Exercise 17.1. *Suppose that D is an integral domain and F is a field that containing D. If $f(x) \in D[x]$ and $f(x)$ is irreducible over F but reducible over D, what can we say about the factorization of $f(x)$ over D.*

Proof. There must be a polynomial of degree 0 that is not a unit in D but a unit in F and that polynomial divides $f(x)$. $\square$

Exercise 17.3. *Show that a non-constant polynomial from $Z[x]$ that is irreducible over Z is primitive.*

Proof. Let $f(x) \in Z[x]$ that is irreducible over Z and non-constant. Let c be the content of $f(x)$. We know $\deg f(x) > 0$ since it is non-constant. If c is not 1, then by $f(x) = cf(x)/c$, we know $f(x)/c$ is a unit since $f(x)$ is irreducible and c is not a unit. However, $\deg f(x)/c = \deg f(x) > 0$, that means $f(x)$ is not a unit since Z is an integral domain. $\square$

Exercise 17.4. *Let $f(x) \in Z[x]$ where the leading coefficient of $f(x)$ is 1. Let r a rational number and $(x - r)$ divides $f(x)$, show that r is an integer.*

Proof. We denote $x - r$ by $g(x)$ and $f(x)/g(x)$ by $h(x)$. Suppose $r = \frac{s}{t}$ where $\gcd(s, t) = 1$, and let q be the lcm of the denominators of the coefficients of $h(x)$. Then both $tg(x)$ and $qh(x)$ are in $Z[x]$, and now $tqf(x) = tg(x)qh(x)$. Let a be the content of $tg(x)$ and b be the content of $qh(x)$, we observe that a is 1 since $\gcd(t, s) = 1$, therefore $tqf(x) = 1(tg(x)/1)b(qh(x)/b)$. The content of lhs is tq (since the leading coefficient of $f(x)$ is 1), and the content of rhs is b (since both $(tg(x))/1$ and $(qh(x)/b)$ are primitive, so is their product), so $b = tq$. Since $(qh(x))/b = (qh(x))/(tq) = h(x)/t \in Z[x]$, so is $h(x)$, therefore q is 1. Since both $f(x)$ and $g(x)$ are monic, so is $h(x)$, therefore the content of $qh(x) = h(x)$ is 1, so $b = 1$, therefore $1 = t$, which implies r is an integer.

The following proof comes from MathStackExchange. Suppose $r = \frac{s}{t}$. Since $x - r$ divides $f(x)$, we know $f(r) = s^n t^{-n} + a_{n-1}(s^{n-1}t^{-n+1}) + \cdots + a_0 = 0$. We may mutiply both side by t^{n-1} so that every term except the leading term is an integer, that is, $t^{n-1}f(r) = s^n t^{-1} + a_{n-1}(s^{n-1}) + a_{n-2}(s^{n-2}p) + \cdots + a_0 p^{n-1} = 0$. Therefore $s^n t^{-1}$ is an inverse under addition of another integer, then $s^n t^{-1}$ has to be an integer, then $t = 1$, which implies r is an integer. $\square$

Mistake. *Suppose $f(x) = g(x)h(x)$, where $f(x)$ $g(x) \in Z[x]$, then $h(x)$ needs not in $Z[x]$*

Proof. It is impossible to show that $h(x)$ has to be an element of $Z[x]$ by Z is UFD (Theorem 17.6), cause the factorization of $g(x)$ may not be contained in the factorization of $f(x)$ when $h(x)$ is NOT in $Z[x]$. Also, dividing the factorization of $h(x)$ from $f(x)$ is actually performed under Q, not Z (when $h(x)$ is not in $Z[x]$).

Counterexample: $f(x) = 1 = 2(1/2)$. $\square$

Exercise 17.5. *Let F a field and let a be a nonzero element of F.*

- *If $af(x)$ is irreducible over F, prove that $f(x)$ is irreducible over F.*
- *If $f(ax)$ is irreducible over F, prove that $f(x)$ is irreducible over F.*
- *If $f(a + x)$ is irreducible over F, prove that $f(x)$ is irreducible over F.*
- *Use the third property to prove $8x^3 - 6x + 1$ is irreducible over Q.*

Proof.

- Suppose $f(x) = g(x)h(x)$, then $af(x) = ag(x)h(x)$ and we know $ag(x)$ is a unit or $h(x)$ is a unit by $af(x)$ is irreducible.
- Suppose $f(x) = g(x)h(x)$, then by $f(ax) = g(ax)h(ax)$ is irreducible, we may suppose $g(ax)$ is a unit. Then $\deg g(ax) = 0 = \deg g(x)$, therefore $g(ax) = g(x)$ and $g(x)$ is a unit.
- Ditto
- ???

