Buď R komutativní okruh, $a, b \in R$.

def: $a \mid b$ v R pokud $\exists c \in R \; b = a \cdot c$

$a \parallel b$ v R pokud $a \mid b$ & $b \mid a$ v R

$a \parallel 1 \iff a \in R^*$

Tvrzení: Buď R obor. Pak $a \parallel b$ v $R \iff \exists q \in R^* \; b = a \cdot q$

$\mid$ je kvaziuspořádání, $\parallel$ je ekvivalence

$a \equiv b \pmod{m}$ v $R \iff m \mid a - b$ v R $\quad (m \neq 0)$

je to ekvivalence, invariantní vzhledem k $+, -, \cdot$

Buď R komutativní okruh, $a, b, c \in R$.

def: Řekneme, že $NSD(a,b) = c$ v R pokud (1) $c \mid a$, $c \mid b$

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

Definujeme $NSD(0,0) = 0$.

Prvky a, b jsou nesoudělné, pokud $NSD(a,b) = 1$.

Pozor! NSD není funkce dvou proměnných.
Je to ternární relace, více c může splňovat definici.

$NSD(a,b) = c_1$, $NSD(a,b) = c_2 \Rightarrow c_1 \parallel c_2$

Pozor! Takové c nemusí existovat žádné.

Buď R obor, $p \in R$.

def.: Prvek p nazveme ireducibilní v R, pokud

$$\underbrace{p \neq 0,\ p \nparallel 1}_{\text{(NEZAPOMÍNEJ)}} \quad \& \quad \underbrace{p \text{ nemá vlastní dělitele.}}_{\text{tj., } a \mid p \Rightarrow a \parallel p \text{ nebo } a \parallel 1}$$

def: Ireducibilní rozklad prvku a v oboru R je zápis

$a \parallel p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$ kde $p_1, \ldots, p_n$ jsou ireducibilní prvky R, $p_i \nparallel p_j$, a $k_1, \ldots, k_n \in \mathbb{N}$.

Řekneme, že prvek a má jednoznačný ireducibilní rozklad, pokud kdykoliv $a \parallel p_1^{k_1} \cdots p_n^{k_n} \parallel q_1^{l_1} \cdots q_m^{l_m}$, pak

$m = n$ & $\exists$ permutace π t.ž. $q_i \parallel p_{\pi(i)}$, $k_i = l_{\pi(i)}$.

Created by Notein

Buď R obor, $p \in R$.

def.: Prvek p nazveme <u>ireducibilní</u> v R, pokud

$$p \neq 0,\ p \nparallel 1 \quad \& \quad \boxed{p = a \cdot b \implies p \parallel a \text{ nebo } p \parallel b}$$

tj. p nemá vlastní dělitele

def.: Prvek p nazveme <u>prvočinitel</u> v R, pokud

$$p \neq 0,\ p \nparallel 1 \quad \& \quad \boxed{p \mid a \cdot b \implies p \mid a \text{ nebo } p \mid b}$$

prvočinitelé jsou ireducibilní

! NAOPAK <u>NE</u>, jen v některých oborech def: Ireducibilní rozklad prvku a v oboru R je zápis

$a \parallel p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$ kde $p_1, \ldots, p_n$ jsou ireducibilní prvky R, $p_i \nparallel p_j$, a $k_1, \ldots, k_n \in \mathbb{N}$.

Řekneme, že prvek a má jednoznačný ireducibilní rozklad, pokud kdykoliv $a \parallel p_1^{k_1} \cdots p_n^{k_n} \parallel q_1^{l_1} \cdots q_m^{l_m}$, pak $m = n$ & $\exists$ permutace π t.ž. $q_i \parallel p_{\pi(i)}$, $k_i = l_{\pi(i)}$.

def: Obor R nazýváme $\boxed{\text{gaussovský}}$ pokud má každý prvek $a \neq 0$, $a \nparallel 1$ jednoznačný ireducibilní rozklad.

Tvrzení: Buď R gaussovský obor, $a, b \in R$, $a \neq 0$, $a \nparallel 1$.

Uvažujme ireducibilní rozklad $a \parallel p_1^{k_1} \dots p_n^{k_n}$.

Pak $b \mid a \iff b \parallel p_1^{l_1} \dots p_n^{l_n}$ pro nějaká $0 \leq l_i \leq k_i$

Důsledky: V gaussovských oborech

(1) $\forall a, b \; \exists c \; NSD(a, b) = c$

(2) ireducibilní prvky jsou prvočinitelé

(3) neexistuje posloupnost $a_1, a_2, a_3, \dots$ t.ž. $a_{i+1} \mid a_i$, $a_{i+1} \nparallel a_i$

Pozn.: Bézoutova rovnost v gauss. oborech platit nemusí.

Tvrzení: Buď R gaussovský obor, $a, b \in R$, $a \neq 0$, $a \not\| 1$.

Uvažujme ireducibilní rozklad $a \| p_1^{k_1} \cdots p_n^{k_n}$.

Pak $b | a \iff b \| p_1^{l_1} \cdots p_n^{l_n}$ pro nějaká $0 \leq l_i \leq k_i$

Důsledky: V gaussovských oborech

(1) $\forall a, b \; \exists c \; NSD(a,b) = c$

(2) ireducibilní prvky jsou prvočinitelé

(3) neexistuje posloupnost $a_1, a_2, a_3, \dots$ t.ž. $a_{i+1} | a_i$, $a_{i+1} \not\| a_i$

Věta: Obor R je gaussovský $\iff$ v oboru R platí

(1) $\forall a, b \; \exists c \; NSD(a,b) = c$

(2) neexistuje posloupnost $a_1, a_2, a_3, \dots$ t.ž. $a_{i+1} | a_i$, $a_{i+1} \not\| a_i$