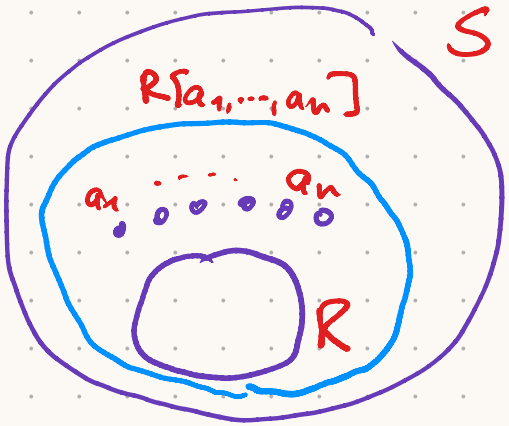
Buď $R \leq S$ komutativní okruhy, $a_1, \dots, a_n \in S$.



Definujeme

$R[a_1, \dots, a_n]$:= nejmenší podokruh S obsahující $R \cup \{a_1, \dots, a_n\}$

$R(a_1, \dots, a_n)$:= nejmenší podtěleso S obsahující $R \cup \{a_1, \dots, a_n\}$

Mluvíme o okruhovém, resp. tělesovém, rozšíření oboru R.

Tvrzení: Za těchto předpokladů

$$R[a] = \{ f(a) : f \in R[x] \} = \{ r_0 + r_1 a + \dots + r_n a^n : n \in \mathbb{N}_0, r_i \in R \}$$
$$R(a) = \{ f(a) g(a)^{-1} : f, g \in R[x], g(a) \neq 0 \}$$

Respektive $R[a_1, \dots, a_n] = \{ f(a_1, \dots, a_n) : f \in R[x_1, \dots, x_n] \}$

$R(a_1, \dots, a_n) = \{ f(\bar{a}) \cdot g(\bar{a})^{-1} : f, g \in R[x_1, \dots, x_n], g(\bar{a}) \neq 0 \}$

KVADRATICKÁ ROZŠÍŘENÍ $\mathbb{Z}[\sqrt{s}]$: $s \in \mathbb{Z}$, $p^2 \nmid s$ $\forall p$ prvoč.

def.: $u \mid v$ pokud $\exists q \in \mathbb{Z}[\sqrt{s}]$ t.ž. $v = u \cdot q$

def.: **norma** $\nu : \mathbb{Z}[\sqrt{s}] \to \mathbb{N}_0$

$a + b\sqrt{s} \mapsto \boxed{|a^2 - b^2 s|}$

$s < 0 \Rightarrow \nu(u) = \underbrace{|u|^2}$ abs. hodnota v $\mathbb{C}$

Tvrzení: $\forall u, v \in \mathbb{Z}[\sqrt{s}]$

(1) $\nu(u \cdot v) = \nu(u) \cdot \nu(v)$

(2) $\nu(u) = 1 \iff u$ je invertibilní

(3) $u \mid v \Rightarrow \nu(u) \leq \nu(v)$

$u \mid v$, $v \nmid u \Rightarrow \nu(u) < \nu(v)$ $\quad (v \neq 0)$

Dělení se zbytkem: dáno $u, v \in \mathbb{Z}[\sqrt{s}]$, $v \neq 0$

chci $q, r \in \mathbb{Z}[\sqrt{s}]$ t.ž. $\boxed{u = v \cdot q + r}$ & $\boxed{\nu(r) < \nu(v)}$

Tvrzení: V oboru $\mathbb{Z}[\sqrt{s}]$ lze dělit se zbytkem.

(ale podíl a zbytek není jednoznačně určen)