Exercise 16.13. *Let $\phi : R \to S$ a ring homomorphism, define $\overline{\phi} : R[x] \to S[x]$ by $\overline{\phi}(a_n x^n + a_{n-1}x^{n-1} + \dots) = \phi(a_n)x^n + \phi(a_{n-1})x^{n-1} + \dots$. Show that $\overline{\phi}$ is a ring homomorphism.*

Exercise 16.14. *If R and S are ring isomorphic, then $R[x]$ and $S[x]$ are ring isomorphic.*

Exercise 16.16. *Let $f(x)$ and $g(x)$ are cubic polynomials with integer coefficients such that $f(a) = g(a)$ for four (distinct) integer values a. Prove that $f(x) = g(x)$, Generalize.*

Proof. Consider $h(x) = f(x) - g(x)$, $\deg h(x) \leq 3$, therefore there are at most 3 zeros. However, we found that there are four values a such that $f(a) - g(a) = 0$, so $h(x) = 0 \to f(x) = g(x)$.

Moreover, we can show that any polynomials with degree n is determined by $n+1$ points. □

Exercise 16.19 (Degree Rule)**.** *Let D be an integral domain and $f(x)$ $g(x) \in D[x]$. Prove that $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$.*

Proof. Let $n = \deg f(x)$ and $m = \deg g(x)$. Degree is determined by the leading term, while the leading term of $f(x)g(x)$ is $f_n x^n g_m x^m = f_n g_m x^{n+m}$. $f_n g_m$ will never be 0, since D is an integral domain. □

Exercise 16.32. *Give an example of a polynomial of $Z_5[x]$ of positive degree that has the property that $f(a) = 1$ for all $a \in Z_5$.*

Proof. Try $(x-4)(x-3)(x-2)(x-1)x + 1$, normalized $x^5 + 4x + 1$.

The Path: I was trying to find it directly, but I failed, cause I assume that its degree is lower than 5, which is an unappropriate assumption, because $x^5 = x$ is the key of this problem.

Moreover, consider $f(x) = x^p + (p-1)x + 1$ for some prime p, we have $f(a) = 1$ for all $a \in Z_p$. □

Exercise 16.43. *Let F a field, $f(x)$ and $g(x)$ in $F[x]$ and not both zero. If there is no polynomial of positive degree in $F[x]$ that divides both $f(x)$ and $g(x)$, prove that there exist polynomials $h(x)$ and $k(x)$ in $F[x]$ such that $f(x)h(x) + g(x)k(x) = 1$.*

Proof. This problem can be solved by showing $1 \in \langle f(x), g(x) \rangle$. Consider the ideal $\langle f(x), g(x) \rangle$, we know it is principal ideal so that there is $h(x) \in F[x]$

such that $\langle h(x)\rangle = \langle f(x), g(x)\rangle$. We also know $h(x)$ has the minimum degree in $\langle f(x), g(x)\rangle$ and there are $s(x)$ $t(x) \in F[x]$ such that $h(x)s(x) = f(x)$ and $h(x)t(x) = g(x)$, therefore $h(x)$ has to have degree 0. So $h(x) = h_0$ and $h_0 h_0^{-1} \in \langle h(x)\rangle$ since $\langle h(x)\rangle$ is an ideal.

We know every element in $\langle f(x), g(x)\rangle$ has form $f(x)h(x) + g(x)k(x)$ for some $h(x)$ $k(x) \in F[x]$ and $1 \in \langle f(x), g(x)\rangle$. □

Exercise 16.44. *Let F a field, $f(x)$ and $g(x)$ in $F[x]$ and not both zero. A polynomial $d(x) \in F[x]$ is said to be a greatest common divisor of $f(x)$ and $g(x)$ if $d(x)$ divides both $f(x)$ and $g(x)$, and $d(x)$ has maximum degree among all such polynomials. Prove that $\langle f(x), g(x)\rangle = \langle d(x)\rangle$, and there is a unique monic gcd.*

Proof. Trivial. □

Exercise 16.57. *For every prime p, show that $x^{p-1}-1 = (x-1)(x-2)\cdots(x-(p-2))(x-(p-1))$ in $Z_p[x]$.*

Proof. It is easy to see that both side have degree $p-1$, and for any element $a \in Z_p$, a is a zero of both side, therefore they are equal to each other (See Exercise 16.16). □

Exercise 16.58 (Wilson's Theorem)**.** *For every integer $n > 1$, prove that $(n-1)! = n-1 \pmod{n}$ iff n is prime.*

Proof.

