Definition 17.1 (Irreducible Polynomials)**.** *Let D an integral domain and $f(x) \in D[x]$ where $f(x)$ is neither zero polynomial nor a unit. We say $f(x)$ is irreducible over D, if $f(x) = g(x)h(x)$ where $g(x)$ $h(x) \in D[x]$, then one of them is unit. A nonzero, nonunit element of $D[x]$ is not irreducible over D is called reducible over D.*

Definition 17.2 (Content)**.** *The content of a non-zero polynomial is the greatest common divisor of the coefficients. A primitive polynomial is an element of $Z[x]$ with content 1.*

Theorem 17.1 (Gauss's Lemma)**.** *The product of two primitive polynomials is primitive.*

Proof. This proof comes from textbook.

Suppose $f(x) = g(x)h(x)$ where $g(x)$ $h(x)$ are primitive. If $f(x)$ is not primitive, then we denote n as the content of $f(x)$, then p divides n where p is prime. Consider $\overline{f}(x)$ $\overline{g}(x)$ $\overline{h}(x)$, which are polynomials with coefficients $\bmod p$.

Then $\overline{f}(x)$ is a zero polynomial in $Z_p[x]$ since the content of $f(x)$ is dividible by p. We know $Z_p[x]$ is an integral domain since Z_p is an integral domain, then either $g(x)$ or $h(x)$ is a zero polynomial, which means the content of $g(x)$ or $h(x)$ is dividible by p, which contradicts to the assumption that $g(x)$ and $h(x)$ are primitive. □

Lemma 17.1. *If $f(x)$ is reducible, then $(n \cdot 1)f(x)$ is reducible where n is a positive integer.*

Proof. Suppose $f(x) = g(x)h(x)$ where both not unit, then $(n \cdot 1)f(x) = (n \cdot 1)g(x)h(x)$. We claim $(n \cdot 1)g(x)$ is not unit. If $(n \cdot 1)g(x)$ is an inverse $\overline{g}$, then $(n \cdot 1)g(x)\overline{g} = g(x)(n \cdot 1)\overline{g} = 1$, therefore $g(x)$ is a unit. (Recall that a polynomial ring is commutative). □

Theorem 17.2. *Let $f(x) \in Z[x]$, if $f(x)$ is reducible over Q, then it is reducible over Z.*

Proof. This proof comes from textbook.

Suppose $f(x) = g(x)h(x)$ where $g(x)$ $h(x) \in Q[x]$ and both not unit. We may suppose $f(x)$ is primitive, otherwise by Lemma 17.1, $nf(x)/n$ is reducible where n is the content of $f(x)$. Let a and b are the lcm of denominators of $g(x)$ and $h(x)$ respectively, then $abf(x) = ag(x)bh(x)$. Furthermore, we may divide $ag(x)$ and $bh(x)$ by their contents, now $abf(x) = cg'(x)dh'(x)$ where c d are the contents of $ag(x)$ $bh(x)$ respectively. We know $g'(x)$ and $h'(x)$ are primitive, so is $g'(x)h'(x)$. Then the content of right hand side is cd and left hand side is ab. Then $f(x) = g'(x)h'(x)$, it is easy to show $g'(x)$ and $h'(x)$ is not unit.

Furthermore, those two polynomials have non-zero degrees, if $f(x)$ is primitive, and $\deg g'(x) = \deg cg'(x) = \deg ag(x) = \deg g(x)$, which implies $g(x)$ is a unit; if $f(x)$ is not primitive, then $f(x)/n$ can be expressed as two polynomials with non-zero degree, so is $nf(x)/n$. □

Theorem 17.3. *Let p a prime and $f(x) \in Z[x]$ with $\deg f(x) \geq 1$. Let $\overline{f}(x)$ be the polynomial in $Z_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x)$ modulo p. If $\overline{f}(x)$ is irreducible over Z_p and $\deg \overline{f}(x) = \deg f(x)$, then $f(x)$ is irreducible over Q.*

Proof. This proof comes from textbook.

