4 Kvadratická rozšíření ob(z)orů

Řešení
Verze ze dne 13. března 2025

Cíle cvičení: Dnes se pustíme do dělení a rozkladů v kvadratických rozšířeních celých čísel. U některých z nich budeme umět s využitím normy dokonce dělit se zbytkem a počítat největší společné dělitele.

Úlohy, které bychom určitě měli umět řešit:

Úloha 4.1. Vydělte se zbytkem číslo α číslem β

(a) v oboru $\mathbb{Z}[i]$, jestliže $\alpha = 5+7i$, $\beta = 3-i$ (nalezněte alespoň dva různé výsledky),

(b) v oboru $\mathbb{Z}[i]$, jestliže $\alpha = 3+2i$, $\beta = 1+i$,

(c) v oboru $\mathbb{Z}[\sqrt{2}i]$, jestliže $\alpha = 4$, $\beta = 1-\sqrt{2}i$,

(d) v oboru $\mathbb{Z}[\sqrt{2}i]$, jestliže $\alpha = 1+4\sqrt{2}i$, $\beta = 3+\sqrt{2}i$

Řešení. (a) Nejprve v komplexních číslech spočítáme „přesný“ podíl

$$\frac{\alpha}{\beta} = \frac{5+7i}{3-i} = \frac{(5+7i)\cdot(3+i)}{(3-i)\cdot(3+i)} = \frac{8+26i}{10} = \frac{4}{5}+\frac{13}{5}i.$$

Nyní budeme hodnotu $\frac{4}{5}+\frac{13}{5}i$ aproximovat Gaussovým celým číslem γ; přičemž platí, že pokud dostaneme $|\gamma - \frac{\alpha}{\beta}|^2 < 1$, bude mít zbytek $\gamma\cdot\beta-\alpha$ menší normu než norma $\nu(\beta) = 3^2+1^2 = 10$ dělitele $\beta = 3-i$. Dostáváme tak tři možné výsledky:

$\alpha = (1+3i)\cdot\beta + (-1-i)$ pro volbu aproximace $\gamma = 1+3i$ (kde $\nu(-1-i) = 2 < 10$),

$\alpha = (1+2i)\cdot\beta + (2i)$ pro volbu $\gamma = 1+2i$ (kde $\nu(2i) = 4 < 10$) a

$\alpha = 3i\cdot\beta + (2-2i)$ pro volbu $\gamma = 3i$ (kde $\nu(2-2i) = 8 < 10$).

(b) Stejně jako v (a) aproximujeme podíl $\frac{\alpha}{\beta} = \frac{3+2i}{1+i} = \frac{1}{2}-\frac{5}{2}i$ a dostaneme tentokrát dokonce 4 možné výsledky: $3+2i = 2\cdot\beta+1 = 3\cdot\beta+(-i) = (2-i)\cdot\beta+i = (3-i)\cdot\beta-1$, pro které je norma zbytku menší než norma $\nu(\beta) = 1^2+1^2 = 2$ dělitele $\beta = 1+i$.

(c) Postupujeme podobně jako v předchozí úloze, tedy budeme aproximovat podíl v komplexním oboru pomocí prvku oboru $\mathbb{Z}[\sqrt{-2}]$ s použitím normy $\nu(a+b\sqrt{2}) = |a^2+2b^2| = a^2+2b^2$. Nejprve spočítáme podíl

$$\frac{4}{1-\sqrt{2}i} = \frac{4\cdot(1+\sqrt{2}i)}{(1-\sqrt{2}i)\cdot(1+\sqrt{2}i)} = \frac{4+4\sqrt{2}i}{1^2+2\cdot 1^2} = \frac{4}{3}+\frac{4}{3}\sqrt{2}i.$$

Oba koeficienty $\frac{4}{3}$ aproximujeme nejbližší hodnotou 1 a dostáváme podíl $1+\sqrt{2}i$ a zbytek $1 = 4-(1+\sqrt{2}i)\cdot(1+\sqrt{2}i)$. Spočítali jsme, že $4 = (1+\sqrt{2}i)(1-\sqrt{2}i)+1$ a vidíme, že $\nu(1) = 1 < \nu(1-\sqrt{2}i) = 1^2+2\cdot 1^2 = 3$.

