Representation:

$$P(x) = 5x^3 + 2x^2 + 1 \rightarrow P(x) = \sum_{i=0}^{n} p_i x^i$$

So we can represent a polynomial with n+1 coefficients

$$\cancel{[p_0, p]} \; [p_0, p_1, p_2, p_3 \cdots p_n]$$

For example the above poly can be written as $[1, 0, 2, 5]$

Fields and Rings

To make sure our computation is always bounded ~~.....~~ the kyber system constrains the system with two more algebraic structures

→ First, numbers in kyber are defined in the finite field

$GF(q) = \mathbb{Z}/q\mathbb{Z}$, here $\mathbb{Z}$ is a set of all integers.

q is a prime

→ The field only contains integers

→ every operation to a number or polynomial coefficient will take a modulo q in the end.

→ ~~ploy~~ polynomials in kyber are defined in another special structure called ring

$$R = GF(q)[x] / X^n + 1$$

every polynomial operation will take modulo $x^n + 1$ in the end

However since our modulus is $x^n + 1$ then $x^n = -1$ we can replace x^n with -1 in the target poly

Polynomial operations

Addition: Simply add each coefficient together modulo q

$$P(x) + Q(x) = \sum_{i=0}^{n} (p_0 + q_0 \bmod q) x^i$$

Subtraction: Subtracting $Q(x)$ from $P(x)$ is equivalent to inverting polynomial $Q(x)$. take modulo q to obtain non-negative numbers and do the addition from above

$$P(x) - Q(x) = \sum_{i=0}^{n} (p_0 - q_0 \bmod q) x^i$$

Multiplication: $P(x)$ and $Q(x)$ multiply every component $p_i x^i$ in $P(x)$ with ~~q~~ $Q(x)$ and sum them up in the end. For the final result we need to take modulo q for all the coefficient ~~&~~ and also need to take modulo $F(x) = x^n + 1$ so that we obtain a polynomial such that we obtain a result with degree $n-1$