Suppose $f(x)$ is reducible over Q, then $f(x)$ is reducible over Z. Then $f(x) = g(x)h(x)$ where $g(x)$ $h(x) \in Z[x]$ and both not unit, and $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$. We know $\deg f(x) = \deg \overline{f}(x)$, then $\deg g(x) = \deg \overline{g}(x)$ and $\deg h(x) = \deg \overline{h}(x)$ cause reducing coefficients of modulo p doesn't increase the degree. Then we know both $\overline{g}(x)$ and $\overline{h}(x)$ are not unit (cause they have non-zero degree), then $\overline{f}(x)$ is reducible over Z_p. □

Theorem 17.5. *Let F a field and $p(x) \in F[x]$. Then $\langle p(x) \rangle$ is a maximal ideal in $F[x]$ iff $p(x)$ is irreducible over F.*

Proof.

- ($\Rightarrow$) If $p(x) = g(x)h(x)$ for some $g(x)$ $h(x) \in F[x]$, we know $\langle p(x) \rangle$ is a prime ideal since it is maximal, then one of $g(x)$ and $h(x)$ is in $\langle p(x) \rangle$. We may suppose $g(x) \in \langle p(x) \rangle$, then $g(x)$ is either zero or $\deg g(x) \geq \deg p(x)$, but $g(x) \neq 0$ and $\deg g(x) \leq \deg p(x)$ (since $p(x) = g(x)h(x)$), therefore $\deg g(x) = \deg p(x)$ and then $\deg h(x) = 0$, which implies $h(x)$ is a unit.

- ($\Leftarrow$) Suppose I is an ideal that properly contains $\langle p(x) \rangle$, we know $F[x]$ is a principal ideal domain. Suppose $I = \langle q(x) \rangle$ for some $q(x)$, then we know $p(x)$ can be expressed by $q(x)r(x)$ for some $r(x)$ since $p(x) \in \langle q(x) \rangle$. Then one of $q(x)$ and $r(x)$ is unit, if $q(x)$ is unit, then $1 \in \langle q(x) \rangle$, if $r(x)$ is unit, then $q(x) = p(x)r^{-1}(x)$, which implies $q(x) \in \langle p(x) \rangle$, it contradict to the assumption that I properly contains $\langle p(x) \rangle$.

□

Corollary 17.1. *Let $p(x)$ a irreducible polynomial of $F[x]$ and $p(x) \mid a(x)b(x)$. Then $p(x) \mid a(x)$ or $p(x) \mid b(x)$.*

Proof. By Theorem 17.5, we know $\langle p(x) \rangle$ is a maximal ideal, therefore it is a prime ideal. The rest of proof is trivial. $\square$

Corollary 17.2. *Let $f(x)$ is irreducible polynomial of $F[x]$, then $F[x]/\langle f(x) \rangle$ is a field.*

Proof. By Theorem 17.5 and Theorem 14.4. $\square$

Theorem 17.6 (Unique Factorization)**.** *Every polynomial in $Z[x]$ that is not a zero polynomial or a unit in $Z[x]$ can be expressed in the form*

$$\boxed{b_0 b_1 \dots b_{s-1} p_0(x) p_1(x) \dots p_{m-1}(x)}$$

where the b_i's are irreducible polynomials of degree 0 (In other words, they are primes), and $p_i(x)$'s are irreducible polynomials of positive degree.

Furthermore, if is can be expressed in two ways, then they have the same s and m, and they have the same b_i's and p_i's with $\pm$ if needed.

Proof. Let $f(x) \in Z[x]$ where $f(x)$ is not a zero polynomial and not a unit in $Z[x]$. Induction on the degree of $f(x)$.

- Base: we can written $f(x) = f_0$ in the product of primes, and we know that is a unique factorization.
- Ind: We can always express $f(x)$ in form $cg(x)$ where c is the content of $f(x)$ when $f(x)$ is not primitive, then c has unique factorization. We need to show that $g(x)$ has unique factorization. If $g(x)$ is irreducible, then we the only factorization of $g(x)$ is itself. If $g(x)$ is reducible, we know there is $p(x) \in Z[x]$ such that $p(x) \mid g(x)$ and $p(x)$ is irreducible and primitive. We know $p(x)$ must be contained in every factorization of $g(x)$ by Corollary 17.1, then by induction hypothesis, $g(x)/p(x)$ has unique factorization and $g(x) = p(x)g(x)/p(x)$.

$\square$