(d) Opět spočteme podíl

$$\frac{1+4\sqrt{2}i}{3+\sqrt{2}i} = \frac{(1+4\sqrt{2}i)\cdot(3-\sqrt{2}i)}{(3+\sqrt{2}i)\cdot(3-\sqrt{2}i)} = \frac{(1+4\sqrt{2}i)\cdot(3-\sqrt{2}i)}{3^2+2\cdot 1^2} = \frac{11-11\sqrt{2}i}{11} = 1+\sqrt{2}i.$$

Protože tato hodnota už leží v $\mathbb{Z}[\sqrt{2}i]$, je zbytek nulový a platí, že $(1+4\sqrt{2}i) = (3+\sqrt{2}i)\cdot(1+\sqrt{2}i)$.

Úloha 4.2. Najděte největší společné dělitele

(a) $\mathrm{NSD}(3+i, 4+2i)$ v oboru $\mathbb{Z}[i]$,

(b) $\mathrm{NSD}(3+4i, 7+2i)$ v oboru $\mathbb{Z}[i]$,

(c) $\mathrm{NSD}(6-3\sqrt{3}, 3+\sqrt{3})$ v oboru $\mathbb{Z}[\sqrt{3}]$.

Řešení. Postupujeme standardně pomocí Eukleidova algoritmu a počítáme zbytky po dělení.

(a) Zvolíme počáteční hodnoty $a_0 = 4+2i$, $a_1 = 3+i$ a poté spočítáme $\frac{4+2i}{3+i} = \frac{14}{10} - \frac{2}{10}i$. Nyní zvolíme nejbližší Gaussovo celé číslo 1 a spočítáme zbytek $a_2 = 4+2i-1(3+i) = 1+i$.

Opět dělíme $\frac{3+i}{1+i} = 2-i \in \mathbb{Z}[i]$, tedy zbytek $a_3 = 0$ a $\mathrm{NSD}(3+i, 4+2i) = a_2 = 1+i$.

(b) I tentokrát bychom mohli postupovat Eukleidovým algoritmem, ale zvolíme efektivnější přístup. Připomeneme si důležitou vlastnost normy ν na kvadratických rozšířeních celých čísel, totiž že zachovává násobení: $\nu(a \cdot b) = \nu(a) \cdot \nu(b)$. To ovšem znamená, že pro každý dělitel $c \mid a$ v kvadratickém rozšíření platí, že $\nu(c) \mid \nu(a)$, speciálně $\nu(\mathrm{NSD}(a,b)) \mid \mathrm{NSD}(\nu(a), \nu(b))$.

V našem případě snadno spočítáme, že $\nu(3+4i) = 3^2+4^2 = 25$, a $\nu(7+2i) = 7^2+2^2 = 53$, a protože $\mathrm{NSD}(25, 53) = 1$, nutně platí, že $\mathrm{NSD}(3+4i, 7+2i) = 1$.

(c) I tentokrát využijeme úvahu z (b), jen tentokrát pracujeme s odlišnou normou $\nu(a+b\sqrt{3}) = |a^2-3b^2|$. Sice spočítáme, že $\nu(6-3\sqrt{3}) = |6^2-3\cdot 3^2| = 9$, a $\nu(3+\sqrt{3}) = |9^2-3\cdot 1^2| = 6$, což není nesoudělné, ale případný netriviální největší společný dělitel musí mít normu 3. Snadno ověříme, že prvek $\sqrt{3}$ normy 3 je opravdu společný dělitel, protože

$$6-3\sqrt{3} = \sqrt{3}(-3+2\sqrt{3}), \quad 3+\sqrt{3} = \sqrt{3}(1+3+\sqrt{3}).$$

Tudíž $\sqrt{3} = \mathrm{NSD}(6-3\sqrt{3}, 3+\sqrt{3})$ v $\mathbb{Z}[\sqrt{3}]$.

Úloha 4.3. Spočítejte ireducibilní rozklady prvků

(a) 3, 5, 6, $10-6i$ v $\mathbb{Z}[i]$,

(b) 2, 3 v $\mathbb{Z}[\sqrt{2}i]$.

Řešení. Nejprve si všimněme, že je norma na kvadratických rozšířeních celých čísel celočíselná, zachovává násobení a normu 1 mají právě invertibilní prvky, proto je prvek s prvočíselnou normou už nutně ireducibilní.

