MTHSC 412 Section 5.2 – Congruence Class Arithmetic

Kevin James

Theorem

Suppose that F is a field and that $p \in F[x]$ with $\deg(p) > 0$. If $[f] = [g]$ and $[h] = [k]$ then,

$$[f + h] = [g + k] \qquad \textit{and} \qquad [fh] = [gk].$$

Definition

Suppose that F is a field and that $p \in F[x]$ with $\deg(p) \neq 0$. We define addition and multiplication on $F[x]/(p)$ as follows.

$$[f] + [g] = [f + g] \qquad \text{and} \qquad [f][g] = [fg].$$

Example

Give the addition and multiplication tables for $\mathbb{Z}_2[x]/(x^2 + x + 1)$.

Theorem

Suppose that F is a field and that $p \in F[x]$ with $\deg(p) \neq 0$. Then $F[x]/(p)$ is a commutative ring with identity which contains a subring which is isomorphic to F.

Remark

So, we can think of F as sitting inside the ring $F[x]/(p)$.

Theorem

Suppose that F is a field and that $p \in F[x]$ with $\deg(p) \neq 0$. If $f \in F[x]$ and $(f, p) = 1$ then $[f]$ is a unit in $F[x]/(p)$.