Math 521A

5.1 – Congruence in $F[x]$ and Congruence Classes

Throughout this section, F will denote a field.

Definition

Let $f(x), g(x), p(x) \in F[x]$ with $p(x) \neq 0$. Then $f(x)$ is congruent to $g(x)$ modulo $p(x)$ if $p(x)$ divides $f(x) - g(x)$. In symbols,

$$f(x) \equiv g(x) \pmod{p(x)} \iff p(x) \mid f(x) - g(x)$$

Example

In $\mathbb{Q}[x]$, $x^3 \equiv -1 \pmod{x^2 - x + 1}$ because $x^3 + 1 = (x+1)(x^2 - x + 1)$.

Theorem

Let $p(x), f(x), g(x), h(x) \in F[x]$ with $p(x) \neq 0$. Then:

(R) $f(x) \equiv f(x) \pmod{p(x)}$.

(S) $f(x) \equiv g(x) \pmod{p(x)} \Rightarrow g(x) \equiv f(x) \pmod{p(x)}$.

(T) $f(x) \equiv g(x) \pmod{p(x)}$ *and* $g(x) \equiv h(x) \pmod{p(x)} \Rightarrow$
$f(x) \equiv h(x) \pmod{p(x)}$.

Theorem

Let $p(x)$ be a nonzero polynomial in $F[x]$. If $f(x) \equiv g(x) \pmod{p(x)}$ and $h(x) \equiv k(x) \pmod{p(x)}$, then:

1. $f(x) + h(x) \equiv g(x) + k(x) \pmod{p(x)}$.
2. $f(x)h(x) \equiv g(x)k(x) \pmod{p(x)}$.

Definition

The congruence class of $f(x)$ modulo $p(x)$ or residue class of $f(x)$ modulo $p(x)$ is the set

$$\begin{aligned}[f(x)] &= \{g(x) \in F[x] \mid g(x) \equiv f(x) \pmod{p(x)}\} \\ &= \{f(x) + k(x)p(x) \mid k(x) \in F[x]\}.\end{aligned}$$

Example

In $\mathbb{Z}_2[x]$, the congruence class of $x+1$ modulo x^3+x+1 is the set

$$[x+1] = \{(x+1) + k(x)(x^3+x+1) \mid k(x) \in \mathbb{Z}_2[x]\}.$$

Theorem

Let $p(x)$ be a nonzero polynomial in $F[x]$. Then

$$f(x) \equiv g(x) \pmod{p(x)} \iff [f(x)] = [g(x)].$$

Example

Let $p(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$. Show that $[x^5 + x^3] = [x^6 + x]$.

Corollary

Let $p(x)$ be a nonzero polynomial in $F[x]$. Two congruence classes modulo $p(x)$ are either disjoint or identical.

Corollary

Let F be a field and $p(x) \in F[x]$ a polynomial of degree n. Then the set of all congruence classes modulo $p(x)$, denoted by $F[x]/((p(x))$, is equal to

$$\{\,[0]\,\} \cup \{\,[f(x)] \mid \deg f(x) < \deg p(x)\}.$$

Any two elements of $F[x]/((p(x))$ are distinct.

The proof is on the board.

Example

Let $p(x) = x^2 + 1 \in \mathbb{Z}_3[x]$. Then:

$$\frac{\mathbb{Z}_3[x]}{(p(x))} = \{[0], [1], [2], [x], [2x], [x+1], [x+2], [2x+1], [2x+2]\}.$$

Let $p(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$. Then:

$$\frac{\mathbb{Z}_2[x]}{(p(x))} = \{[0], [1], [x], [x+1], [x^2], [x^2+1], [x^2+x], [x^2+x+1]\}.$$