- ($\Rightarrow$) Suppose n is not prime and does **NOT** have form p^2 where p is prime, then there is a pair of zero-divisor that makes the left hand side zero. So we suppose $n = p^2$, then the product of all element in $U(p^2) \cup \{p\}$ is $n-1$, then $p = (n-1)(\text{product of } U(p^2))^{-1} \in U(p^2)$.

- ($\Leftarrow$) By let x in Exercise 16.57 be 0, we know $-1 = (-1)^{n-1}(n-1)!$, recall that $-1 = n-1$ in Z_n (even n is not prime) and $a^{n-1} = 1$ in $U(n)$, since $|U(n)| = n-1$. So $n-1 = 1(n-1)!$.

□

Exercise 16.66. *Let R a commutative ring with unity, I is a prime ideal of R. Prove that $I[x]$ is a prime ideal of $R[x]$.*

Proof. For any $f(x)$ $g(x) \in R[x]$ where $f(x)g(x) \in I[x]$, we induction on $(\deg f(x), \deg g(x))$.

- Base (Left): If $\deg f(x) = 0$, since each coefficients are in I, we know that either $f_0 \in I$ or $g(x) \in I[x]$. If $f(x) = 0$, then trivial.
- Base (Right): Ditto.
- Induction: Suppose $\deg f(x) = m$ and $\deg g(x) = n$ where m and n are positive. Consider the leading coefficient of $f(x)g(x)$, it is produced by $f_m g_n$, therefore, one of them is in I. We may suppose $f_m \in I$, otherwise we just swap them. Then $f(x)g(x) = f_m g(x) + f'(x)g(x)$ (where $f'(x)$ is $f(x)$ without leading coefficient), we know $f_m g(x) \in I[x]$ since $f_m \in I$, then by induction hypothesis, we know either $f'(x)$ or $g(x)$ in $I[x]$. If $f'(x) \in I[x]$, so is $f(x) = f_m x^m + f'(x)$, otherwise, $g(x) \in I[x]$.

Note that we don't claim which one is in $I[x]$ at the beginning, cause we don't have sufficient information. □

Exercise 16.70. *Let F a field and let $I = \{\ f(x) \in F[x] \mid \forall a \in F, f(a) = 0\ \}$. Prove that I is an ideal of $F[x]$. Prove that I is infinite when F is finite and $I = \{0\}$ when F is infinite. Find a monic polynomial $g(x)$ such that $I = \langle g(x) \rangle$ when F is finite.*

Proof. I is an ideal cause:

- Non-empty
- For any $f(x)$ $g(x) \in I$, $a \in F$, $f(a) + g(a) = 0$.
- For any $f(x) \in I$, $g(x) \in F[x]$, $a \in F$, $f(a)g(a) = 0g(a) = 0$

Suppose F is finite, then the polynomial $f(x) = (x - a_0)(x - a_1)\cdots$ where $a_i \in F$ is in I, and for any positive integer n, $f(x)x^n \in I$ with degree $\deg f(x) + n$, therefore I is infinite. If F is infinite, then there is no polynomial has infinite zeros except $f(x) = 0$.

If F is finite, the $f(x)$ above is such monic polynomial. □

Exercise 16.75. *Suppose F is a field and there is a ring homomorphism from Z onto F. Show that F is isomorphic to Z_p for some prime p.*

Proof. Why this exercise here...?

$Z/\operatorname{Ker}\phi$ has to be a integral domain, therefore $\operatorname{Ker}\phi = \langle p \rangle$. □