Cvičení 2, 20.10.2020 - návody a řešení

Noetherovskost

1. (!) Rozhodněte, zda je okruh $\mathbb{Q}$ konečně generovaný jako a) $\mathbb{Z}$-modul, b) $\mathbb{Q}$-modul, c) okruh, d) těleso.

   Návod: Ptám se: existují čísla $a_1, \ldots, a_n \in \mathbb{Q}$ taková, že každé racionální číslo lze vyjádřit jako a) lineární kombinaci $a_1, \ldots, a_n$ s celočíselnými koeficienty, b) lineární kombinaci $a_1, \ldots, a_n$ s racionálními koeficienty, c) jako hodnota polynomu $f \in \mathbb{Q}[x_1, \ldots, x_n]$ na $(a_1, \ldots, a_n)$ (což je to samé, jako že se dostanu z čísel $a_1, \ldots, a_n$ kamkoliv pomocí $+, -, \cdot$), d) to samé pro racionální funkce, resp. navíc operaci $^{-1}$.

   Řešení: a,c) ne, problém je nagenerovat všechny zlomky $\frac{1}{p}$, b) ano, stačí jeden generátor 1, každé q je $q \cdot 1$, d) ano, stačí jeden generátor 1, z ní dostanete sčítáním všechna celá čísla, inverzem zlomky $\frac{1}{a}$, součinem všechny zlomky

2. (!) Buď M noetherovský modul a N jeho podmodul. Dokaž, že pak je faktormodul M/N noetherovský.

   Řešení: Použijme definici, že modul je noetherovský právě tehdy, když je každý podmodul konečně generovaný. Vemte podmodul v M/N, ten bude podle 2. věty o izomorfismu tvaru U/N, kde U je modmodul M. Z noetherovskosti je U je konečně generovaný, generátory onačme $u_1, \ldots, u_n$, čili každý prvek $u \in U$ lze napsat jako lineární kombinaci $u = \sum r_i u_i$ pro nějaká $r_i \in R$. Čili každý prvek $[u] \in U/N$ lze napsat jako $[u] = [\sum r_i u_i] = \sum r_i [u_i]$, tedy $[u_1], ..., [u_n]$ generují podmodul U/N.

3. (*) Buď M modul a N jeho podmodul. Pokud jsou N a M/N oba noetherovské, pak je noetherovský také M (použij tvrzení 1.10).

   Návod: Uvažujte ideál U, koukněte na U/M, rozšiřte jeho konečnou bázi pomocí konečné báze N.

4. Buď K těleso. Dokažte, že $K[x_1, x_2, \ldots]$ (nekonečně mnoho proměnných) je gaussovský, ale ne noetherovský, a není to ani obor hlavních ideálů.

   Návod: Kdybych měl posloupnost vlastních dělitelů začínající f, pak ten f je jen v k proměnných a měl bych taky posloupnost vlastních dělitelů v $K[x_1, \ldots, x_k]$, spor s Gaussovou větou. Podobný argument pro NSD(f, g). Rostoucí posloupnost ideálů: $I_j = (x_1, \ldots, x_j)$.

Čínská věta o zbytcích

1. (!) Popiš všechny ideály v okruhu $\mathbb{Z}/(150)$ a charakterizuj, které dvojice z nich jsou komaximální.

   Návod: Je to OHI, takže pátrám po dělitelnosti čísel 0..149, maximální je totéž co prvočíslo, komaximální je totéž co ???

2. (!) Buď R obor hlavních ideálů, $m_1, \ldots, m_n$ jeho po dvou nesoudělné prvky a označme $M = m_1 \cdot \ldots \cdot m_n$. Dokažte pomocí čínské věty o zbytcích, že

$$R/(M) \simeq R/(m_1) \times \ldots \times R/(m_n).$$

   Návod: Ověřte předpoklady ČVZ. Proč je průnik všech $(m_i) = m_i R$ roven $(M) = MR$? Koukněte na minulá cvičení. Proč jsou $m_i R$ po dvou komaximální? Koukněte na předchozí úlohu.

Idea: když nějaká abstraktní myšlenka funguje v $\mathbb{Z}$, nejspíš bude fungovat ve všech OHI.

3. (!) Buď R okruh a $I_1, \dots, I_n$ po dvou komaximální ideály v R. Dokaž, že pak máme izomorfismus multiplikativních grup

$$(R/(I_1 \cdots I_n))^\times \simeq (R/I_1)^\times \times \cdots \times (R/I_n)^\times .$$

Řešení: Vezměte zúžení izomorfismu z ČVZ na invertibilní prvky. Násobení to zachovává, prosté to bude. Chceme dokázat, že to je dobře definované (tj. obraz invertibilního prvku je invertibilní) a že to je na (vzor n-tice invertibilních prvků je invertibilní). Ale to je obecná vlastnost, kdykoliv mám izomorfismus okruhů $\varphi : S \to T$, pak a je invertibilní v S právě tehdy, když $\varphi(a)$ je invertibilní v T.

PS: Připomeňte si důkaz vzorce na výpočet Eulerovy funkce, který jste nejspíš dělali v druháku. Tohle pro $R = \mathbb{Z}$ vám dá rozklad $\varphi(n)$ na součin $\varphi(p^{\cdots})$.

4. Buď R komutativní okruh s jednotkou, který má pouze konečně mnoho ideálů. Dále předpokládejme, že průnik maximálních ideálů v R je triviální. Dokažte, že R je direktním součinem konečně mnoha těles. Uveďte příklad konečného komutativního okruhu s jednotkou, který má netriviální průnik maximálních ideálů.

Axiom výběru

1. (!) Pomocí Zornova lemmatu dokaž, že každá lineárně nezávislá podmnožina vektorového prostoru jde rozšířit na bázi. (Skripta obsahují podrobný návod.)

   Návod: $M = \{A \subseteq V : A$ je lineárně nezávislá posloupnost vektorů$\}$, uspořádání $\subseteq$. Dokažte, že splňuje přepdoklady Zornova lemmatu a dokažte, že maximální prvek výsledek je báze, tj. že generuje V.

2. (!) Pomocí Zornova lemmatu dokaž, že každé zobrazení $f : A \to B$, které je *na* B, má pravý inverz, tj. že existuje zobrazení $g : B \to A$ takové, že $fg(x) = x$ pro všechna $x \in B$.

   Návod: $M = \{g : B \to A : \ fg = id\}$, uspořádání $\subseteq$ (ve smyslu: jedna funkce je větší než druhá, pokud má vetší definiční obor a na něm se shodují). Dokažte, že splňuje přepdoklady Zornova lemmatu a dokažte, že maximální prvek je definovaný všude.

3. (!) Pomocí Zornova lemmatu dokaž, že každé částečné uspořádání na dané množině lze rozšířit do lineárního uspořádání. (Rozšířením uspořádání $\leq$ se rozumí uspořádání $\preccurlyeq$ na téže množině takové, že pokud $x \leq y$, pak $x \preccurlyeq y$.)

   Návod: $M =$ množina všech částečných uspořádání na dané množině, uspořádání rozšířením (ve smyslu zadání). Dokažte, že splňuje přepdoklady Zornova lemmatu a dokažte, že maximální prvek výsledek je lineární.

4. (*) Pomocí Zornova lemmatu dokaž, že pokud v okruhu R existuje vlastní ideál, který není konečně generovaný, pak v něm také existuje prvoideál, který není konečně generovaný.