(a) Na oboru $\mathbb{Z}[i]$ máme normu $\nu(a+bi) = a^2+b^2$. Protože $\nu(3) = 9$, netriviální dělitel by musel mít normu 3. Ovšem podmínka $a^2+b^2 \leq 3$ pro celá a, b, znamená, že $|a|, |b| \leq 1$, tudíž snadnou diskusí dostáváme $a^2+b^2 \in \{0,1,2\}$. To znamená, že normu 3 nemá v $\mathbb{Z}[i]$ žádný netriviální dělitel, a proto je to ireducibilní prvek.

Protože $\nu(5) = 25$, musí mít netriviální dělitel normu 5, tentokrát ovšem (například) probráním prvků $a+bi$ splňujících $|a|, |b| \leq 2$ dostáváme ireducibilní rozklad $5 = (1+2i)(1-2i)$, kde oba faktory už mají prvočíselnou normu. Můžeme si navíc i všimnout, že Eukleidův algoritmus nám zjistí, že $\mathrm{NSD}(1+2i, 1-2i) = 1$, tedy se jedná o neasociované ireducibilní prvky.

$6 = 2\cdot 3$ v $\mathbb{Z}$ i v $\mathbb{Z}[i]$, o prvku 3 už víme, že je v $\mathbb{Z}[i]$ ireducibilní a snadno nahlédneme, že $2 = (1+i)(1-i)$ je ireducibilní rozklad s faktory normy 2 (tentokrát si můžeme povšimnout, že $1+i = i(1-i)$, tedy jde o asociované ireducibilní prvky). Našli jsme ireducibilní faktorizaci $6 = 3(1+i)(1-i)$.

Pro počítání ireducibilního rozkladu prvku $10-6i$ vidíme, že můžeme vytknout hodnotu 2, kterou už umíme ireducibilně rozložit. Zbývá rozklad prvku $5-3i$ normy $34 = 2\cdot 17$. Stačí nám tedy otestovat, zda nějaký prvek normy 2 dělí $5-3i$ a spočítat například, že $\frac{5-3i}{1+i} = 1-4i$. Protože $\nu(1-4i) = 17$, jedná se o ireducibilní prvek a my jsme získali ireducibilní rozklad

$$10-6i = 2\cdot(5-3i) = (1+i)(1-i)(1+i)(1-4i) = -(1+i)^3(4+i)$$

(b) Tentokrát pracujeme s normou $\nu(a+b\sqrt{2}i) = a^2+2b^2$. Norma čísla 2 je v oboru $\mathbb{Z}[\sqrt{2}i]$ rovna $\nu(2) = 4$, proto jediný možný netriviální dělitel musí mít normu 2, tedy prvek $\pm i\sqrt{2}$, snadno si rozmyslíme, že $2 = -(i\sqrt{2})^2$ je tudíž ireducibilní rozklad.

Protože $\nu(3) = 3^2 = 9$, hledáme případné ireducibilní faktory mezi prvky normy 3. Opět tedy snadno najdeme ireducibilní rozklad $3 = (1 + i\sqrt{2})(1 - i\sqrt{2})$.

Úloha 4.4. Vysvětlete následující „rozpor“:

- V oboru $\mathbb{Z}[\sqrt{3}i]$ platí $(-2)2 = (i\sqrt{3} + 1)(i\sqrt{3} - 1)$, a proto se nejedná o obor s jednoznačným rozkladem (tj. Gaussův obor).
- V oboru $\mathbb{Z}[\sqrt{2}]$ platí $\sqrt{2}\sqrt{2} = (-4 + 3\sqrt{2})(4 + 3\sqrt{2})$, a přesto se jedná o obor s jednoznačným rozkladem.

Řešení. V prvním případě snadno spočítáme, že podíly $\frac{\pm 2}{i\sqrt{3}\pm 1}, \frac{i\sqrt{3}\pm 1}{\pm 2}$ neleží v $\mathbb{Z}[i\sqrt{3}]$, proto prvky ± 2 a $i\sqrt{3} \pm 1$ nejsou asociované, podmínka jednoznačnosti ireducibilních rozkladů tak není splněna.

