

Komutativní okruhy

Celistvost a Dedekindovy obory

Pavel Růžička

ruzicka@karlin.mff.cuni.cz
www.karlin.mff.cuni.cz/~ruzicka
Karlín - místnost 307, tel: 2-2191-3359

Zimní Semestr, 2008

Celířství a Dedekindovy obory

Část I

Dělitelnost a struktura modulů nad obory hlavních ideálů

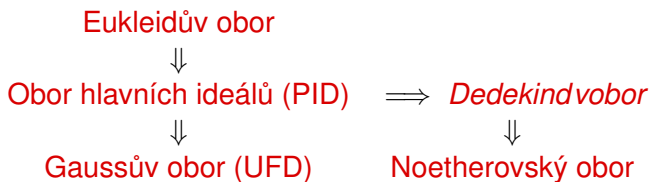
Úmluva

Nebude-li řečeno jinak, okruhem vždy míníme komutativní okruh s jednotkou.

Definice

Obor integrity (též jen obor) je okruh R ve kterém je $ab \neq 0$ pro každou dvojici nenulových prvků.

Postupně dospějeme k následující hierarchii oborů integrity:



Bud' R komutativní okruh.

- Pro $a, b \in R$ řekneme, že b **dělí** a , existuje-li $c \in R$ tak, že $a = bc$. Toto zapíšeme relací $b \mid a$.
- Řekneme, že prvky $a, b \in R$ jsou **asociované**, jestliže $a \mid b$ a zároveň $b \mid a$. Toto zapíšeme $b \sim a$.

Definice

Bud' R komutativní okruh. Prvek $a \in R$ je

- **prvočinitel**, jestliže z $a \mid bc$ plyne $a \mid b$ nebo $a \mid c$.
- **nerozložitelný**, jestliže z $a = bc$ plyne $a \sim b$ nebo $a \sim c$.

Snadno nahlédneme, že

$$\text{prvočinitel} \implies \text{nerozložitelný}.$$

Naopak to obecně neplatí.

Definice

Obor integrity R je **Eukleidův**, jestliže existuje zobrazení $N: R \rightarrow \mathbb{N}_0$ splňující pro všechna $a, b \in R$, $b \neq 0$ následující:

- 1 pokud $a \mid b$, tak $N(a) \leq N(b)$;
- 2 existují $c, d \in R$ tak, že $a = bc + d$ a zároveň $N(d) < N(b)$;

Příklad 1.1

- 1 Obor $\mathbb{Z}$ celých čísel s normou $N(a) = |a|$;
- 2 Obor $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ **Gaussových celých čísel** s normou $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2$;
- 3 Obor $T[x]$ polynomů v neurčité x nad (libovolným) tělesem T s normou $N(f) = \deg f$;

Pro dvojici neprázdných podmnožin A, B okruhu R definujeme

- ① $A + B = \{a + b \mid a \in A, b \in B\},$
- ② $AB = \{\sum_{i=1}^n a_i b_i \mid a_i \in A, b_i \in B \text{ a } n \in \mathbb{N}\}.$

Definice

Ideál je neprázdna podmnožina I okruhu R splňující

- ① $I + I \subseteq I,$
- ② $RI \subseteq I.$

Úmluva

Ideálem vždy míníme „vlastní“ ideál, tedy $I \subsetneq R$.

Definice

Ideál okruhu R je **hlavní** je-li generován jedním prvkem. Ideál generovaný prvkem a budeme značit (a) .

Obecněji, ideál generovaný prvky $a_1, a_2, \dots, a_n$ budeme značit $(a_1, a_2, \dots, a_n)$.

Definice

Obor integrity R je **obor hlavních ideálů**, je-li každý jeho ideál hlavní.

Lemma 1.2

Eukleidův obor je obor hlavních ideálů.

Příklad 1.3

- ❶ Obory $\mathbb{Z}[\sqrt{2}] = \{\alpha = a + \sqrt{2}b \mid a, b \in \mathbb{Z}\}$ s normou $N(\alpha) = |a^2 - 2b^2|$ je Eukleidův;
- ❷ Obor $\mathbb{Z}[\sqrt{-2}] = \{\alpha = a + \sqrt{-2}b \mid a, b \in \mathbb{Z}\}$ s normou $N(\alpha) = \alpha\bar{\alpha} = a^2 + 2b^2$ je Eukleidův;
- ❸ Obor $\mathbb{Z}[\zeta] = \{\alpha = a + \zeta b \mid a, b \in \mathbb{Z}\}$, kde $\zeta = e^{i\frac{2\pi}{3}}$ s normou $N(\alpha) = \alpha\bar{\alpha} = a^2 + ab + b^2$ je Eukleidův;
- ❹ Obor $\mathbb{Z}[\beta]$, kde $\beta = \frac{1}{2}(1 + \sqrt{-19})$ je obor hlavních ideálů, ale není Eukleidův;
- ❺ Obory $\mathbb{Z}[\sqrt{5}]$, $\mathbb{Z}[\sqrt{-3}]$, $T[x, y]$ nejsou obory hlavních ideálů;

Definice

Ideál P okruhu R je **prvoideál**, jestliže pro libovolné dva ideály I, J okruhu R platí

$$IJ \subseteq P \implies I \subseteq P \text{ nebo } J \subseteq P.$$

Lemma 1.4 (I.1.2)

Každý maximální ideál je prvoideál.

Tvrzení 1.5 (I.1.3)

Bud' Q ideál okruhu R .

- Q je maximální právě když R/Q je těleso.*
- Q je prvoideál právě když R/Q je obor integrity.*

Podívejme se jak souvisí dělitelnost se strukturou hlavních ideálů:

- 1 $a \mid b$ právě když $(b) \subseteq (a)$;
- 2 $a \sim b$ právě když $(b) = (a)$;

Prvek p oboru R je

- 1 nerozložitelný, právě když je ideál (p) maximální hlavní ideál;
- 2 prvočinitel, právě když je (p) prvoideál;

Pro prvky a, b, c oboru R platí

- 1 $(a) + (b) = (c)$ právě když c je největší společný dělitel a, b ;
- 2 $(a) \cap (b) = (c)$ právě když c je nejmenší společný násobek a, b ;

Definice

Rozklady $a = b_1 b_2 \cdots b_n = c_1 c_2 \cdots c_m$ prvku a v oboru R nazveme **asociované** jestliže $m = n$ a existuje permutace σ množiny $\{1, 2, \dots, n\}$ taková, že $b_i \sim c_{\sigma(i)}$ pro každé $i \in \{1, 2, \dots, n\}$.

Definice

Obor R je **Gaussův** jestliže pro každé nenulové $a \in R$ existuje rozklad $a = p_1 p_2 \cdots p_n$ v součin nerozložitelných prvků a každé dva takové rozklady jsou asociované.

Věta 1.6

Obor R je Gaussův právě když

- 1 *neexistuje nekonečný ostře rostoucí řetězec hlavních ideálů;*
- 2 *každý nerozložitelný prvek R je prvočinitel;*

Poznámka

- V libovolném oboru implikuje existence největšího společného dělitele to, že je každý nerozložitelný prvek prvočinitel.
- V Gaussově oboru má každá dvojice prvků největší společný dělitel. Ve Větě 1.6 lze tedy podmínku 2 nahradit podmínkou existence největšího společného dělitele.

Tvrzení 1.7

Obor hlavních ideálů je Gaussův obor.

Definice

R -modul M je **noetherovský**, je-li splněna některá z následujících vzájemně ekvivalentních podmínek:

- 1 Každý podmodul modulu M je konečně generovaný;
- 2 Každá množina podmodulů M má maximální prvek;
- 3 Neexistuje nekonečná ostře rostoucí poslupnost podmodulů modulu M ;

Lemma 1.8 (I.1.6)

Bud' N podmodul R -modulu M . Modul M je noetherovský právě když jsou moduly N a M/N noetherovské.

Definice

Okruh R je **noetherovský**, je-li splněna některá z následujících vzájemně ekvivalentních podmínek:

- 1 Každý ideál okruhu R je konečně generovaný;
- 2 Každá množina ideálů R má maximální prvek;
- 3 Neexistuje nekonečná ostře rostoucí poslupnost ideálů R ;

Tvrzení 1.9

Okruh R je noetherovský právě když je noetherovský každý konečně generovaný R -modul.

Věta 1.10 (Hilbertova o bázi I.2.1)

Okruh R je noetherovský právě když je noetherovský okruh $R[x]$.

Důkaz.

Nejprve ukážeme snadnou implikaci ($\Leftarrow$):

- Konečně generovaný R -modul M můžeme chápat jako $R[x]$ -modul, kde $xm = 0$ pro každé $m \in M$, se stejnou množinou generátorů.
- Ten je dle předpokladu noetherovský.



Pokračování důkazu Věty 1.10.

Nyní ukážeme netriviální implikaci ($\Rightarrow$): Buď R noetherovský okruh.

- Pro **spor** předpokládejme v $R[x]$ existuje ideál I který není konečně generovaný.
- Induktivně pak lze sestavit následující posloupnost polynomů:
 - $f_0 = 0$;
 - f_{n+1} je polynom nejmenšího stupně z polynomů v (neprázdné) množině $I \setminus (f_0, f_1, \dots, f_n)$;
- Označme a_n vedoucí koeficient polynomu f_n a s_n jeho stupeň.
- Z konstrukce plyne, že $s_0 \leq s_1 \leq s_2 \leq \dots$



Dokončení důkazu Věty 1.10.

