Buď R okruh, $a, b, \ldots \in R$.

<u>def</u>: $a \mid b$ v okruhu R $\iff$ $\exists c \in R \quad b = ac$

$a \parallel b$ v okruhu R $\iff$ $a \mid b, \; b \mid a$

"<u>asociované</u> prvky"

<u>Tvrzení</u>: $a \parallel b$ v R $\iff$ $\exists q \in R^* \quad b = aq$

<u>def</u>: $c = NSD_R(a, b)$ $\iff$ (1) $c \mid a, \; c \mid b$ v R

(2) $d \mid a, \; d \mid b$ v R $\Rightarrow$ $d \mid c$ v R

a, b <u>nesoudělné</u> v R $\iff$ $1 = NSD_R(a, b)$

Navíc def. $NSD_R(0, 0) = 0$.

def: b je <u>vlastní dělitel</u> a $\iff$ $b \mid a$, $b \nparallel 1$, $b \nparallel a$

def: a je <u>ireducibilní</u> v R $\iff$ $a \neq 0$, $a \nparallel 1$, $\boxed{\text{a nemá vlastní dělitele}}$

tj., $b \mid a \Rightarrow b \parallel 1$ nebo $b \parallel a$

tj., $a = bc \Rightarrow b \parallel 1$ nebo $c \parallel 1$

def: <u>ireducibilní rozklad</u> prvku a je zápis

$a \parallel p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ kde $p_1, \dots, p_n$ jsou ireducibilní prvky, $p_i \nparallel p_j$ $\forall i \neq j$, $k_1, \dots, k_n \in \mathbb{N}$

Řekneme, že a má <u>jednoznačný ireducibilní rozklad</u>, pokud má právě jeden rozklad až na pořadí a asociovanost,

tj. $a \parallel p_1^{k_1} \cdots p_n^{k_n} \parallel q_1^{l_1} \cdots q_m^{l_m}$ dva rozklady

$\Rightarrow$ $m = n$ & existuje permutace π indexů t.ž. $\forall i$ $p_i \parallel q_{\pi(i)}$, $k_i = l_{\pi(i)}$

def: p je <u>prvočinitel</u> v R $\iff$ $p \neq 0$, $p \nparallel 1$, $\boxed{p \mid a \cdot b \Rightarrow p \mid a \text{ nebo } p \mid b}$