Obor $\mathbb{Z}[\sqrt{2}]$ je eukleidovský, protože v něm máme k dispozici algoritmus dělení se zbytkem snižující normu zbytku, a tudíž je podle věty z přednášky i Gaussův. V uvedeném případě si všimneme, že $(\pm 4 + 3\sqrt{2}) = \sqrt{2}(3 \pm 2\sqrt{2})$, přičemž $3 \pm 2\sqrt{2}$ jsou zde invertibilní (mají normu 1), tudíž $(\pm 4 + 3\sqrt{2}) \parallel (\pm\sqrt{2})$ a žádný rozpor jsme tak neobdrželi.

Úloha 4.5. Ukažte na příkladu, že standardní norma na okruhu $\mathbb{Z}[\sqrt{7}i]$ není eukleidovská. (Nápověda: Vyjděte z toho, že obor $\mathbb{Z}[\sqrt{7}i]$ není ani Gaussův – najděte podobnou situaci, jako v předchozí úloze u $\mathbb{Z}[\sqrt{3}i]$.)

Řešení. Uvedený obor není ani Gaussův, jak dosvědčuje dvojí rozklad

$$2 \cdot 2 \cdot 2 = (1 + \sqrt{7}i)(1 - \sqrt{7}i),$$

přičemž uvedené prvky s normami 4, resp. 8 jsou ireducibilní z toho důvodu, že se v $\mathbb{Z}[\sqrt{7}i]$ nenachází prvek řádu 2, jak ukáže snadný rozbor. Pro konkrétní příklad toho, že nelze dělit se zbytkem, uvažme dělení $1 + \sqrt{7}i$ prvkem 2, tj. měly by existovat $q, r \in \mathbb{Z}[\sqrt{7}i]$ splňující $1 + \sqrt{7}i = 2q + r$ a $\nu(r) < \nu(2) = 4$. Vzhledem k neexistenci prvků norem 2 a 3 ovšem musí nutně mít r normu 1, tedy musí jít o ± 1. Ani jeden z prvků $1 + \sqrt{7}i \pm 1$ ale není dělitelný dvěma v $\mathbb{Z}[\sqrt{7}i]$.

A teď něco na konec cvičení a následnou afterparty:

Úloha 4.6. Vysvětlete, proč například pro prvky $\sqrt{5} + 1$ a 2 v oboru $\mathbb{Z}[\sqrt{5}]$ Eukleidův algoritmus selže. Jak dopadne Eukleidův algoritmus v témže oboru pro prvky $1 - 2\sqrt{5}$ a 2?

Řešení. Pokud – stejně jako jsme to dělali v úloze 4.2 – vydělíme v tělese komplexních čísel $\frac{\sqrt{5}+1}{2} = \frac{1}{2}\sqrt{5} + \frac{1}{2}$, dostáváme možné aproximace 0, 1, $\sqrt{5}$, $\sqrt{5}+1$ a odpovídající zbytky $\sqrt{5}+1$, $\sqrt{5}-1$, $1-\sqrt{5}$, $-1-\sqrt{5}$, tedy s prvky stejné normy, jakou měl prvek 2. Po snadné diskusi zjistíme, že se nám aproximací nikdy nepodaří snížit normu zbytku, tedy aplikací Eukleidova algoritmu nikdy nedostaneme zbytek 0. Nicméně je možné si rozmyslet, že uvedené dva prvky mají největšího společného dělitele 1 – díky neexistenci prvku normy 2 v $\mathbb{Z}[\sqrt{5}]$ jde o ireducibilní prvky, které navíc nejsou asociované, tedy jsou nesoudělné.

Když prvky $1 - 2\sqrt{5}$ a 2 vydělíme $\frac{1-2\sqrt{5}}{2} = \frac{1}{2} - \sqrt{5}$ a aproximujeme podíl prvkem $-\sqrt{5}$, dostaneme zbytek $1 = 1 - 2\sqrt{5} - 2 \cdot (-\sqrt{5})$, který už dělí číslo 2, takže Eukleidův algoritmus skončí a dá správný výsledek, třebaže obor $\mathbb{Z}[\sqrt{5}]$ není Gaussův a proto ani eukleidovský.

