Math 521A

5.2 – Congruence Class Arithmetic

Theorem (Theorem 5.6)

Let F be a field and $p(x)$ a nonconstant polynomial in $F[x]$. If

$$[f(x)] = [h(x)] \quad \textit{and} \quad [g(x)] = [k(x)]$$

then

$$[f(x) + g(x)] = [h(x) + k(x)] \quad \textit{and} \quad [f(x)g(x)] = [h(x)k(x)]$$

Important consequence of Theorem 5.6: The result of "adding" or "multiplying" two congruence classes is independent of the choice of the representatives of the classes, which motivates the following:

Definition

Let F be a field and $p(x)$ a nonconstant polynomial in $F[x]$. Addition and multiplication in $F[x]/(p(x))$ are defined by

$$\begin{aligned} [f(x)] + [g(x)] &= [f(x) + g(x)] \\ [f(x)][g(x)] &= [f(x)g(x)] \end{aligned}$$

Example

(a) Calculate $[f(x)] + [g(x)]$ and $[f(x)][g(x)]$ in $\frac{\mathbb{Z}_2[x]}{(x^3+x+1)}$ when $f(x) = x^2 + x + 1$ and $g(x) = x$.

(b) Calculate $[f(x)] + [g(x)]$ and $[f(x)][g(x)]$ in $\frac{\mathbb{Q}[x]}{(x^2-3)}$ when $f(x) = x + 1$ and $g(x) = x + \frac{1}{2}$.

- It is possible to show that if $p(x) \in F[x]$ is nonconstant then $F[x]/(p(x))$ *forms a commutative ring with identity*:

$$\begin{aligned} [0] &= \text{additive identity} \\ [1] &= \text{multiplicative identity} \end{aligned}$$

  Moreover, $F[x]/(p(x))$ *always contains* F *as a subring*: Any two constant polynomials are in different classes. These statements are essentially Theorems 5.7 and 5.8.
- When the context is clear, we can drop the brackets from $[f(x)]$.
- We will work out several examples of computations in the ring $\frac{\mathbb{Z}_2[x]}{(x^3+x+1)}$ on the board.

Recall: $a \in \mathbb{Z}_n$ is a unit if $\exists\ x \in \mathbb{Z}_n$ such that $ax = 1$ in $\mathbb{Z}_n$. The condition for this to happen is $\gcd(a, n) = 1$. We have a similar result in $F[x]/(p(x))$:

Theorem (Theorem 5.9)

Let F be a field and $p(x)$ a nonconstant polynomial in $F[x]$. Then:

$$f(x) \text{ is a unit in } F[x]/(p(x)) \iff \gcd(f(x), p(x)) = 1.$$

Example

(a) $p(x) = x^3 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$, so $f(x) = x^2 + x + 1$ is relatively prime to $p(x)$ in $\mathbb{Z}_2[x]$. What is the multiplicative inverse of $f(x)$ in $\mathbb{Z}_2[x]/(p(x))$? Repeat the exercise now considering $p(x) = x^4 + x + 1$ and $f(x) = x^3 + x + 1$.

(b) Let $p(x) = x^2 - 5x + 6$ in $\mathbb{Q}[x]$. Determine whether $f(x) = (x - 5)$ is a unit in $R = \mathbb{Q}[x]/(p(x))$. If so, find $g(x)$ such that $f(x)g(x) = 1$ in R.