Cvičení 8. 3. 2012

Buď R komutativní okruh. Řekneme, že prvek r dělí prvek s (a napíšeme $r|s$), pokud existuje $t \in R$, že $rt = s$. Dělitelnost je kvaziuspořádání na prvcích R (tj. je tranzitivní a reflexivní, ale nemusí být antisymetrická).

Máme ireducibilní prvky (v uspořádání dělitelností nejmenší prvky nad invertibilními) a prvočinitele.

Obor integrity R je euklidovský, pokud můžeme dělit se zbytkem, tj. existuje funkce $\phi : R \to \mathbb{Z}$, že

1. $\phi(a) \leq \phi(b)$ kdykoli $a|b$, $b \neq 0$,
2. (to hlavní) kdykoli $a, b \in R$, $b \neq 0$, tak existují $r, s \in R$, že $\phi(s) < \phi(b)$ a $a = br + s$.

Pokud je okruh R euklidovský, tak funguje Euklidův algoritmus, všechny ireducibilní prvky jsou prvočinitelé a každý prvek $r \in R \setminus \{0\}$ lze psát jako součin prvočinitelů jednoznačně až na pořadí a asociovanost. (Obrácená implikace ale neplatí.)

Příklad 1. Rozhodněte, zda pro R libovolný komutativní okruh platí:

1. $a|b$, $c|d$ implikuje $ac|bd$,
2. $a|b$, $c|d$ implikuje $a + c|b + d$,
3. pokud R je obor integrity, tak z $ab = ac$ plyne $b = c$.

Příklad 2. Najděte v $\mathbb{Z}[x]$, $\mathbb{R}[x, y]$ ideály, které nejsou hlavní.

Příklad 3. Množina $2\mathbb{Z}$ není okruh (nemá jednotku), ale můžeme na ní definovat dělitelnost. Popište ireducibiliní prvky a prvočinitele $2\mathbb{Z}$ a najděte na $2\mathbb{Z}$ prvek, který nemá jednoznačný rozklad na prvočinitele.

Příklad 4. Buď R obor integrity. Dokažte, že a, b jsou asociované, právě tehdy když existuje invertibilní $r \in R$, že $a = rb$. Co to znamená pro $R = \mathbb{Z}$ a $R = \mathbb{R}[x]$?

Příklad 5. Dokažte, že $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\} \subset \mathbb{C}$ je euklidovský obor integrity (tj. najděte euklidovskou normu).

Příklad 6. Dokažte, že v okruhu $\{a + \sqrt{5}b : a, b \in \mathbb{Z}\}$ existuje ireducibilní prvek, který není prvočinitel.

Příklad 7. Dokažte, že každý konečný obor integrity je těleso.