- Označme $J_n = (a_0, a_1, \dots, a_n)$.
- Protože $J_0 \subseteq J_1 \subseteq J_2 \subseteq \dots$ a R je dle předpokladu noetherovský, existuje k tak, že $J_k = J_{k+1}$.
- To znamená, že $a_{k+1} \in (a_0, a_1, \dots, a_k)$, tj. $a_{k+1} = \sum_{i=0}^k r_i a_i$ pro vhodná $r_i \in R$.
- Pak má ale polynom $f_{k+1} - \sum r_i x^{s_{k+1}-s_i} f_i$ stupeň menší než s_{k+1} a přitom neleží v ideálu $(f_0, f_1, \dots, f_k)$.
- To je **spor**.



Důsledek 1.11 (1.2.2)

Okruh R je noetherovský právě když je noetherovský okruh $R[x_1, x_2, \dots, x_n]$.

Věta 1.12 (I.2.7)

Je-li R Gaussův obor je také $R[x]$ Gaussův obor.

Důsledek 1.13

Je-li R Gaussův obor je také $R[x_1, x_2, \dots, x_n]$ Gaussův obor.

Příklad 1.14

- 1 Obor $T[x, y]$ je Gaussův, ale ideál (x, y) není hlavní;
- 2 Obory $\mathbb{Z}[\sqrt{5}]$, $\mathbb{Z}[\sqrt{-3}]$ nejsou ani Gaussovy;

Budeme směřovat k důkazu Věty 1.12.

Bud' R Gaussův obor a T jeho podílové těleso. Necht' $p \in R$ je nerozložitelný prvek.

- 1 Pro $a \in R$ označme $\mathbf{v}_p(a)$ největší $\alpha \in \mathbb{N}_0$ takové, že $p^\alpha \mid a$. Číslo $\mathbf{v}_p(a)$ nazveme **p -valuace** a .
- 2 Pro $u = a/b \in T$ položíme $\mathbf{v}_p(u) = \mathbf{v}_p(a) - \mathbf{v}_p(b)$.
- 3 Pro polynom $f = a_n x^n + \dots + a_1 x + a_0$ položíme $\mathbf{c}_p(f) = \min\{\mathbf{v}_p(a_i) \mid i = 0, 1, \dots, n\}$.

Lemma 1.15 (I.2.3)

Bud' R Gaussův obor, T jeho podílové těleso a $p \in R$ nerozložitelný prvek. Pro nenulové $u \in T$ a $f \in T[x]$ je

$$\mathbf{c}_p(uf) = \mathbf{v}_p(u) + \mathbf{c}_p(f).$$

Definice

Polynom $f \in R[x]$ nazveme **primitivní**, jestliže jsou jeho koeficienty nesoudělné.

Polynom f je primitivní právě když $\mathbf{c}_p(f) = 0$ pro každé nerozložitelné $p \in R$.

Lemma 1.16 (Gaussovo I.2.4)

Součin primitivních polynomů je opět primitivní polynom.

Důsledek 1.17 (I.2.5)

Pro všechny nenulové $f, g \in T[x]$ platí

$$\mathbf{c}_p(fg) = \mathbf{c}_p(f) + \mathbf{c}_p(g).$$

Tvzení 1.18 (I.2.6)

Bud' R Gaussův obor a T jeho podílové těleso. Polynom $f \in R[x]$ je nerozložitelný právě když

- ① $\deg f = 0$ a f je nerozložitelný prvek R ;
- ② f je primitivní polynom, který je nerozložitelný v $T[x]$;

Důkaz.

- Je-li $\deg f = 0$, tedy $f \in R$, jsou dělitelé f prvky R a tedy f je nerozložitelný v $R[x]$ právě když je nerozložitelný v R .
- Předpokládejme, že $\deg f > 0$ a f je nerozložitelný v $R[x]$.
- Je $f = af_1$, kde $f_1 \in R[x]$ je primitivní a $a \in R$. Potom je a nutně invertibilní v R a tedy $f \sim f_1$, odkud plyne, že f je primitivní.



Pokračování důkazu Tvzení 1.18.

- Nechť $f = gh$ v $T[x]$.
- Existují rozklady $g = ug_1$, $h = vh_1$, kde $u, v \in T$ a g_1, h_1 jsou primitivní.
- Buď $p \in R$ nerozložitelný. Polynomy f, g_1, h_1 jsou primitivní, tedy $0 = \mathbf{c}_p(f) = \mathbf{c}_p(g_1) = \mathbf{c}_p(h_1)$.
- Podle Lemmatu 1.15 je $\mathbf{c}_p(g) = \mathbf{v}_p(u) + \mathbf{c}_p(g_1) = \mathbf{v}_p(u)$ a $\mathbf{c}_p(h) = \mathbf{v}_p(v) + \mathbf{c}_p(h_1) = \mathbf{v}_p(v)$.
- Podle Důsledku 1.17 je $0 = \mathbf{c}_p(f) = \mathbf{c}_p(g) + \mathbf{c}_p(h) = \mathbf{v}_p(u) + \mathbf{v}_p(v)$.
- Lze tedy předpokládat, že $uv = 1$. Potom je $f = g_1 h_1$ rozklad f v $R[x]$ a tedy, například, g_1 je invertibilní. Odtud plyne, že je g invertibilní v $T[x]$.



Dokončení důkazu Tvzení 1.18.

- Předpokládejme, že f je primitivní a nerozložitelný v $T[x]$.
- Nechť $f = gh$ v $R[x]$.
- Protože f je nerozložitelný v $T[x]$ je nutně stupeň jednoho z polynomů g, h nulový. Nechť například $\deg g = 0$, tedy $g = a \in R$.
- Bud' $p \in R$ nerozložitelný. Protože $a \in R$ a $h \in R[x]$ je $0 \leq \mathbf{v}_p(a), \mathbf{c}_p(h)$.
- Z předpokladu, že f je primitivní a z Lemmatu 1.15 dostáváme, že $0 = \mathbf{c}_p(f) = \mathbf{v}_p(a) + \mathbf{c}_p(h)$.
- Odtud $\mathbf{v}_p(a) = 0$ a tedy a je invertibilní v R .



Věta 1.12 (I.2.7)

Je-li R Gaussův obor je také $R[x]$ Gaussův obor.

Důkaz.

- Bud' $(f_1) \subseteq (f_2) \subseteq \dots$ nekonečná rostoucí posloupnost ideálů $R[x]$. Potom $f_j \mid f_i$ pro $i \leq j$ a $\deg f_1 \geq \deg f_2 \geq \dots$. Existuje tedy n tak, že $\deg f_n = \deg f_j$ pro všechna $j \geq n$.
- Označme a_i vedoucí koeficient polynomu f_i . Nutně $a_j \mid a_i$ pro $i \leq j$ a tedy $(a_1) \subseteq (a_2) \subseteq \dots$
- Protože R je Gaussův, existuje $m \geq n$ tak, že $(a_m) = (a_j)$, tj., $a_m \sim a_j$, pro každé $j \geq m$. Pak ale $f_m \sim f_j$ pro každé $j \geq m$, tj., $(f_m) = (f_{m+1}) = \dots$
- Obor $R[x]$ tedy splňuje podmínku 1 z Věty 1.6.



Pokračování důkazu Věty 1.12.

- Zbývá ukázat, že každý nerozložitelný prvek $R[x]$ je prvočinitelem.
- Nechť $f \in R[x]$ je nerozložitelný a $f \mid gh$.
- Je-li $f = p \in R$, je $0 < \mathbf{c}_p(gh) = \mathbf{c}_p(g) + \mathbf{c}_p(h)$ podle Důsledku 1.17. Proto $p \mid g$ nebo $p \mid h$.
- Předpokládejme, že $\deg f > 0$. Podle Tvrzení 1.18 je f primitivní a nerozložitelný v $T[x]$.
- Protože je f nerozložitelný (a tedy prvočinitel) v $T[x]$, dělí v $T[x]$ jeden z polynomů g, h . Nechť například $g = tf$ pro některé $t \in T[x]$.



Dokončení důkazu Věty 1.12.

- Stačí ukázat, že $t \in R[x]$.
- Buď p nerozložitelný prvek z R . Podle Důsledku 1.17 je

$$\mathbf{c}_p(g) = \mathbf{c}_p(t) + \mathbf{c}_p(f).$$

- Protože je f primitivní je $\mathbf{c}_p(f) = 0$ a tedy $0 \leq \mathbf{c}_p(g) = \mathbf{c}_p(t)$.
- Odtud již plyne, že $t \in R[x]$ a tedy $f \mid g$ v $R[x]$.



Pro ideály I, J okruhu R platí, že $IJ \subseteq I \cap J$, přitom obecně neplatí rovnost. Rozmyslete si jak je to v oboru celých čísel.

Definice

Ideály I, J oboru R nazveme **komaximální**, je-li $I + J = R$.

Lemma 1.19 (I.3.1)

Jsou-li ideály I, J komaximální, potom $IJ = I \cap J$.

Poznámka

Uvědomme si, že předchozí lemma je zobecněním faktu, že nejmenší společný násobek nesoudělných čísel je roven jejich součinu.

