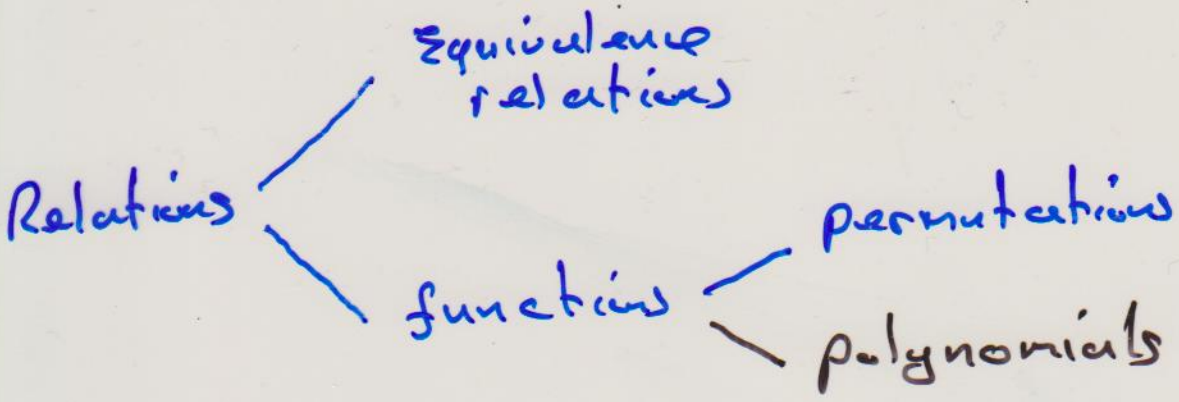
Summary



Polynomials

Expressions such as

$$a(x) = x^4 + 6x + 1$$

$$b(x) = x^2 + x - 4$$

are called polynomials. Such expressions can be viewed as functions, say

$$a : \mathbb{Z} \longrightarrow \mathbb{Z}, \quad x \longmapsto x^4 + 6x + 1.$$

So $a(2) = 2^4 + 6.2 + 1 = 29$

In this course we are more interested in

adding

$$a(x) + b(x) = x^4 + x^2 + 7x - 3$$

subtracting

$$a(x) - b(x) = x^4 - x^2 + 5x + 5$$

multiplying

$$a(x)\,b(x) = x^6 + x^5 - 4x^4 + 6x^3 + 7x^2 - 23x - 4$$

dividing

$b(x)$ divided into $a(x)$

$$\begin{array}{r} x^2 - x + 5 \\ x^2 + x - 4 \overline{)\, x^4 + 6x + 1} \\ \underline{x^4 + x^3 - 4x^2} \\ -x^3 + 4x^2 + 6x + 1 \\ \underline{-x^3 - x^2 + 4x} \\ 5x^2 + 2x + 1 \\ \underline{5x^2 + 5x - 20} \\ -3x + 21 \end{array}$$

This means $b(x)$ goes into $a(x)$

$x^2 - x + 5$ times, with remainder $-3x + 21$

Alternatively

$$a(x) = (x^2 - x + 5)\, b(x) + (-3x + 21)$$

All of the above calculations we performed over the integers, $\mathbb{Z}$. We let

$$\mathbb{Z}[x]$$

denote the set of all polynomials with integer coefficients. We let $\mathbb{Z}_5[x]$ denote the set of all polynomials with coefficients modulo 5.

Again

$$a(x) = x^4 + x + 1 \quad \in \mathbb{Z}_5[x]$$

$$b(x) = x^2 + x + 1 \quad \in \mathbb{Z}_5[x]$$

$$a(x) + b(x) = x^4 + x^2 + 2x + 2$$

$$a(x)\, b(x) = x^6 + x^5 + x^4 + x^3 + 2x^2 + 2x + 1$$

Let's divide $b(x)$ into $a(x)$ working mod 5

$$
\begin{array}{r}
x^2 - x \\
x^2+x+1 \;\overline{)\; x^4 + x + 1} \\
\underline{x^4 + x^3 + x^2} \\
-x^3 - x^2 + x + 1 \\
\underline{-x^3 - x^2 - x} \\
2x + 1
\end{array}
$$

So

$$a(x) = (x^2 - x)\, b(x) + (2x + 1)$$

FACT This division algorithm will always work over $\mathbb{Z}_p[x]$ when p is prime.