Negaussovský obor se všemi NSD

Aneb dovysvětlení příkladu z přednášky, které jsem nestihl a které nyní do-dovysvětluji psanou formou...

Budiž

$$R := x\mathbb{Q}[x] + \mathbb{Z} = \{f \in \mathbb{Q}[x] \mid f(0) \in \mathbb{Z}\}.$$

V tomto okruhu existují nekonečné, v dělitelnosti ostře klesající řetězce, pročež nemůže být gaussovský – např. $2^k x \mid 2^{k+1}x$ pro každé celé k, ale opačná dělitelnost neplatí, takže volbami $k = 0, -1, -2, -3, \ldots$ získáme nekonečný řetězec ostře klesající v dělitelnosti.

Přesto však existují největší společní dělitelé libovolných dvou prvků. K tomu nám postačí ukázat, že součet hlavních ideálů je opět hlavní. Pokud totiž $(f) + (g) = (h)$, znamená to, že h dělí f i g, ale také jsme vyjádřili $h = uf + vg$ $(u, v \in R)$, takže každý společný dělitel f a g rázem dělí i h – tím je naplněna definice největšího společného dělitele.

Uvažujme tedy libovolná $f, g \in R$ a dokažme, že $(f) + (g)$ je hlavní. BÚNO f, g nemají (netriviálního) společného dělitele v R: když $d \mid f, g$ a $d \nmid 1$, pak stačí ukázat, že $\left(\frac{f}{d}\right) + \left(\frac{g}{d}\right)$ je hlavní, jeho součin s (d) totiž bude roven $(f) + (g)$.

Toto BÚNO dále zesílíme: tvrdím, že pak už f, g nemají netriviálního společného dělitele ani ve větším okruhu $\mathbb{Q}[x]$. Odteď budu u konceptů jako dělitelnost a generování ideálů pomocí indexu rozlišovat, zda je myslím ve smyslu okruhu R či ve smyslu okruhu $\mathbb{Q}[x]$. Pro spor nechť nějaký nekonstantní polynom $d \in \mathbb{Q}[x]$ splňuje $d \mid_{\mathbb{Q}[x]} f, g$. Nechť je to polynom

$$d = d_n x^n + \cdots + d_1 x + d_0.$$

Tvrdím, že $d_0 \neq 0$. Kdyby totiž $d_0 = 0$, použili bychom...

Pozorování. *Když $p \in R$ splňuje $p(0) = 0$, pak pro libovolné $z \in \mathbb{Z} \setminus \{0\}$ platí $z \mid_R p$.*

Důkaz. p vydělíme celým číslem z. Obdržíme polynom z $\mathbb{Q}[x]$, který má absolutní člen 0, což je celé číslo, takže je to prvek R. □

Tedy $d_0 = 0$ by implikovalo i $f(0) = g(0) = 0$, takže $2 \mid_R f, g$, ale přitom $2 \nmid_R 1$, takže f, g by měly netriviálního společného dělitele v R. Následně je tedy d_0 nenulové racionální číslo. Pak je polynom $\tilde{d} := \frac{d}{d_0}$ prvkem $\mathbb{Q}[x]$ a splňuje $\tilde{d}(0) = 1$, takže $\tilde{d} \in R$ a přitom stále $\tilde{d} \mid_{\mathbb{Q}[x]} f, g$. Podíl $f/\tilde{d}$ je polynom s racionálními koeficienty (díky dělitelnosti v $\mathbb{Q}[x]$) a jeho absolutní člen je $f(0)/\tilde{d}(0) = f(0)/1 = f(0) \in \mathbb{Z}$, takže $\tilde{d} \mid_R f$. Analogicky $\tilde{d} \mid_R g$, takže $\tilde{d}$ je netriviální společný dělitel f, g v R.

Nyní tak máme f, g nesoudělné v okruhu $\mathbb{Q}[x]$. To je OHI, takže už máme $(f)_{\mathbb{Q}[x]} + (g)_{\mathbb{Q}[x]} = (1)_{\mathbb{Q}[x]}$, takže existují nějaká $a, b \in \mathbb{Q}[x]$, že

$$af + bg = 1.$$

$a(0)$ a $b(0)$ jsou racionální čísla, zvolme tedy nějaký společný násobek jejich jmenovatelů $m \in \mathbb{Z}_{>0}$. To zajistí, že $ma, mb \in R$, takže máme

$$m = (ma)f + (mb)g \in (f)_R + (g)_R.$$

Tedy ve zkoumaném ideálu $(f)_R + (g)_R$ máme nenulové celé číslo. Podle pozorování takové m v okruhu R dělí jakýkoliv polynom s nulovým absolutním členem, takže odečtením vhodného násobku m musí v $(f)_R + (g)_R)$ ležet i absolutní členy $f_0 := f(0)$, $g_0 := g(0)$, což jsou celá čísla.

