**Definition**

Suppose that $F$ is a field and that $f, g, p \in F[x]$ with $p \neq 0$. Then we say that $f$ is congruent to $g$ modulo $p$ and write $f \equiv g \pmod{p}$ if $p|(f - g)$.
**Definition**

Suppose that $F$ is a field and that $f, g, p \in F[x]$ with $p \neq 0$. Then we say that $f$ is congruent to $g$ modulo $p$ and write $f \equiv g \pmod{p}$ if $p|(f - g)$.

**Example**

In $\mathbb{Q}[x]$, $x^3 + 3x^2 + 4x + 1 \equiv x - 1 \pmod{x^2 + x + 1}$
**Definition**

Suppose that $F$ is a field and that $f, g, p \in F[x]$ with $p \neq 0$. Then we say that $f$ is congruent to $g$ modulo $p$ and write $f \equiv g \pmod{p}$ if $p|(f - g)$.

**Example**

In $\mathbb{Q}[x]$, $x^3 + 3x^2 + 4x + 1 \equiv x - 1 \pmod{x^2 + x + 1}$

**Theorem**

Let $F$ be a field and $0 \neq p \in F[x]$. Then congruence modulo $p$ is an equivalence relation on $F[x]$. 

Kevin James

MTHSC 412 Section 5.1 –Congruence in $F[x]$ and Congruence Classes
**Definition**

Suppose that $F$ is a field and that $f, g, p \in F[x]$ with $p \neq 0$. Then we say that $f$ is congruent to $g$ modulo $p$ and write $f \equiv g \pmod{p}$ if $p|(f - g)$.

**Example**

In $\mathbb{Q}[x]$, $x^3 + 3x^2 + 4x + 1 \equiv x - 1 \pmod{x^2 + x + 1}$

**Theorem**

Let $F$ be a field and $0 \neq p \in F[x]$. Then congruence modulo $p$ is an equivalence relation on $F[x]$.

**Theorem**

Let $F$ be a field and $0 \neq p \in F[x]$. Suppose that $f \equiv g \pmod{p}$ and $h \equiv k \pmod{p}$. Then

$$f + h \equiv g + k \pmod{p} \quad \text{and} \quad fh \equiv gk \pmod{p}.$$
**Definition**

Suppose that $F$ is a field and that $f, p \in F[x]$ with $p \neq 0$. We define the congruence class of $f$ as

$$[f] = \{ g \in F[x] \mid f \equiv g \pmod{p} \}.$$
**Definition**

Suppose that $F$ is a field and that $f, p \in F[x]$ with $p \neq 0$. We define the congruence class of $f$ as

$$[f] = \{ g \in F[x] \mid f \equiv g \pmod{p} \}.$$  

**Theorem**

$f \equiv g \pmod{p}$ if and only if $[f] = [g]$.  

**Corollary**

Two congruence classes modulo $p$ are either identical or disjoint.
**Definition**
Suppose that $F$ is a field and that $f, p \in F[x]$ with $p \neq 0$. We define the congruence class of $f$ as

$$[f] = \{ g \in F[x] \mid f \equiv g \pmod{p} \}.$$ 

**Theorem**
$f \equiv g \pmod{p}$ if and only if $[f] = [g]$.

**Corollary**
Two congruence classes modulo $p$ are either identical or disjoint.
**Corollary**

Suppose that $F$ is a field and that $0 \neq p \in F[x]$. Let

$$S = \{ f \in F[x] : \deg(f) < \deg(p) \} \cup \{0\}.$$ 

Then, $\bigcup_{f \in S} [f] = F[x]$ and if $f, g \in S$ then $[f] = [g]$ if and only if $f = g$. 

Example

Consider congruence modulo $x^2 + 1$ in $\mathbb{R}[x]$. What are the congruence classes. Which one is congruent to $x^2$?

Notation

We denote the set of congruence classes of $F[x]$ modulo $p$ by $F[x]/(p)$. 

Kevin James 

MTHSC 412 Section 5.1 –Congruence in $F[x]$ and Congruence Classes
**Corollary**

Suppose that $F$ is a field and that $0 \neq p \in F[x]$. Let

$$S = \{ f \in F[x] : \deg(f) < \deg(p) \} \cup \{0\}.$$

Then, $\bigcup_{f \in S} [f] = F[x]$ and if $f, g \in S$ then $[f] = [g]$ if and only if $f = g$.

**Example**

Consider congruence modulo $x^2 + 1$ in $\mathbb{R}[x]$. What are the congruence classes. Which one is congruent to $x^2$?
**Corollary**

Suppose that $F$ is a field and that $0 \neq p \in F[x]$. Let

$$S = \{f \in F[x] : \deg(f) < \deg(p)\} \cup \{0\}.$$

Then, $\bigcup_{f \in S} [f] = F[x]$ and if $f, g \in S$ then $[f] = [g]$ if and only if $f = g$.

**Example**

Consider congruence modulo $x^2 + 1$ in $\mathbb{R}[x]$. What are the congruence classes. Which one is congruent to $x^2$?

**Notation**

We denote the set of congruence classes of $F[x]$ modulo $p$ by $F[x]/(p)$. 