

Principal ideals, cosets and congruence in a polynomial ring

$$x^2 - 2 \in \mathbb{Q}[x]$$

$I = (x^2 - 2) = \{(x^2 - 2)p(x) \mid p(x) \in \mathbb{Q}[x]\}$
is a principal ideal in $\mathbb{Q}[x]$

$cR = \{cr \mid r \in R\}$ is a **principal ideal** of R

Congruence classes are cosets of I :

$$[2x+1] = 2x+1+I = \{2x+1+(x^2-2)p(x) \mid p(x) \in \mathbb{Q}[x]\}$$

$a+I = \{a+i \mid i \in I\}$ is a **coset**
(also called equivalence class)

Polynomials are congruent if:

$$f(x), g(x) \in \mathbb{Q}[x]$$

$$g(x) - f(x) \in I = (x^2 - 2)$$

$$g(x) - f(x) = (x^2 - 2)p(x)$$

$$x^2 - 2 \mid g(x) - f(x)$$

a is congruent to b modulo I if
 $b + (-a) \in I$. We write $a \equiv b \pmod{I}$

The equivalence classes form a ring:

$$\begin{aligned} \mathbb{Q}[x]/(x^2 - 2) &= \{f(x) + I \mid f(x) \in \mathbb{Q}[x]\} \\ &= \{[f(x)] \mid f(x) \in \mathbb{Q}[x]\} \end{aligned}$$

The quotient ring of R mod I is
 $R/I = \{a+I \mid a \in R\}$