Cvičení 15. 3. 2012

Buď $d \in \mathbb{Z}$. Potom definujeme okruh $\mathbb{Z}[\sqrt{d}]$ jako okruh na množině

$$\{a + \sqrt{d}b : a, b \in \mathbb{Z}\}$$

s aritmetickými operacemi zděděnými z $\mathbb{C}$ (pro případ $d < 0$). Pokaždé nám vznikne komutativní okruh, ale jeho vlastnosti se mohou výrazně lišit podle volby d. Celá konstrukce přináší něco nového pouze pokud d není čtverec celého čísla (tj. $d \neq n^2$), což budeme dále předpokládat.

Užitečná funkce na $\mathbb{Z}[\sqrt{d}]$ je *norma*: $N : a + \sqrt{d}b \mapsto |a^2 - db^2|$. Pro normu platí:

1. $N(x) \in \mathbb{N}_0$
2. $N(x) = 0 \Leftrightarrow x = 0$
3. $N(xy) = N(x)N(y)$
4. Pokud $x|y$ v $\mathbb{Z}[\sqrt{d}]$, tak $N(x)|N(y)$ v $\mathbb{Z}$.
5. Prvek x je invertibilní, právě když $N(x) = 1$.
6. Pokud $N(x)$ je prvočíslo, tak x je ireducibilní.

Norma obecně nemusí být euklidovská norma (funkce ϕ z minulého cvičení). Například pro $d = \sqrt{-1}$ (tzv. Gaussova celá čísla) tomu tak ale je.

Příklad 1. Rozhodněte, zda je ireducibilní:

1. $2x + 2$ v $\mathbb{Z}[x]$
2. 5 v $\mathbb{Z}$
3. 5 v $\mathbb{Z}[\sqrt{-1}]$
4. 5 v $\mathbb{Z}[\sqrt{-2}]$
5. 5 v $\mathbb{Z}[\sqrt{5}]$

Příklad 2. Rozložte v $\mathbb{Z}[i]$ na součin ireducibilních prvků:

1. $2 + 2i$
2. $1 - 5i$

3. 6
4. 11

Příklad 3. Najděte $NSD(3i, 2i+1)$ v $\mathbb{Z}[\sqrt{-1}]$.

Příklad 4. Dokažte vlastnosti normy z úvodu.

Příklad 5. Dokažte, že v okruhu $\mathbb{Z}[\sqrt{5}]$ existuje ireducibilní prvek, který není prvočinitel.

Příklad 6. Dokažte, že $\mathbb{Z}[\sqrt{-1}]$ je euklidovský.

Příklad 7 (Pellova rovnice pro $d = 5$)**.** Označme G množinu všech kladných čísel $a + \sqrt{5}b$, že $a, b \in \mathbb{Z}$ a platí $a^2 - 5b^2 = 1$. Dokažte:

1. G s násobením zděděným z $\mathbb{R}$ tvoří grupu
2. G je nekonečná cyklická grupa (najděte generátor!).