Lemma 1.20

Nechť I, J jsou ideály okruhu R . Uvažme homomorfismus

$$\varphi: R \rightarrow R/I \times R/J, \quad r \mapsto (r + I, r + J).$$

Potom $\ker \varphi = I \cap J$ a φ je na právě když jsou ideály I, J po dvou komaximální.

Důkaz Lemmatu 1.20.

- Rovnost $\ker \varphi = I \cap J$ je zřejmá.
- Předpis $(r + I, s + J) \mapsto (r + (I + J), s + (I + J))$ definuje projekci $\pi: R/I \times R/J \rightarrow R/(I + J) \times R/(I + J)$.
- Platí $\pi \circ \varphi(r) = (r + (I + J), r + (I + J))$.
- Odtud je vidět, že je-li φ a tedy i složení $\pi \circ \varphi$ na, je nutně $I + J = R$, tedy ideály I, J jsou komaximální.



Dokončení důkazu Lemmatu 1.20.

- Předpokládejme, že $I + J = R$.
- Uvažme $(b + I, a + J) \in R/I \times R/J$. Vzhledem k $I + J = R$ lze předpokládat, že $a \in I$ a $b \in J$.
- Potom $\varphi(a + b) = (b + I, a + J)$, odkud je vidět, že φ je na.



Tvrzení 1.21 (I.3.2)

Nechť $I_1, I_2, \dots, I_n$ jsou po dvou komaximální ideály. Potom

- 1 $I_1 I_2 \cdots I_n = I_1 \cap I_2 \cap \cdots \cap I_n$;
- 2 ideály $I_1 I_2 \cdots I_{n-1}$ a I_n jsou komaximální;

Lemma 1.22 (I.3.3)

Nechť $I_1, I_2, \dots, I_n$ jsou ideály okruhu R . Uvažme homomorfismus

$$\varphi: R \rightarrow (R/I_1) \times (R/I_2) \times \cdots \times (R/I_n),$$

$$r \mapsto (r + I_1, r + I_2, \dots, r + I_n).$$

Potom

- ❶ φ je na právě když jsou ideály $I_1, I_2, \dots, I_n$ po dvou komaximální;
- ❷ $\ker \varphi = I_1 \cap I_2 \cap \cdots \cap I_n$;

Důkaz.

Indukcí s využitím Lemmatu 1.20 a Tvrzení 1.21. □

Důsledek 1.23 (I.3.3)

Nechť $I_1, I_2, \dots, I_n$ jsou ideály okruhu R . Potom je homomorfismus

$$f: R \rightarrow (R/I_1) \times (R/I_2) \times \cdots \times (R/I_n),$$

$$r \mapsto (r + I_1, r + I_2, \dots, r + I_n).$$

izomorfismem právě když jsou ideály $I_1, I_2, \dots, I_n$ po dvou komaximální a mají nulový průnik.

Důsledek 1.24 (Čínská věta o zbytcích – I.3.4)

Bud' R okruh a $I_1, I_2, \dots, I_n$ po dvou komaximální ideály R , které mají nulový průnik. Potom pro každé $r_1, r_2, \dots, r_n$ existuje právě jedno $r \in R$ tak, že $r \equiv r_i \pmod{I_i}$ pro $i = 1, 2, \dots, n$.

Ještě se podívejme na klasickou formulaci Čínské věty o zbytcích v případě, kdy $R = \mathbb{Z}$.

Důsledek 1.25 (Čínská věta o zbytcích (případ $R = \mathbb{Z}$))

Mějme po dvou nesoudělná přirozená čísla $n_1, n_2, \dots, n_k$ a nezáporná celá čísla $r_1, r_2, \dots, r_k$ taková, že $r_i < n_i$. Potom má soustava rovnic

$$x \equiv r_1 \pmod{n_1}$$

$$x \equiv r_2 \pmod{n_2}$$

$$\vdots$$

$$x \equiv r_k \pmod{n_k}$$

právě jedno řešení splňující $0 \leq x < n_1 n_2 \cdots n_k$.

Lemma 1.26 (I.3.6)

Každý ideál okruhu R je obsažen v maximálním ideálu.

Množina nenulových prvků okruhu R která je uzavřena na násobení se nazývá **multiplikativní podmnožina** R .

Tvrzení 1.27 (I.3.7)

Bud' S multiplikativní podmnožina okruhu R a I ideál s ní disjunktní. Potom existuje prvoideál P tak, že $I \subseteq P$ a $S \cap P = \emptyset$.

Ideál P okruhu R je prvoideál právě když je $R \setminus P$ multiplikativní množina. Podle předchozího tvrzení naopak pro každou multiplikativní množinu existuje prvoideál s ní disjunktní.

Pro ideál I okruhu R položme

$$\sqrt{I} = \{a \in R \mid a^n \in I \text{ pro nějaké } n \in \mathbb{N}\}.$$

Tvrzení 1.28

Pro ideál I okruhu R platí

$$\sqrt{I} = \bigcap \{P \mid I \subseteq P \text{ a } P \text{ je prvoideál}\}.$$

- **Nilradikál** okruhu R je průnik všech jeho nenulových prvoideálů. Nilradikál je roven $\sqrt{0}$.
- **Jacobsonův radikál** okruhu R je průnik všech jeho maximálních ideálů. Značíme jej $J(R)$.

Tvrzení 1.29 (1.3.15)

$a \in J(R)$ právě když $1 - ar$ je invertibilní pro každé $r \in R$.

Nechť M_i , $i \in I$, jsou R -moduly.

- $\prod M_i = \{(m_i) \mid m_i \in M_i\}$;
- $\bigoplus M_i = \{(m_i) \in \prod M_i \mid m_i = 0 \text{ pro skoro všechna } i\}$;

Tvrzení 2.1 (I.4.1)

Nechť M_i , $i \in I$ jsou podmoduly modulu M . Uvažme zobrazení

$$\mu: \bigoplus M_i \rightarrow M, \quad (m_i) \mapsto \sum m_i.$$

Potom platí, že

- 1 zobrazení μ je prosté právě když $M_i \cap \sum_{j \neq i} M_j = 0$ pro každé $i \in I$ (moduly M_i jsou **nezávislé**);
- 2 zobrazení μ je na právě když $\sum M_i = M$ (moduly M_i generují M);

Necht' M_i , $i \in I$ jsou R -moduly. Jsou-li všechny moduly M_i rovny nějakému modulu M , píšeme $\bigoplus M_i = M^{(I)}$.

Uvažme pro množinu B modul $R^{(B)}$. Přiřazením

$$b \mapsto (b_i), \quad b_i = \begin{cases} 1 & : i = b \\ 0 & : i \neq b \end{cases}$$

lze ztotožnit množinu B s podmnožinou modulu $R^{(B)}$.

Definice

- Podmnožina B modulu F je jeho **volnou bází**, jestliže pro každý modul M a zobrazení $f: B \rightarrow M$ existuje právě jeden homomorfismus $\varphi: F \rightarrow M$ tak, že $\varphi(b) = f(b)$ pro každé $b \in B$.
- R -modul F je **volný**, má-li nějakou volnou bázi.

Tvrzení 2.2 (I.4.2 + I.4.7)

Dva volné moduly nad okruhem R jsou izomorfní, právě když jejich báze mají stejnou mohutnost.

Definice

Mohutnost báze volného modulu budeme nazývat jeho **hodností**.

Tvrzení 2.3

Modul $R^{(B)}$ je volný s bází B .

Tvrzení 2.4 (I.4.4)

Bud' B podmnožina R -modulu F . Je ekvivalentní

- ① *B je volná báze F ;*
- ② *každý prvek $a \in F$ lze jednoznačně vyjádřit jako lineární kombinaci prvků B , tj., ve tvaru*

$$a = \sum_{b \in B} a_b b, \text{ kde } a_b \in R;$$

- ③ *homomorfismus $\iota: R^{(B)} \rightarrow F$ rozšiřující identické vnoření $i: B \rightarrow F$ je izomorfismus.*

Tvrzení 2.5 (I.4.11)

Bud' N podmodul R -modulu M . Je-li modul M/N volný, existuje podmodul F modulu M tak, že $M = N \oplus F$. Zřejmě pak $F \simeq M/N$.

Poznámka

Vlastnost popsaná v předchozím tvrzení charakterizuje **projektivní** moduly což jsou právě direktní sčítance volných modulů. Obecně však projektivní modul nemusí být volný.

V závěru této kapitoly zkoumejme strukturu volných modulů nad obory hlavních ideálů.

- Buď R obor a F -volný R -modul konečné hodnosti n a $a \in F$;
- Buď $e_1, e_2, \dots, e_n$ volná báze F a $a = \sum r_i e_i$;
- Označme $C(a)$ ideál R generovaný prvky $r_1, r_2, \dots, r_n$.
- Ideál $C(a)$ nezávisí na volbě báze.

Tvrzení 2.6 (I.4.9)

Nechť R je obor hlavních ideálů a s je generátor $C(a)$. Potom existuje volná báze $e_1, e_2, \dots, e_n$ modulu F tak, že $a = se_i$.

Tvrzení 2.7 (I.4.10)

Buď R obor hlavních ideálů a M podmodul volného R -modulu F konečné hodnosti. Potom mezi ideály $C(a)$, $a \in M$, existuje největší.