$\square$

Exercise 17.6. *Let F a field and $f(x) \in F[x]$, let a the leading coefficient of $f(x)$, then $a^{-1}f(x)$ is irreducible implies $f(x)$ is irreducible. Note that $a^{-1}f(x)$ is monic (the leading coefficient is 1).*

Proof. Suppose $f(x) = g(x)h(x)$, then $a^{-1}f(x) = a^{-1}g(x)h(x)$ and one of $a^{-1}g(x)$ and $h(x)$ is unit, if $h(x)$ is unit, then trivial. If $a^{-1}g(x)$ is unit, then $g(x)$ is unit with inverse $a^{-1}(a^{-1}g(x))^{-1}$. $\square$

Exercise 17.10. *Suppose that $f(x) \in Z_p[x]$ and $f(x)$ is irreducible over Z_p, where p is a prime. If $\deg f(x) = n$, prove that $Z_p[x]/\langle f(x)\rangle$ is a field with p^n elements.*

Proof. $Z_p[x]/\langle f(x)\rangle$ is a field by Corollary 17.2. Every distinct element in $Z_p[x]$ with degree that below $\deg f(x)$ implies distinct element in $Z_p[x]/\langle f(x)\rangle$, cause they will never produce an element in $\langle f(x)\rangle$, unless they are equal to each other. Therefore $Z_p[x]/\langle f(x)\rangle$ has the same elements as $(Z_p)_0 \oplus (Z_p)_1 \oplus \cdots \oplus (Z_p)_{n-1}$ (the coefficients), which is exactly p^n. □

Exercise 17.18. *Let $f(x) \in Z_2[x]$ and $\deg f(x) = 5$. If neither 0 nor 1 is a zero of $f(x)$. Show that it is sufficient to prove that $f(x)$ is irreducible over Z_2 by showing $x^2 + x + 1$ is not a factor of $f(x)$.*

Proof. Since $f(x)$ has no zero, we know there is no factor with degree 1. Since $f(0) = 1$, we know $f_0 = 1$, therefore any factor $g(x)$ of $f(x)$ must has the property $g(0) = 1$. Now consider $x^2 + 1$, obviously 1 is a zero, but $f(x)$ does not have one. For any factor with degree $n > 2$, we know it must have a factor with degree $5 - n \leq 2$. Therefore the last cast is $x^2 + x + 1$, comes from the hypothesis. □

Exercise 17.19. *For the field $Z_7[x]/I$ where $I = \langle x^2 + 2\rangle$. Find the multiplicative orders of $x + I$ and $x + 1 + I$. Find the multiplicative inverse of $x + I$.*

Proof. By Exercise 17.10, we know $|Z_7[x]/I| = 7^2 = 49$, therefore the order of the multiplicative group of $Z_7[x]$ is 48. It is easy to see that $x^2 = -2$, and $|-2| = |5| = 6$ since $-2 \in U(7)$, therefore $(x^2)^6 = 1$. Since $|x| \neq 1$, $|x|$ is even (otherwise $x^{|x|}$ would have degree 1) and $|x| \geq 12$ (otherwise $|-2|$ will no longer 6), we know that $|x| = 12$. By simply calculate $(x + 1)^4 = 3x$, we see $(x + 1)^{24} = 1$. We need to show that $3, 6, 12$ can not be the order of $x + 1$:

- By $(x + 1)^7 = x^7 + 1 = 6x + 1$ (since $\operatorname{char} Z_7[x]/I = 7$), we know $|x + 1| \neq 6$, otherwise $6x + 1 = x + 1$.
- $|x + 1| \neq 12$ by $|(x + 1)^4| = 6 \neq 3$.
- $|x + 1| \neq 3$ since $(x + 1)^4 = 3x$ and $3x \neq x + 1$.

It is easy to see that $3x$ is an inverse of x since $-6 = 1$. □

Exercise 17.20. *Let F be a field and $f(x) \in F[x]$ be reducible over F with $\deg f(x) > 1$. Prove that $F[x]/\langle f(x)\rangle$ is not an integral domain.*

Proof. By Theorem 14.3, we only need to show that $\langle f(x)\rangle$ is not a prime ideal. Since $f(x)$ is reducible, we know $f(x) = g(x)h(x)$ and both $g(x)$ and $h(x)$ are not unit. We also know that $\deg g(x)$ and $\deg h(x)$ are lower than $\deg f(x)$, therefore both $g(x)$ and $h(x)$ are not in $\langle f(x)\rangle$, which implies $\langle f(x)\rangle$ is not a prime ideal. □

Exercise 17.32. *Let $f(x) \in Z_p[x]$ (or any field). Prove that $f(x)$ has no quadratic factor over Z_p if $f(x)$ has no factor of the form $x^2 + ax + b$.*

Proof. For any quadratic factor of $f(x)$, it has the form $ax^2 + bx + c$, then $ax^2 + bx + c = a(x^2 + a^{-1}bx + a^{-1}c)$, which is impossible. □