Nyní už můžeme v okruhu celých čísel vzít $s := \mathrm{NSD}(f_0, g_0)$. Toto s dělí (v R) f i g, protože dělí jejich absolutní členy a díky pozorování pak i všechny vyšší členy. Jelikož tedy předpokládáme, že f, g nemají netriviální společné dělitele, nutně $s = 1$. Tudíž jsou f_0, g_0 nesoudělná celá čísla, a protože $\mathbb{Z}$ je OHI, můžeme opět najít $U, V \in \mathbb{Z}$ taková, že $Uf_0 + Vg_0 = 1$. Jelikož $\mathbb{Z} \subset R$, tato lineární kombinace zachová náležitost ideálu nad R, takže konečně zjišťujeme, že $1 \in (f)_R + (g)_R$, což už znamená $(f)_R + (g)_R = (1)_R$, takže se jedná o hlavní ideál, jak jsme chtěli.

Alternativní důkaz

Namísto dokazování silnější vlastnosti (že součet hlavních ideálů je hlavní) lze taky NSD vyrobit explicitně. Bude se hodit:

Pozorování. *f dělí g v okruhu R, právě když $f \mid g$ v $\mathbb{Q}[x]$ a navíc má podíl celočíselný absolutní člen.*

Nyní tedy uvažujme $f, g \in R$, BÚNO ne obě nulová, a najděte $\mathrm{NSD}(f, g)$. Označme $n = \max\{\deg f, \deg g\}$ a dále

$$f = \sum_{k=0}^{n} f_k x^k, \qquad g = \sum_{k=0}^{n} g_k x^k.$$

Poté jako j zvolme nejmenší index takový, že alespoň jedno z f_j, g_j není nulové. Dále nechť je

$$d = \sum_{k=0}^{n} d_k x^k$$

největší společný dělitel f, g v okruhu $\mathbb{Q}[x]$. Zjevně musí pro $i < j$ také platit $d_i = 0$ a zároveň $d_j \neq 0$. Víme také, že v $\mathbb{Q}[x]$ smíme d přenásobit libovolnou nenulovou konstantou a stále to bude největší společný dělitel f, g. Tvrdím, že když ho takto vhodně přenásobíme, stane se i největším společným dělitelem f, g v okruhu R.

Pro volbu tohoto vhodného přenásobení se podívejme na f_j, g_j. To jsou obecně nějaká racionální čísla, zvolme a zafixujme tedy nějaký společný násobek $m \in \mathbb{Z}_{>0}$ jejich jmenovatelů, takže bude $mf_j, mg_j \in \mathbb{Z}$. Jakožto dvě celá čísla, která nejsou obě nulová, mají v $\mathbb{Z}$ největšího společného dělitele, označme ho $t := \mathrm{NSD}(mf_j, mg_j)$. Pak tvrdím, že vhodnou volbou přenásobení d je takové, kde nastane $d_j = \frac{t}{m}$ (toho lze přenásobením docílit, protože už jsme věděli, že původní d_j je nenulové).

Dokažme tedy, že takto zvolené d je největším společným dělitelem f, g v R. Nejprve, že je to společný dělitel. Víme, že $d \mid f, g$ v $\mathbb{Q}[x]$, podle pozorování tedy stačí vyšetřit absolutní členy podílů $\frac{f}{d}$, $\frac{g}{d}$. Vzhledem k $d_i = 0$ pro $i < j$ a $d_j \neq 0$ je absolutní člen $\frac{f}{d}$ roven $\frac{f_j}{d_j} = \frac{mf_j}{t} \in \mathbb{Z}$, protože $t = \mathrm{NSD}(mf_j, mg_j)$, takže podle pozorování d dělí f v R. Zcela analogicky d dělí g v R.

Nyní naopak budiž h společný dělitel f, g v R a dokažme, že pak už $h \mid d$. Opět z pozorování musí platit $h \mid f, g$ v $\mathbb{Q}[x]$, kde je máme $d = \mathrm{NSD}(f, g)$, takže nutně $h \mid d$ v okruhu $\mathbb{Q}[x]$. Zbývá tak dokázat, že $\frac{d}{h}$ má celočíselný absolutní člen. Kdyby náhodou

$$h = \sum_{k=0}^{n} h_k x^k$$

mělo pro $i < j$ nějaký koeficient $h_i \neq 0$, nutně by to znamenalo, že $\frac{d}{h}$ má nulový absolutní člen, takže bychom měli hotovo. Jinak tedy $h_i = 0$ pro všechna $i < j$, pak už z $h \mid f, g$ (v $\mathbb{Q}[x]$) nutně plyne $h_j \neq 0$, takže absolutní člen $\frac{d}{h}$ je přesně $\frac{d_j}{h_j}$. Přitom absolutní členy $\frac{f}{h}$, $\frac{g}{h}$, což jsou celá čísla, jsou $\frac{f_j}{h_j}$, $\frac{g_j}{h_j}$. Když jsme měli $t = \mathrm{NSD}(mf_j, mg_j)$, z rovnosti ideálů $(mf_j) + (mg_j) = (t)$ nad $\mathbb{Z}$, to značí, že máme celá čísla $a, b \in \mathbb{Z}$ taková, že $amf_j + bmg_j = t$, takže pak lze vyjádřit

$$\frac{d_j}{h_j} = \frac{t}{mh_j} = \frac{amf_j + bmg_j}{mh_j} = a \cdot \frac{f_j}{h_j} + b \cdot \frac{g_j}{h_j} \in \mathbb{Z},$$

čímž je dokončen důkaz, že $h \mid d$ v okruhu R, čili d je $\mathrm{NSD}(f, g)$ v R.