Důkaz Tvzení 2.6.

- Tvzení ukážeme indukcí podle n . Pro $n = 1$ není co dokazovat.
- Buď $a = \sum r_i e_i$ a položíme $b = a - r_1 e_1$.
- Podle indukčního předpokladu existuje báze $e_1, f_2, f_3, \dots, f_n$ modulu F tak, že $b = tf_2$, kde $C(b) = (t)$.
- Buď s generátor $C(a)$. Potom pro vhodné $u, v \in R$, $r_1 = us$ a $t = vs$.
- Zároveň, protože $(s) = (r_1, t)$, existují $x, y \in R$ tak, že $s = xr_1 + yt$.
- Odtud dostaneme, že $s = (xu + yv)s$. Protože je R obor, plyne odtud $xu + yv = 1$.
- Položíme $g_1 = ue_1 + vf_2$, $g_2 = -ye_1 + xf_2$ a $g_j = f_j$ pro $j = 3, \dots, n$.
- Potom je $g_1, g_2, \dots, g_n$ volná báze F taková, že $a = sg_1$.



Důkaz Tvzení 2.7.

- Protože je M noetherovský, existuje $c \in M$ s maximálním $C(c)$.
- R je obor hlavních ideálů, tedy $C(c) = (s)$ pro některé $s \in S$. Podle Tvzení 2.6 existuje báze $e_1, e_2, \dots, e_n$ tak, že $c = se_1$.
- Buď $b = \sum r_i e_i$ libovolné. Ukážeme, že $r_i \in (s)$.
- Nechť t je generátor (s, r_1) a x, y jsou takové, že $t = xs + yr_1$.
- Potom $a = xc + yb = xse_1 + y \sum r_i e_i = te_1 + y \sum_{i=2}^n r_i e_i$.
- Vidíme, že $t \in C(a)$ a tedy $(s) \subseteq (t) \subseteq C(a)$. Z maximality (s) dostáváme, že $(s) = C(a)$.
- Odtud ihned plyne, že $r_i \in (s)$ pro $i = 2, \dots, n$.
- Zároveň ale $t \in (s)$ a tedy $(s) = (t) = (s, r_1)$. Proto také $r_1 \in (s)$.



Definice

Bud' R okruh a M modul nad R .

- Pro $a \in M$ položme

$$\text{Ann}(a) = \{r \in R \mid ra = 0\}.$$

$\text{Ann}(a)$ tvoří ideál R , který nazveme **anihilátor** a .

- Množina

$$\tau(M) = \{a \in M \mid \text{Ann}(a) \neq 0\}$$

tvoří podmodul M , který nazveme **torzní část** M .

Definice

Bud' R obor integrity. Modul M nazveme

- **torzní**, je-li $M = \tau(M)$;
- **beztorzní**, je-li $\tau(M) = 0$;

Lemma 2.8 (I.5.2)

Bud' M modul nad oborem integrity. Potom je modul $M/\tau(M)$ beztorzní.

Tvzení 2.9 (I.5.4)

Konečně generovaný beztorzní modul nad oborem hlavních ideálů je volný.

Důkaz.

- Existuje projekce $\varphi: F \rightarrow M$ z volného modulu F konečné hodnosti n . Volme navíc φ tak, že hodnost n je minimální.
- Pro spor předpokládejme, že $\ker \varphi \neq 0$ a zvolme nenulové $c \in \ker \varphi$.
- Podle Tvzení 2.6 existují báze $e_1, e_2, \dots, e_n$ a $s \in R$ tak, že $c = se_1$. Protože $c \neq 0$ je také $s \neq 0$.
- Pak ale $s \in \text{Ann}\varphi(e_1)$, odkud plyne $\varphi(e_1) = 0$. To vede ke sporu s minimalitou n .



Důsledek 2.10 (I.5.6)

Bud' M konečně generovaný modul nad oborem hlavních ideálů. Potom existuje volný modul F tak, že $M = F \oplus \tau(M)$.

Pro ideál I okruhu R a R -modul M definujeme

- $M_n^I = \{a \in M \mid I^n \subseteq \text{Ann}(a)\};$
- $\tau_I(M) = \bigcup M_n^I = \{a \in M \mid \exists n: I^n \subseteq \text{Ann}(a)\};$

Tvrzení 2.11

Pro obor hlavních ideálů R označme $\mathcal{P}$ množinu všech jeho nenulových prvoideálů. Pro torzní R -modul M platí

$$M = \bigoplus_{P \in \mathcal{P}} \tau_P(M).$$

Důkaz Tvzení 2.11.

- Nejprve ukážeme, že $M = \sum \tau_P(M)$.
- Zvolme $u \in M$ a buď $r \in \text{Ann}(u)$ s rozkladem $r = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ v součin prvočinitelů.
- Položme $s_i = r/p_i^{\alpha_i}$. Ideál generovaný s_i je roven R , tedy $1 = \sum x_i s_i$ pro vhodné x_i .
- Je $s_i u \in \tau_{(p_i)}(M)$ a $u = \sum x_i s_i u$. Odtud vidíme, že ideály $\tau_P(M)$ generují M .
- Zbývá ukázat, že $\tau_P(M) \cap \sum_{Q \neq P} \tau_Q(M) = 0$. Pro spor předpokládejme, že tento průnik obsahuje nenulové v .
- Buď $P = (p)$. Pak $p^\alpha v = 0$ pro nějaké kladné α a zároveň $rv = 0$ pro nějaké r nesoudělné s p .
- Proto existují x, y tak, že $1 = xp^\alpha + yr$, odkud $v = (xp^\alpha + yr)v = xp^\alpha v + yrv = 0$, což je spor.



Zaměříme se na strukturu modulů $\tau_P(M)$ (kde M je torzní modul nad oborem hlavních ideálů R a $P \in \mathcal{P}$).

- Buď P nenulový prvoideál R a p prvočinitel takový, že $P = (p)$.
- Modul M splňující $M = \tau_P(M)$ budeme nazývat **p -modul**.
- Buď $a \in M$. Nejmenší $n \in \mathbb{N}$ takové, že $p^n a = 0$ budeme nazývat **p -výškou** prvku a (a značit **$h_p(a)$**).
- Pro $n \in \mathbb{N}_0$ položme $M_n^p = \{a \in M \mid h_p(a) \leq n\}$.
- M_n^p je podmodul M a platí $0 = M_0^p \subseteq M_1^p \subseteq M_2^p \subseteq \dots$.
- V oboru hlavních ideálů jsou nenulové prvoideály maximální. Faktor R/P je tedy těleso.
- Je $P \subseteq \text{Ann}(M_{n+1}^p/M_n^p)$ a na M_{n+1}^p/M_n^p lze nahlížet jako na vektorový prostor nad R/P .

Tvrzení 2.12 (I.5.7)

Bud' M p -modul, $a \in M$ a $r \in R$ nesoudělné s p . Potom $h_p(a) = h_p(ra)$ a prvky a, ra generují stejný podmodul R .

Lemma 2.13 (I.5.8 + I.5.10)

- Konečně generovaný p -modul lze vyjádřit jako direktní součet $\bigoplus_{i=1}^n Ra_i$ cyklických modulů, kde $Ra_i \simeq R/(p^{m_i})$ pro vhodné $m_i \in \mathbb{N}$.*
- Tento rozklad je až na pořadí jednoznačný.*

Důkaz.

- Bud' M konečně generovaný p -modul. Bud' k nejmenší takové, že $M = M_k^p$.*
- Je-li $k = 0$ je M nulový. Je-li $k = 1$ je M vektorový prostor nad tělesem $R/(p)$ a tedy je izomorfní $\bigoplus R/(p)$.*



Pokračování důkazu Lemmatu 2.13.

- Dále budeme postupovat indukcí podle k . Podle indukčního předpokladu existují prvky $u_1, u_2, \dots, u_s$ tak, že $M/M_1^p = \bigoplus R(u_i + M_1^p)$. Označme $N = \sum Ru_i$.
- Ukážeme, že $\sum r_i u_i = 0$ implikuje $r_i u_i = 0$, tj., že $N = \bigoplus Ru_i$.
- Je $\sum r_i(u_i + M_1^p) = (\sum r_i u_i) + M_1^p = M_1^p$, odkud $r_i u_i \in M_1^p$.
- Bud' $r_i = p^{m_i} x_i$, kde $p \nmid x_i$. Je $m_i \geq h_p(u_i + M_1^p) \geq 1$.
- Proto $0 = p(\sum p^{m_i-1} x_i u_i)$, odkud $\sum p^{m_i-1} x_i u_i \in M_1^p$.
- To znamená, že $\sum p^{m_i-1} x_i(u_i + M_1^p) = M_1^p$, odkud, dle indukčního předpokladu, $p^{m_i-1} x_i(u_i + M_1^p) = M_1^p$ a tedy $m_i - 1 \geq h_p(u_i + M_i)$.
- Protože je $h_p(u_i + M_i) = h_p(u_i) - 1$, je $m_i \geq h_p(u_i)$.
- To ale znamená, že $p_i^{m_i} x_i u_i = 0$ podle Tvzení 2.12.
- Bud' $M_1^p = (N \cap M_1^p) \oplus K$.
- Potom $M = N \oplus K = (\bigoplus Ru_i) \oplus (\bigoplus R/(p))$.



