is a principal integral domain.*

Proof. F is an integral domain, so is $F[x]$. For any ideal I, let $f(x) \in I$ where $\deg f(x)$ is smallest in I beside the element 0, we claim $\langle f(x) \rangle = I$. For any element $g(x)$ in I, we know $f(x) = g(x)q(x) + r(x)$, then $r(x) = f(x) - g(x)q(x) \in I$. We know $r(x) = 0$ or $\deg r(x) < \deg f(x)$, if $r(x) = 0$, then $g(x) \in \langle f(x) \rangle$, otherwise, $\deg r(x) < \deg f(x)$ contradicts the selection of $f(x)$. Therefore, $I \subseteq \langle f(X) \rangle$.

The Path: We may suppose the proposition is true, and find out what properties the generator should hold. Obviously, it has to have the smallest degree, unless it will unable to generate the element those have smaller degree. Also, it is easy to see that any element with the smallest degree is acceptable since F is a field, we can always get other elements by multiple a field element (degree 0). □