Úloha 4.7. Spočítejte

(a) ireducibilní rozklady prvků 7, $9 + 3i$ v oboru $\mathbb{Z}[i]$,

(b) $\mathrm{NSD}(3 + 6i, 12 - 3i)$, $\mathrm{NSD}(5 + 3i, 13 + 18i)$ v oboru $\mathbb{Z}[i]$,

(c) ireducibilní rozklady prvků $3 - i\sqrt{2}$ a $5 - i\sqrt{2}$ v oboru $\mathbb{Z}[i\sqrt{2}]$,

(d) ireducibilní rozklady prvku $3 + \sqrt{2}$ a $3 - 8\sqrt{2}$ v oboru $\mathbb{Z}[\sqrt{2}]$.

Řešení. (a) 7 má normu 49, ovšem žádné Gaussovo celé číslo s normou 7 neexistuje, muselo by být tvaru $a + bi$ pro $|a|, |b| \leq 2$, ale normy takových čísel leží v množině $\{0, 1, 2, 5, 8\}$. Tedy 7 je v $\mathbb{Z}[i]$ ireducibilní.

Nyní si rozmyslíme, že $9 + 3i = 3(3 + i)$, kde o číslu 3 víme z 4.3, že je v $\mathbb{Z}[i]$ ireducibilní. Zbývá rozložit číslo $(3+i)$ normy $3^2+1^2 = 10$. Protože $\nu(1+i) = 2$ a snadno spočítáme $\frac{3+i}{1+i} = 2-i \in \mathbb{Z}[i]$, kde $\nu(2-i) = 5$ je prvočíslo, dostáváme ireducibilní rozklady $3 + i = (1 + i)(2 - i)$ a $9 + 3i = 3(1 + i)(2 - i)$.

(b) Postupujeme jako v 4.2. Vidíme, že 3 je společný dělitel prvků $3+6i = 3\cdot(1+2i)$ a $12-3i = 3\cdot(4-i)$. Protože jsou normy $\nu(1 + 2i) = 5$ a $\nu(4 - i) = 17$ nesoudělné, znamená to, že $\mathrm{NSD}(3 + 6i, 12 - 3i) = 3$.

V druhém případě pomocí Eukleidova algoritmu zjistíme, že $\mathrm{NSD}(5 + 3i, 13 + 18i) = 1 + 4i$.

(c) $3 - i\sqrt{2} = 3 - i\sqrt{2}$ je ireducibilní, neboť má normu $3^2 + 2 = 11$, což je prvočíslo a žádný prvek s pozitivní normou (tedy neinvertibilní) tento prvek nedělí.

Protože $\nu(5 - i\sqrt{2}) = 27$, jsou kandidáti na ireducibilní faktory prvky $1 \pm i\sqrt{2}$. Zkusmo zjistíme, že $5 - i\sqrt{2} = -(1 + i\sqrt{2})^3$.

(d) Pracujeme s normou $\nu(a+b\sqrt{2}) = |a^2 - 2b^2|$. Protože $\nu(3+\sqrt{2}) = |3^2 - 2| = 7$ je prvočíselná, je prvek $3 + \sqrt{2}$ ireducibilní. Norma $\nu(3 - 8\sqrt{2}) = |3^2 - 28^2| = 119 = 7 \cdot 17$, tedy případné netriviální dělitele by musel mít normu 7 a 17, najdeme-li kandidáta $\sqrt{2} - 3$ normy 7 (všimněme si, že prvek $3 + \sqrt{2}$ vhodný kandidát není), pak už snadno ověříme, že $3 - 8\sqrt{2} = (\sqrt{2} - 3) \cdot (1 + 3\sqrt{2})$ je hledaný ireducibilní rozklad.

Úloha 4.8. Najděte v oboru $\mathbb{Z}[\sqrt{3}]$ nekonečně mnoho invertibilních prvků.

Řešení. Všimneme si, že $a = 2 + \sqrt{3}$ je invertibilní, jelikož má normu $|2^2 - 3 \cdot 1^2| = 1$, proto jsou prvky $a^k, k \in \mathbb{N}$ také invertibilní a $a^k \neq a^j$ pro $k \neq j$.

⋆ **Úloha 4.9.** Buď $\mathcal{R}$ komutativní okruh a $a \in R$ splňující $a^n = 0$. Dokažte, že je prvek $1 - a$ invertibilní v $\mathcal{R}$. Platí toto tvrzení i v okruzích s nekomutativním násobením?