Dokončení důkazu Lemmatu 2.13.

- Jednoznačnost rozkladu $M = \bigoplus Ru_i$ plyne z toho, že počet u_i s výškou větší než k je roven dimenzi M_{k+1}^p / M_k^p . □

Věta 2.14 (I.5.11)

Bud' M konečně generovaný modul nad oborem hlavních ideálů. Potom

$$M = F \oplus \bigoplus_{i=1}^n M_i,$$

kde F je volný modul konečné hodnosti a M_i jsou p_i -moduly pro po dvou neasociované prvočinitele p_i . Navíc

$$M_i \simeq \bigoplus_{j=1}^{n_i} R/(p^{k_{i,j}}).$$

Tyto rozklady jsou až na pořadí určeny jednoznačně.

Věta 2.15 (I.6.2)

Nechť F je volný modul hodnosti $n \in \mathbb{N}$ nad oborem hlavních ideálů. Potom pro každý podmodul M modulu F existuje volná báze $e_1, e_2, \dots, e_n$ modulu F a klesající posloupnost ideálů $I_1 \supseteq I_2 \supseteq \dots \supseteq I_n$ okruhu R tak, že $M = \bigoplus I_i e_i$.

Důkaz.

- Důkaz provedeme indukcí podle n . Pro $n = 1$ je důkaz zřejmý.
- Podle Lemmat 2.6 a 2.7 existuje $a \in M$ s největším $C(a) = (s_1)$ a báze $f_1, f_2, \dots, f_n$ tak, že $a = s_1 f_1$.
- Označme $F' = \sum_{i>1} Rf_i$ a $M' = M \cap F'$.
- Je-li $b = \sum r_i f_i \in M$, je $r_1 \in C(a)$ a tedy $s_1 \mid r_1$, tj. $r_1 = s_1 t$.
- Potom $b - ta \in M'$ a tedy $M = Ra \oplus M'$.



Dokončení důkazu Věty 2.15.

- Dle indukčního předpokladu existují báze $e_2, \dots, e_n$ modulu F' a prvky $s_2, \dots, s_n$ okruhu R splňující $(s_2) \supseteq \dots \supseteq (s_n)$ tak, že $M' = \bigoplus R s_i e_i$.
- Vzhledem k tomu, že $C(a)$ je největší, platí navíc $(s_1) \supseteq (s_i)$.
- Položíme-li $e_1 = f_1$ a $I_i = (s_i)$, platí $I_1 \supseteq I_2 \supseteq \dots \supseteq I_n$ a $M = \bigoplus I_i e_i$.



Důsledek 2.16 (I.6.3)

Nechť F je volný modul hodnosti $n \in \mathbb{N}$ nad oborem hlavních ideálů. Potom pro každý podmodul M modulu F existuje volná báze $e_1, e_2, \dots, e_n$ modulu F a prvky $r_1, r_2, \dots, r_n$ okruhu R splňující $r_i \mid r_j$ pro $i \leq j$ takové, že $M = \bigoplus R r_i e_i$.

Je-li k největší takové, že $r_k \neq 0$, tvoří prvky $r_1 e_1, r_2 e_2, \dots, r_k e_k$ volnou bázi M .

Pro podmoduly A, B modulu M označme

$$(A : B) = \{r \in R \mid rB \subseteq A\}.$$

Lemma 2.17 (I.6.6)

Pro dvojici I, J ideálů okruhu R platí:

- ① $(I : J)$ je ideál obsahující I ;
- ② $(I : J) = R$ právě když $J \subseteq I$;
- ③ $(I : J) = (I : I + J)$;
- ④ je-li J hlavní ideál, potom $J(R/I) \simeq R/(I : J)$;

Lemma 2.18 (I.6.7)

Bud' R obor hlavních ideálů. Potom

① *pro ideály $I \subseteq J$ platí $I = J(I : J)$*

② *pro ideály $J_1, J_2 \subseteq J$ ideály, platí*

$$(J_1 : J) = (J_2 : J) \text{ právě když } J_1 = J_2.$$

Věta 2.19 (I.6.8)

Pro konečně generovaný modul M nad oborem hlavních ideálů R existuje jednoznačně určená klesající posloupnost ideálů

$I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n$ tak, že $M \simeq \bigoplus R/I_i$.

Důkaz Věty 2.19.

- Vzhledem k Důsledku 2.16 stačí ukázat jednoznačnost.
Předpokládejme, že $M \simeq \bigoplus R/I_i \simeq \bigoplus R/J_j$, kde $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n$ a $J_1 \supseteq J_2 \supseteq \cdots \supseteq J_m$.
- Důkaz povedeme indukcí podle $m + n$. Předpokládejme, že $m \geq n$ a položme $I = I_1$.
- Podle Lemmatu 2.17 je

$$IM \simeq \bigoplus R/(I_i : I) \simeq \bigoplus R/(J_j : I),$$

navíc $(I_1 : I) \supseteq \cdots \supseteq (I_n : I)$ a $(J_1 : I) \supseteq \cdots \supseteq (J_m : I)$.

- Protože $(I_1 : I) = R$, můžeme použít na získané rozklady indukční předpoklad, odkud dostaneme nutně $(J_1 : I) = R$ což znamená, že $I \subseteq J_1$.
- Buď P prvoideál obsahující J_1 . Potom $PM \simeq \bigoplus P/I_i \simeq P/J_j$ odkud $P/MP \simeq \bigoplus (R/I_i)/(P/I_i) \simeq (R/P)^n \simeq \bigoplus (R/J_j)/(P/J_j) \simeq (R/P)^m$. Proto $m = n$.



Dokončení důkazu Věty 2.19.

- Položme $J_1 = J$. Je

$$JM \simeq \bigoplus R/(I_i : J) \simeq \bigoplus R/(J_j : J).$$

- Porovnáním rozkladů modulu JM dostaneme $(I_i : J) = (J_j : J)$ pro každé $i = 1, \dots, n$.
- Protože J je největší z ideálů I_i, J_j , jsou podle Lemmatu 2.18 $I_i = J_j$.



Část II

Teorie těles a její aplikace

Rozšíření těles a stupeň rozšíření

- Dvojici těles $T \leq U$ nazveme **rozšířením**.
- Je-li $T \leq U$ rozšíření a $M \subseteq U$, označíme
 - $T[M]$ nejmenší podokruh U obsahující T a M .
 - $T(M)$ nejmenší podtěleso U obsahující T a M .
- Buď $T \leq U$ rozšíření. **Stupeň** tohoto rozšíření je $[U : T] = \dim_T U$.
- Jsou-li $T \leq U \leq V$ rozšíření těles, platí

$$[V : T] = [V : U][U : T].$$

Algebraický prvek

- Buď $T \leq U$ rozšíření. Prvek $\alpha \in U$ je **algebraický** nad T je-li kořenem nějakého polynomu $f \in T[x]$.
- Polynomy $\{f \in T[x] \mid f(\alpha) = 0\}$ tvoří ideál. Monický generátor tohoto ideálu nazýváme **minimální polynom** α (nad T) a značíme $m_{T,\alpha}$.
- Prvek, který není algebraický se nazývá **transcendentní**;
- Buď $T \leq U$ rozšíření, $\alpha \in U$. Je ekvivalentní
 - α je algebraický;
 - $T(\alpha) = T[\alpha]$;
 - stupeň $[T : T(\alpha)]$ je konečný;

Navíc pak $[T : T(\alpha)] = \deg m_{T,\alpha}$.

Algebraické rozšíření

- Rozšíření $T \leq U$ je **algebraické**, je-li každý prvek z U algebraický nad T .
- Pro rozšíření $T \leq U$ je ekvivalentní
 - $T \leq U$ je algebraické;
 - pro každou $M \subseteq U$, $T(M) = T[M]$;
 - pro každou konečnou $F \subseteq U$ je stupeň $[T : T(F)]$ konečný;
- Bud' $T \leq U$ rozšíření. Množina

$$\{\alpha \in U \mid \alpha \text{ je algebraický nad } T\}$$

tvoří těleso nazývané **algebraický uzávěr** T v U .

- Těleso je **algebraicky uzavřené** nemá-li vlastní algebraické rozšíření.
- **Algebraický uzávěr** tělesa je jeho algebraické, algebraicky uzavřené rozšíření.

Definice

Bud' $T \leq U$ rozšíření a $f \in T[x]$ je nerozložitelný polynom. Je-li $U = T[\alpha]$ pro nějaký kořen α polynomu f , nazveme U **kořenové nadtěleso** polynomu f nad T .

- Bud' $T \leq U, T \leq V$ dvojice rozšíření. Homomorfismus $f: U \rightarrow V$, který je identický na T (tj., $f(t) = t$ pro každé $t \in T$) nazveme **T -homomorfismem**.
- Tělesa U, V jsou **T -izomorfní**, existuje-li T -izomorfismus U na V .

Lemma 3.1

Kořenová nadtělesa polynomu f nad T jsou T -izomorfní.

Definice

Bud' $T \leq U$ rozšíření a $f \in T[x]$ je polynom. Je-li $U = T[A]$ pro nějakou množinu A kořenů polynomu f a f se v U rozkládá na kořenové činitele, nazveme U **rozkladové nadtěleso** polynomu f nad T .

Lemma 3.2

Rozkladová nadtělesa polynomu f nad T jsou T -izomorfní.