Exercise 17.34. *Given that π is not the zero of a nonzero polynomial with rational coefficients, prove that π^2 cannot be written in the form $a\pi + b$, where a b are rational.*

Proof. Consider $f(x) = -x^2 + ax + b$, then π is not the zero of $f(x)$, therefore $\pi^2 \neq a\pi + b$. □

Exercise 17.35 (Rational Root Theorem)**.** *Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 \in Z[x]$ with degree n. If r and s are relatively prime integers and $f(\frac{r}{s}) = 0$, show that $r \mid a_0$ and $s \mid a_n$.*

Proof. We know $(x - \frac{r}{s})$ divides $f(x)$ since $f(\frac{r}{s}) = 0$, so does $sx - r$. Therefore there must be $c \in Z$ such that $sxcx^{n-1} = a_nx^n$, which implies $sc = a_n$ and then $s \mid a_n$. Similarly, at the final step of division, there is $c \in Z$ such that $rc = a_0$. □

Exercise 17.38. *If p is a prime, prove that $f(x) = x^{p-1} - x^{p-2} + x^{p-3} - \cdots - x + 1$ is irreducible over Q.*

Proof. If $p = 2$, then $x + 1$ is irreducible over Q. If $p \neq 2$, then p is an odd integer, we need to show that $f(-x) = x^{p-1} - (-x^{p-2}) + x^{p-3} - \cdots - (-x) + 1$ is irreducible over Q. It follows that the pth Cyclotomic Polynomial is irreducible over Q when p is a prime. (Corollary of Theorem 17.4, I am sorry that it is not in my note) □

Exercise 17.39. *Let F be a field and let $p(x) \in F[x]$ be irreducible over F. If E a field and $F \subseteq E$ and $a \in E$ such that $p(a) = 0$. Show that the mapping $\phi(f(x)) = f(a) : F[x] \to E$ is a ring homomorphism with kernel $\langle p(x)\rangle$.*

Proof. It is easy to see that $\phi(f(x)+g(x)) = f(a)+g(a) = \phi(f(x))+\phi(g(x))$ and $\phi(f(x)g(x)) = f(a)g(a) = \phi(f(x))\phi(g(x))$.

We first show that $\deg p(x)$ is minimal such that $p(a) = 0$. Let $f(x) \in F[x]$ a non-zero element with minimal degree such that $f(a) = 0$, then we know $p(x) = f(x)q(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg f(x)$. Then $p(a) = f(a)q(a) + r(a)$ which is $0 = 0 + r(a)$, therefore $r(a) = 0$ and then $r(x) = 0$, otherwise it contradicts to the assumption that $\deg f(x)$ is minimal such that $f(a) = 0$. Then $p(x) = f(x)q(x)$, since $p(x)$ is irreducible over F, and $f(x)$ is not a unit (since $f(x) \neq 0$ and $f(a) = 0$), therefore $q(x)$ is a unit, and then $\deg f(x) = \deg p(x)$.

For any $f(x) \in F[x]$ such that $f(a) = 0$, we have $f(x) = p(x)q(x) + r(x)$, since $\deg p(x)$ is minimal such that $p(a) = 0$, we know $r(x) = 0$, therefore $p(x)$ divides $f(x)$, which means $f(x) \in \langle p(x) \rangle$.

The Path: I was trying to show that $p(x)$ divides $f(x)$ where $f(a) = 0$, but there is an annoying remainder, so I trying to show that $\deg p(x)$ is minimal by supposing a $g(x) \in F[x]$ such that $\deg g(x) \leq \deg p(x)$ and $g(a) = 0$. However, it is not enough, there is still a remainder, but I found that supposing $\deg g(x)$ is minimal such that $g(a) = 0$ may solve this problem. That is why I don't like LEM. $\square$

Exercise 17.41. *Let F be a field and let $p(x) \in F[x]$ such that $p(x)$ is irreducible over F. Show that $\{ a+\langle p(x) \rangle \mid a \in F \}$ is a subfield of $F[x]/\langle p(x) \rangle$ that is isomorphic to F. For any $a+\langle p(x) \rangle$ and $b+\langle p(x) \rangle$, if $a+\langle p(x) \rangle = b+\langle p(x) \rangle$, then $a-b \in \langle p(x) \rangle$, which means $\langle p(x) \rangle = F[x]$ since $a-b \in F$ is a unit unless $a = b$. Therefore $a = b$, and it is isomorphic to F (bijective), therefore it is a field, and a subfield of $F[x]/\langle p(x) \rangle$.*

Exercise 17.43. *The polynomial $2x^2 + 4$ is irreducible over Q but reducible over Z. State a condition on $f(x)$ that makes the converse of Theorem 17.2 true.*

Proof. $f(x)$ is primitive. Then whenever $f(x)$ is reducible, it must be the product of two non-constant polynomial (otherwise $f(x)$ is no longer primitive), therefore it is reducible over Q. $\square$