Řešení. Snadno zjistíme, že $(1 - a) \cdot \sum_{i=0}^{n-1} a^i = 1 - a^n = 1$, a proto je prvek $1 - a$ invertibilní a platí, že $(1 - a)^{-1} = \sum_{i=0}^{n-1} a^i$. Komutativitu násobení jsme nikde nepotřebovali, tvrzení tedy platí obecně.

⋆ **Úloha 4.10.** Rozhodněte, pro která $s, t \in \mathbb{Z}$ platí $\sqrt{s} \in \mathbb{Z}[\sqrt{t}]$. Uvažujte s, t taková, že nejsou dělitelná čtvercem prvočísla.

⋆ **Úloha 4.11.** Najděte všechna řešení $u, v \in \mathbb{Z}$ rovnice $u^2 + 47^2 = v^3$.

Řešení. Podobným postupem jako na str. 39 ve skriptech zjistíme, že jediná řešení jsou $u = \pm 52$, $v = 17$.

⋆⋆ **Úloha 4.12.** Označme $\varphi = \frac{1}{2}(1 + \sqrt{5})$.

(a) Dokažte, že $\mathbb{Z}[\varphi] = \{a + b\varphi \mid a, b \in \mathbb{Z}\}$.

(b) Nalezněte na $\mathbb{Z}[\varphi]$ nějakou normu, která bude multiplikativní a euklidovská.

(c) Rozhodněte, zda je $\sqrt{5}$ ireducibilní prvek $\mathbb{Z}[\varphi]$.

Řešení. (a) Stačí ukázat, že $\{a+b\varphi \mid a, b \in \mathbb{Z}\}$ (jakožto podmnožina $\mathbb{C}$) je uzavřená na okruhové operace; pro sčítání a opačný prvek je to snadné, pro násobení využijeme toho, že $\varphi^2 = \varphi + 1$.

(b) Inspirujeme se normami na okruzích $\mathbb{Z}[\sqrt{d}]$, které v zásadě fungují tak, že prvek vynásobíme vhodným „sdruženým“ prvkem. Sdružený prvek k φ by měl být takový prvek $\bar{\varphi}$, který bude splňovat $\varphi + \bar{\varphi} \in \mathbb{Z}$ a $\varphi \cdot \bar{\varphi} \in \mathbb{Z}$; tuto vlastnost má druhý kořen polynomu $x^2 - x - 1$, kterým je $\frac{1}{2}(1 - \sqrt{5}) = 1 - \varphi$. Položíme tedy

$$\nu(a + b\varphi) = |(a + b\varphi)(a + b\bar{\varphi})| = |a^2 + ab - b^2|.$$

Jelikož $\bar{\varphi}$ také splňuje $\bar{\varphi}^2 = \bar{\varphi} + 1$, není těžké nahlédnout, že takto definovaná norma je opravdu multiplikativní. Eukleidovskost dokážeme standardně: pro $u = a + b\varphi$ a $v = c + d\varphi$ uvážíme přesný podíl

$$z = \frac{u}{v} = \frac{(a + b\varphi)(c + d\bar{\varphi})}{c^2 + cd - d^2} = \frac{ac + ad - bd}{c^2 + cd - d^2} + \frac{bc - ad}{c^2 + cd - d^2}\varphi,$$

přičemž obě složky zaokrouhlíme na nejbližší celá čísla, získavajíc tak prvek $q \in \mathbb{Z}[\varphi]$. Položíme $r = u - vq$. Pak

$$\nu(r) = \nu(u - vq) = \nu(v) \cdot \nu\left(\frac{u}{v} - q\right)$$

(zde aplikujeme normu ν i na prvky $\mathbb{Q}[\varphi]$), takže chceme dokázat $\nu(z-q) < 1$. Položme $w = z - q = e + f\varphi$; jelikož q vzniklo zaokrouhlením z, platí $|e|, |f| \leq \frac{1}{2}$, tedy

$$\nu(w) = |e^2 + ef - f^2| \leq |e^2| + |ef| + |f^2| \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = \frac{3}{4} < 1,$$

což jsme chtěli.

(d) Platí $\sqrt{5} = -1 + 2\varphi$, tedy $\nu(\sqrt{5}) = |(-1)^2 + (-1) \cdot 2 - 2^2| = 5$. Jelikož je norma prvočíselná, jde o ireducibilní prvek.