Věta 3.3

- *Pro každé těleso existuje algebraický uzávěr.*
- *Algebraické uzávěry tělesa T jsou T -izomorfní.*

Prvotěleso

- Každé těleso T obsahuje minimální podtěleso nazývané **prvotěleso**. Prvotěleso je izomorfní
$$\begin{cases} \mathbb{F}_p : & \text{je-li charakteristika } T \text{ rovna prvočíslu } p; \\ \mathbb{Q} : & \text{je-li charakteristika } T \text{ rovna } 0; \end{cases}$$
- Prvotěleso je fixní při každém endomorfismu tělesa T .

Konečná charakteristika

- Je-li T těleso konečné charakteristiky p , určuje přiřazení $x \mapsto x^p$ endomorfismus T nazývaný **Frobeniův endomorfismus**.
- Konečné těleso charakteristiky p má p^k prvků a je rozkladovým nadtělesem polynomu $x^{p^k} - x$ nad $\mathbb{F}_p$. Značíme jej $\mathbb{F}_{p^k}$.
- Multiplikativní grupa nenulových prvků konečného tělesa je cyklická.

Necht' $T \leq U$, $T \leq V$ jsou rozšíření. Množinu všech T -homomorfismů z U do V budeme značit $\text{hom}_T(U, V)$.

Definice

Necht' $T \leq U \leq W$ jsou algebraická rozšíření, kde W je algebraicky uzavřené. Mohutnost množiny $\text{hom}_T(U, W)$ nazveme **stupeň separability** U nad T a označíme $[U : T]_S$.

Lemma 3.4

Necht' $T \leq U \leq W$ jsou algebraická rozšíření a W je algebraicky uzavřené. Potom

- 1 Každý T -homomorfismus z U do W lze rozšířit na T -endomorfismus W .
- 2 Každý T -endomorfismus W je automorfismem.

Lemma 3.5 (II.2.1)

Necht' $T \leq U \leq V \leq W$ je posloupnost algebraických rozšíření těles, přičemž W je algebraicky uzavřené. Pro každé $\varphi \in \text{hom}_T(U, W)$ zvolme rozšíření $\bar{\varphi} \in \text{hom}_T(W, W)$ (které existuje a je automorfismem podle předcházejícího lemmatu). Potom přiřazení $(\psi, \varphi) \mapsto \bar{\varphi} \circ \psi$ určuje bijekci

$$\text{hom}_U(V, W) \times \text{hom}_T(U, W) \rightarrow \text{hom}_T(V, W).$$

Důsledek 3.6 (II.2.2)

Jsou-li $T \leq U \leq V$ algebraická rozšíření, potom

$$[V : T]_S = [V : U]_S [U : T]_S.$$

Věta 3.7 (II.2.3)

Bud' $T \leq U$ algebraické rozšíření konečného stupně. Platí

- ① $[U : T]_S \leq [U : T]$;
- ② *je-li $\alpha \in U$ takové, že $\deg m_{T,\alpha} = n$ a $m_{T,\alpha}$ má ve svém rozkladovém nadtělese právě k různých kořenů, je*
 $[U : T]_S \leq k/n[U : T]$;

Definice

- Polynom $f \in T[x]$ je **separabilní**, nemá-li ve svém rozkladovém nadtělese vícenásobné kořeny;
- Prvek α je **separabilní**, je-li $m_{T,\alpha}$ separabilní;
- Rozšíření $T \leq U$ je **separabilní**, je-li každé $\alpha \in U$ separabilní;

Tvrzení 3.8 (II.2.4)

Pro rozšíření $T \leq U$ konečného stupně je ekvivalentní

- 1 $T \leq U$ je separabilní;
- 2 $U = T[A]$ pro konečnou množinu A separabilních prvků;
- 3 $[U : T]_S = [U : T]$;

Definice

Všechny prvky z U separabilní nad T tvoří těleso nazývané **separabilní uzávěr** T v U .

Tvrzení 3.9 (II.2.7)

Nechť $T \leq U \leq V$ jsou rozšíření. Je-li U separabilní nad T a V separabilní nad U , je také V separabilní nad T .

Tvrzení 3.10 (II.2.7)

Nechť T je těleso a $f \in T[x]$ polynom, který není separabilní. Potom platí

- *charakteristika T je $p > 0$;*
- *existuje $g \in T[x]$ tak, že $f(x) = g(x^p)$;*
- *některý z koeficientů f neleží v obrazu Frobeniova endomorfismu;*

Definice

Těleso T se nazývá **perfektní**, jestliže je charakteristiky 0, nebo je Frobeniův endomorfismus automorfismem. Například konečná a algebraicky uzavřená tělesa jsou perfektní.

Důsledek 3.11 (II.2.8)

Algebraické rozšíření perfektního tělesa je separabilní.

Rozšíření $T \leq U$ je **jednoduché**, je-li $U = T[\alpha]$.

Věta 3.12 (II.3.1)

Separabilní rozšíření konečného stupně je jednoduché.

Důkaz.

Bud' $T \leq U$ separabilní rozšíření konečného stupně.

- Je-li těleso T konečné, je i U konečné a jednoduchost rozšíření plyne z cykličnosti U^* .
- Předpokládejme, že T je nekonečné a bud' $\alpha \in U$ zvoleno tak, že je stupeň $[T(\alpha) : T]$ maximální. Pro spor předpokládejme, že existuje $\beta \in U \setminus T(\alpha)$. Označme $V = T(\alpha, \beta)$.
- Bud' $\text{hom}_T(V, K) = \{f_1, f_2, \dots, f_n\}$. Ze separability plyne

$$n = [V, T] > [T(\alpha) : T].$$



Dokončení důkazu Věty 3.12.

- Pro každé $i < j$ je buďto $f_i(\alpha) - f_j(\alpha) \neq 0$ nebo $f_i(\beta) - f_j(\beta) \neq 0$. Proto je polynom

$$g(t) = \prod_{i < j} (f_i(\alpha) - f_j(\alpha)) + t(f_i(\beta) - f_j(\beta))$$

nenulový.

- Protože T je podle předpokladu nekonečné, existuje $t \in T$ tak, že $g(t) \neq 0$.
- Pak ale pro $i \neq j$ platí $f_i(\alpha + t\beta) \neq f_j(\alpha + t\beta)$ a tedy $[T(\alpha + t\beta) : T]_S \geq n$.
- Odtud plyne, že $V = T(\alpha + t\beta)$ což je **spor** s volbou α .



Definice

Rozšíření $T \leq U$ nazveme **normální** je-li algebraické a pro každý endomorfismus $f \in \text{hom}_T(U, W)$, kde W je algebraický uzávěr U , $f(U) = U$.

Normální separabilní rozšíření konečného stupně se nazývá **Galoisovo**.

Tvrzení 3.13 (II.3.3)

- 1 *Rozkladové nadtěleso polynomu je normální.*
- 2 *Rozkladové nadtěleso separabilního polynomu je Galoisovo.*

Tvrzení 3.14 (II.3.4)

Každé Galoisovo rozšíření je rozkladovým nadtělesem nerozložitelného separabilního polynomu.

Bud' $\mathcal{M} \subset T[x]$ množina polynomů. Rozkladové nadtěleso množiny $\mathcal{M}$ je nejmenší rozšíření U tělesa T ve kterém se každý polynom z $\mathcal{M}$ rozkládá v součin lineárních polynomů.

Tvrzení 3.15 (II.3.5)

Rozšíření $T \leq U$ je normální právě když existuje množina polynomů $\mathcal{M} \subseteq T[x]$ taková, že U je jejím rozkladovým nadtělesem.

Tvrzení 3.16 (II.3.6)

Bud' $T \leq U$ rozšíření. Uvažme meztěleso V , které se skládá ze všech α jejichž minimální polynom se v U rozkládá v součin lineárních polynomů. Potom je V největší normální rozšíření T jež je obsaženo v U .

*Těleso V nazveme **normálním uzávěrem** T v U .*

Bud' $T \leq U$ algebraické rozšíření. Označme

$$\text{Gal}(U, T) = \text{hom}_T(U, U).$$

Pro podgrupu G grupy $\text{Aut}(U)$ položme

$$\text{Fix}(U, G) = \{\alpha \in U \mid g(\alpha) = \alpha \text{ pro každé } g \in G\}.$$

Tvrzení 3.17 (II.3.7)

Bud' $T \leq U$ rozšíření a $G \subseteq \text{Aut}(U)$. Potom

- ① $T \leq \text{Fix}(U, \text{Gal}(U, T));$
- ② $G \leq \text{Gal}(U, \text{Fix}(U, G));$

Lemma 3.18 (II.3.2)

Bud' U těleso a necht' G je n -prvková podgrupa grupy $\text{Aut}(U)$. Potom je U separabilní rozšíření tělesa $\text{Fix}(U, G)$ stupně n a platí, že

$$G = \text{Gal}(U, \text{Fix}(U, G)).$$

Důkaz.

- Označme $T = \text{Fix}(U, G)$. Pro $\alpha \in U$ položme $G(\alpha) = \{g(\alpha) \mid g \in G\}$ a uvažme polynom

$$f_\alpha = \prod_{\beta \in G(\alpha)} (x - \beta).$$

- Protože $hG(\alpha) = G(\alpha)$ pro každé $g \in G$, je polynom f_α invariantní vzhledem ke všem automorfismům z grupy G a proto $f_\alpha \in T[x]$.
- Protože je navíc α kořen f_α , platí že $m_{\alpha, T} \mid f_\alpha$.



