Let $k$ be a field.

**Theorem** (6.25)**.** Every ideal in $k[x]$ is principal, and every nonzero ideal has a unique monic generator.

**Definition.** The gcd of the zero polynomial and itself is the zero polynomial. A gcd of polynomials $f(x)$ and $g(x)$ (at least one of which is nonzero) is a common divisor of $f$ and $g$ in $k[x]$ of maximal degree.

**Proposition.** Every nonzero polynomial in $k[x]$ has a **unique** monic associate.

*Proof.* That every nonzero polynomial in $k[x]$ has a monic associate is Proposition 6.4. We claim that it is unique. Suppose $f$ and $g$ are both monic associates of $h$. Then $f = uh$ and $g = vh$ for $u, v$ nonzero constants in $k$, by Proposition 6.4, and $f = (uv^{-1})g$. Since $f$ and $g$ are monic, their leading coefficients are one. On the other hand, the leading coefficient of $f$ is $uv^{-1}$. Thus $uv^{-1} = 1$, and $f = g$. □

**Proposition.** Let $f$ and $g$ be polynomials in $k[x]$ of the same degree. If $f|g$, then $f$ and $g$ are associate. If, in addition, $f$ and $g$ are monic, then $f = g$.

*Proof.* Suppose $f|g$. Then there is a polynomial $h \in k[x]$ such that $g = fh$. By Lemma 5.8(ii), $\deg g = \deg f + \deg h$. Since $\deg g = \deg f$, $\deg h = 0$, i.e. $h$ is a nonzero constant. Since $k$ is a field, $h$ is a unit in $k$ and thus a unit in $k[x]$ by Proposition 6.2, proving that $f$ and $g$ are associates in $k[x]$.

Suppose, in addition, that $f$ and $g$ are monic. In this case they must be equal, since each polynomial is associate to a *unique* monic polynomial. □

**Theorem** (6.30(i))**.** Let $f$ and $g$ be polynomials in $k[x]$, at least one of which is nonzero. Let $d$ be a monic polynomial. Then $d$ is a gcd of $f$ and $g$ if and only if $(f, g) = (d)$.

*Proof.* If $(f, g) = (d)$, then the argument in the text for the proof of Theorem 6.28 (analogous to Theorem 1.19) proves that $d$ is a gcd of $f$ and $g$.

Now suppose $d$ is a gcd of $f$ and $g$, and let $h$ be the unique monic generator for $(f, g)$. Since $d$ divides $f$ and $g$, it divides every linear combination of $f$ and $g$ (by the "two out of three" rule), so $d|h$, and $\deg d \leq \deg h$ by Lemma 6.1. On the other hand, since $h$ is a common divisor of $f$ and $g$, $\deg h \leq \deg d$, by the definition of gcd. Thus $\deg h = \deg d$. Thus $h$ and $d$ are monic polynomials of the same degree with $d|h$. By the proposition above, $d = h$, and thus $(f, g) = (d)$. □

**Note.** This means that we can characterize a gcd of $f$ and $g$ as a monic polynomial of least degree that is a linear combination of $f$ and $g$.

**Note.** The theorem also shows that every linear combination of $f$ and $g$ is a multiple of $d$ in $k[x]$.

**Corollary** (6.29)**.** Let $d$ be a monic common divisor of $f$ and $g$ in $k[x]$. Then $d$ is the gcd of $f$ and $g$ if and only if every common divisor of $f$ and $g$ also divides $d$, i.e. if $h|f$ and $h|g$, then $h|d$.

*Proof.* Let $h$ be a common divisor of $f$ and $g$.

First, suppose that every common divisor of $f$ and $g$ divides $d$. Then $h|d$ and $\deg h \leq \deg g$, by Lemma 6.1. Thus $d$ is of maximal degree among common divisors of $f$ and $g$. By definition, $d$ is a gcd of $f$ and $g$.

On the other hand, suppose that $d$ is a gcd of $f$ and $g$. Then, by the theorem, we can write $d$ as a linear combination $f$ and $g$. By the "two out of three" rule, $h$ divides $d$, since $h$ divides $f$ and $g$. □

**Corollary** (Theorem 6.30(ii))**.** GCDs in $k[x]$ are unique.

*Proof.* This follows immediately from the theorem and from the uniqueness of monic generators for ideals in $k[x]$ (Theorem 6.25). □