Pokračování důkazu Lemmatu 3.18.

- Polynom f_α je separabilní, proto je $m_{\alpha,T}$ separabilní a tedy je rozšíření $T \leq U$ separabilní.
- Ukážeme, že rozšíření $T \leq U$ je konečného stupně. Pro spor předpokládejme, že tomu tak není. Potom existuje mezirozšíření $T \leq V \leq U$ stupně $k > n$.
- Podle Věty 3.12 existuje $\beta \in U$ tak, že $V = T(\beta)$. Potom ale

$$k = [V : T] = \deg m_{\beta,T} \leq \deg f_\beta \leq n,$$

což je spor.

- Opět podle Věty 3.12 existuje $\alpha \in U$ tak, že $U = T(\alpha)$. Platí

$$n \leq |\operatorname{Aut}_T(U)| \leq [U : T] = \deg m_{\alpha,T} \leq \deg f_\alpha \leq |G| = n.$$

- Proto platí, že $n = [U : T] = [U : T]_S$ a tedy $G = \operatorname{Gal}(U, T)$. □

Lemma 3.19 (II.3.8)

Bud' $T \leq U$ Galoisovo rozšíření. Potom

$$T = \text{Fix}(U, \text{Gal}(U, T)).$$

Důkaz.

- Položme $S = \text{Fix}(U, \text{Gal}(U, T))$.
- Podle Lemmatu 3.18 je $S \leq U$ separabilní rozšíření stupně $n = |\text{Gal}(U, T)|$.
- $T \leq U$ je normální a separabilní, proto $[U : T] = |\text{Gal}(U, T)| = n$. Odtud $[U : T] = [U : S]$.
- Podle Lemmatu 3.17 je $T \leq S$ a tedy $T = S$. □

Lemma 3.20 (II.3.9)

Bud' U těleso a necht' $G \leq \text{Aut}(U)$. Potom pro každé $f \in \text{Aut}(U)$ platí

$$\text{Fix}(U, fGf^{-1}) = f(\text{Fix}(U, G)).$$

Důkaz.

- Pro každé $u \in \text{Fix}(U, G)$ a $g \in G$ platí

$$fgf^{-1}(f(u)) = fg(u) = f(u),$$

odkud plyne, že $f(\text{Fix}(U, G)) \subseteq \text{Fix}(U, fGf^{-1})$.

- Podobně platí

$$f^{-1}(\text{Fix}(U, fGf^{-1})) \subseteq \text{Fix}(U, f^{-1}fGf^{-1}f) = \text{Fix}(U, G),$$

odkud $\text{Fix}(U, fGf^{-1}) \subseteq f(\text{Fix}(U, G))$.



Definice

- Mějme uspořádané množiny A, B . Zobrazení $\alpha: A \rightarrow B$ nazveme **anti-monotonní** jestliže

$$a_1 \leq a_2 \implies \alpha(a_1) \geq \alpha(a_2)$$

pro všechna $a_1, a_2 \in A$.

- Dvojice (α, β) anti-monotónních zobrazení $\alpha: A \rightarrow B$ a $\beta: B \rightarrow A$ tvoří **Galoisovu korespondenci** je-li splněno:

$$a \leq \alpha\beta\alpha(a), \quad b \leq \beta\alpha\beta(b)$$

Lemma 3.21 (II.4.1)

Zobrazení α, β poskytují vzájemně inverzní bijekce množin $\beta(B)$ a $\alpha(A)$.

Důsledek 3.22 (II.4.2)

- *Jsou-li α, β surjektivní, jsou bijekcemi.*
- *Tvoří-li navíc A, B svazy, jsou α, β vzájemně inverzními anti-izomorfismy těchto svazů.*

Věta 3.23 (Hlavní věta Galoisovy teorie – II.4.3)

- ❶ *Nechť U je Galoisovo rozšíření tělesa T . Potom zobrazení určené předpisy*

$$V \mapsto \text{Gal}(U, V) \text{ a } G \mapsto \text{Fix}(U, G)$$

tvoří anti-izomorfismus svazu všech meztěles rozšíření $T \leq U$ a všech podgrup grupy $\text{Gal}(U, T)$.

- ❷ *Normální rozšíření T odpovídají normálním podgrupám grupy $\text{Gal}(U, T)$.*
- ❸ *Je-li $T \leq V(\leq U)$ normální rozšíření, platí*

$$\text{Gal}(V, T) \simeq \text{Gal}(U, T) / \text{Gal}(U, V).$$

Důkaz Věty 3.23.

- Obě zobrazení surjektivní jsou antimonotónní. K důkazu ① stačí ověřit, že jsou surjektivní. To plyne z Lemmat 3.18 a 3.17.
- Ukážeme ②. Buď $T \leq V \leq U$ takové, že $T \leq V$ je normální. Pro $g \in \text{Gal}(U, T)$ je potom $g^{-1}(V) = V$.
- Proto pro libovolná $h \in \text{Gal}(U, V)$ a $v \in V$ platí $ghg^{-1}(v) = gg^{-1}(v) = v$ a tedy $ghg^{-1} \in \text{Gal}(U, V)$. To znamená, že $\text{Gal}(U, V) \trianglelefteq \text{Gal}(U, T)$.
- Buď $G \trianglelefteq \text{Gal}(U, T)$. Pro libovolné $f \in \text{Gal}(U, T)$ pak máme podle Lemmatu 3.20 $f(\text{Fix}(U, G)) = \text{Fix}(U, fGf^{-1}) = \text{Fix}(U, G)$.
- Z normality U nad T pak plyne normalita $\text{Fix}(U, G)$ nad T .
- Přiřazení $f \mapsto f \upharpoonright V$ určuje homomorfismus z $\text{Gal}(U, T)$ na $\text{Gal}(V, T)$ jehož jádrem je právě grupa $\text{Gal}(U, V)$. Odtud ③.



Lemma 3.24

Pro těleso T značme T^ multiplikativní grupu jeho nenulových prvků. Je-li G konečná podgrupa grupy T^* , potom je G cyklická.*

Lemma 3.25

Nechť $T \leq U$ rozšíření, kde U je rozkladové nadtěleso polynomu $x^n - 1$. Potom je grupa $\text{Gal}(U, T)$ Abelova.

Důkaz.

- Kořeny polynomu f tvoří konečnou podgrupu grupy U^* , která je tedy cyklická. Buď α její generátor.
- Pro každé $g \in \text{Gal}(U, T)$ je $g(\alpha) = \alpha^j$ a j jednoznačně určuje g .
- Pro $g, h \in \text{Gal}(U, T)$, $h(\alpha) = \alpha^k$, platí

$$gh(\alpha) = g(\alpha^k) = (\alpha^j)^k = (\alpha^k)^j = h(\alpha^j) = hg(\alpha)$$

a vidíme, že grupa $\text{Gal}(U, T)$ je Abelova.



Lemma 3.26

Bud' T těleso, $a \in T$ a necht' U je rozkladové nadtěleso polynomu $x^n - a$. Pokud T obsahuje rozkladové nadtěleso polynomu $x^n - 1$, je grupa $\text{Gal}(U, T)$ Abelova.

Důkaz.

- Bud' α kořen polynomu $x^n - a$.
- Ostatní kořeny polynomu $x^n - a$ jsou tvaru $\beta\alpha$, kde β je kořen $x^n - 1$.
- T -automorfismy tělesa U jsou určeny přiřazeními $\alpha \mapsto \beta\alpha$.
- Necht' $\varphi: \alpha \mapsto \beta\alpha$ a $\psi: \alpha \mapsto \gamma\alpha$ jsou dva z nich.
- Potom

$$\varphi\psi(\alpha) = \varphi(\gamma\alpha) = \gamma\varphi(\alpha) = \gamma\beta\alpha = \beta\gamma\alpha = \beta\psi(\alpha) = \psi(\beta\alpha) = \psi\varphi(\alpha).$$

- Proto $\varphi\psi = \psi\varphi$ a grupa $\text{Gal}(U, T)$ je komutativní.



Definice

- Grupa G je **řešitelná**, jestliže existuje řetězec

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

splňující $G_i \triangleleft G_{i+1}$ a G_{i+1}/G_i je Abelova.

- Posloupnost $G_0, \dots, G_n$ nazveme **kompoziční řadou** grupy G .

Lemma 3.27

Je-li H normální podgrupa grupy G , je grupa G řešitelná právě když jsou řešitelné grupy H a G/H .

Věta 3.28

Pro $n > 4$ není symetrická grupa $\mathbf{S}_n$ řešitelná.

Lemma 3.29

Bud' $T \leq U$, kde U je rozkladové nadtěleso polynomu $x^n - a$ nad T . Pokud charakteristika tělesa T nedělí n , je $\text{Gal}(U, T)$ řešitelná.

Důkaz.

- Derivace polynomu $x^n - a$ je nx^{n-1} . Protože charakteristika T nedělí n , je tato derivace nenulová, nesoudělná s f , a tedy f nemá vícenásobné kořeny.
- Necht' $\alpha_1, \dots, \alpha_n$ jsou všechny kořeny polynomu f . Předpokládejme, že $\alpha_1 \neq 0$.
- Potom tvoří zlomky α_i/α_1 právě všechny kořeny polynomu $x^n - 1$ a ten se tedy v U rozkládá.
- Bud' V rozkladové nadtěleso $x^n - 1$. Je $T \leq V \leq U$ a tato rozšíření jsou normální.



Dokončení důkazu lemmatu 3.29.

- Podle Lemmatu 3.26 je grupa $\text{Gal}(U, V)$ Abelova.
- Podle lemmatu 3.25 je grupa $\text{Gal}(V, T)$ Abelova.
- Podle Věty 3.23 je $\text{Gal}(U, V) \trianglelefteq \text{Gal}(U, T)$ a platí

$$\text{Gal}(V, T) \simeq \text{Gal}(U, T)/\text{Gal}(U, V).$$

- Podle Lemmatu 3.27 je pak grupa $\text{Gal}(U, T)$ řešitelná. □

Definice

Rozšíření $T \leq U$ nazveme **radikálové** jestliže $U = T(\alpha_1, \dots, \alpha_m)$, kde pro každé j existuje $n_j \in \mathbb{N}$ takové, že $\alpha_j^{n_j} \in T(\alpha_1, \dots, \alpha_{j-1})$.

Lemma 3.30

Normální uzávěr radikálového rozšíření je opět radikálové rozšíření.

Důkaz.

- Bud' $T \leq T(\alpha_1, \dots, \alpha_m)$ radikálové a U jeho normální uzávěr.
- Důkaz provedeme indukcí podle m . Označme ještě V normální uzávěr rozšíření $T \leq T(\alpha_1, \dots, \alpha_{m-1})$. Podle indukčního předpokladu je rozšíření $T \leq V$ radikálové.
- Potom je rozšíření $V \leq V(\alpha_m)$ radikálové a U je jeho normální uzávěr a tedy vznikne přidáním všech kořenů minimálního polynomu prvku α_m nad V .
- Protože $\alpha_m^{n_m} \in V$, platí totéž pro každý z těchto kořenů a rozšíření $V \leq U$ a tedy také $T \leq U$ jsou radikálová.



Věta 3.31

Je-li $T \leq U = T(\alpha_1, \dots, \alpha_n)$, kde $\alpha_j^{n_j} \in T(\alpha_1, \dots, \alpha_{j-1})$, normální radikálové rozšíření a charakteristika T nedělí n_j , je grupa $\text{Gal}(U, T)$ řešitelná.

Důkaz.

- Tvzení ukážeme indukcí podle n . Nechť $\alpha_1^{n_1} = a \in T$ a uvažme rozkladové nadtěleso V polynomu $x^{n_1} - a$ nad T .
- Potom je $U = V(\alpha_2, \dots, \alpha_n)$ normální radikálové rozšíření a dle indukčního předpokladu je grupa $\text{Gal}(U, V)$ řešitelná.
- Podle Lemmatu 3.29 je grupa $\text{Gal}(V, T)$ řešitelná a podle Věty 3.23 je $\text{Gal}(U, V) \trianglelefteq \text{Gal}(U, T)$ a platí

$$\text{Gal}(V, T) \simeq \text{Gal}(U, T) / \text{Gal}(U, V).$$

- Podle Lemmatu 3.27 je pak grupa $\text{Gal}(U, T)$ řešitelná. □

Definice

Necht' T je těleso, $f \in T[x]$ a U rozkladové nadtěleso f . Řekneme, že polynom f je **řešitelný pomocí radikálů** je-li U obsaženo v nějakém radikálovém rozšíření T .

Definice

Necht' T je těleso, $f \in T[x]$ a U rozkladové nadtěleso f . Galoisovou grupou polynomu f (nad T) rozumíme grupu $\text{Gal}(U, T)$.

Věta 3.32

Bud' T těleso stupně 0. Je-li polynom $f \in T[x]$ řešitelný pomocí radikálů, je jeho Galoisova grupa řešitelná.

Důkaz.

- Označme U rozkladové nadtěleso polynomu f nad T . Podle předpokladu je $T \leq U \leq V$ pro nějaké radikálové rozšíření V tělesa T .
- Podle Lemmatu 3.30 lze předpokládat, že rozšíření $T \leq V$ je normální.
- Podle Věty 3.31 je Galoisova grupa $\text{Gal}(V : T)$ řešitelná.
- Rozšíření $T \leq U$ je normální a tedy podle Věty 3.23 je

$$\text{Gal}(U, T) \simeq \text{Gal}(V, T) / \text{Gal}(V, U).$$

- Podle Lemmatu 3.27 je grupa $\text{Gal}(U, T)$ řešitelná.



Definice

Podgrupa G symetrické grupy $\mathbf{S}_n$ se nazývá **tranzitivní** jestliže pro každé $i, j \in \{1, \dots, n\}$ existuje $g \in G$ tak, že $g(i) = j$.

Lemma 3.33

Bud' p prvočíslo a G tranzitivní podgrupa grupy $\mathbf{S}_p$. Obsahuje-li G transpozici, je rovna $\mathbf{S}_p$.

Věta 3.34

Bud' $f \in \mathbb{Q}[x]$ nerozložitelný polynom prvočíselného stupně p . Má-li f právě dva nereálné kořeny, je jeho Galoisova grupa nad $\mathbb{Q}$ izomorfní $\mathbf{S}_p$.

Věta 3.35

Rovnice $x^5 - np x + p = 0$ pro $n > 1$ není řešitelná pomocí radikálů.

- Uvažme rozšíření $T \leq U$ konečného stupně n a zvolme bázi $\mathbf{e} = (e_1, e_1, \dots, e_n)$ prostoru U nad T .
- Prvek $\alpha \in U$ určuje endomorfismus tělesa U daný předpisem $u \mapsto \alpha u$.
- Matici tohoto endomorfismu vzhledem k bázi $\mathbf{e}$ označíme $\mathbf{M}_{\mathbf{e}}(\alpha)$.

Definice

- **Normou** prvku α v U nad T nazveme hodnotu $N_{U|T}(\alpha) = \det \mathbf{M}_{\mathbf{e}}(\alpha)$.
- **Stopou** prvku α v U nad T nazveme hodnotu $\text{Tr}_{U|T}(\alpha) = \text{tr } \mathbf{M}_{\mathbf{e}}(\alpha)$ (tj., součet prvků na diagonále).

- Charakteristický polynom c_α matice $\mathbf{M}_e(\alpha)$ nezávisí na volbě báze e a je roven

$$c_\alpha = \det(x\mathbf{I}_n - \mathbf{M}_e(\alpha)) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0.$$

- Z definice plyne, že $\text{Tr}_{U|T}(\alpha) = -c_{n-1}$ a $N_{U|T}(\alpha) = (-1)^n c_0$.
- Proto hodnoty $N_{U|T}(\alpha)$ a $\text{Tr}_{U|T}(\alpha)$ nezávisí na volbě báze.

Tvrzení 4.1 (II.5.1)

Bud' $T \leq U$ rozšíření konečného stupně n a necht' $\alpha \in U$. Potom

- $c_\alpha = m_{\alpha, T}^d$, kde $d = [U : T(\alpha)]$;
- $N_{U|T}(\alpha) = (-1)^n c_0 = (-1)^n a_0^d = (N_{T(\alpha)|T}(\alpha))^d$;
- $\text{Tr}_{U|T}(\alpha) = -c_{n-1} = d \text{Tr}_{T(\alpha)|T}(\alpha)$;

Tvrzení 4.2 (II.5.2)

Bud' $T \leq U$ separabilní rozšíření a $\alpha \in U$. Potom

- ① $c_\alpha = \prod (x - g(\alpha)),$
- ② $N_{U|T}(\alpha) = \prod g(\alpha),$
- ③ $\text{Tr}_{U|T}(\alpha) = \sum g(\alpha),$

kde g probíhá všechny T -homomorfismy z U do jeho algebraického uzávěru.

Pro $\alpha, \beta \in U$ je

- $N_{U|T}(\alpha\beta) = N_{U|T}(\alpha)N_{U|T}(\beta)$;
- $\text{Tr}_{U|T}(\alpha + \beta) = \text{Tr}_{U|T}(\alpha) + \text{Tr}_{U|T}(\beta)$;

Máme tak grupové homomorfismy $N_{U|T}: (U^*, \cdot) \rightarrow (T^*, \cdot)$ a $\text{Tr}_{U|T}: (U, +) \rightarrow (T, +)$.

Tvrzení 4.3

Nechť $T \leq U \leq V$ jsou separabilní rozšíření konečného stupně. Potom

- 1 $\text{Tr}_{V|T} = \text{Tr}_{U|T} \circ \text{Tr}_{V|U}$;
- 2 $N_{V|T} = N_{U|T} \circ N_{V|U}$;

Definice

Bud' $T \leq U$ separabilní rozšíření stupně n a $\alpha_1, \alpha_2, \dots, \alpha_n \in U$.
Definujeme **diskriminant** jako $\Delta(\alpha_1, \alpha_2, \dots, \alpha_n) = \det(\text{Tr}_{U|T}(\alpha_i \alpha_j))$.

Lemma 4.4 (II.5.5)

*Bud' W algebraický uzávěr U a $\text{hom}_T(U, W) = \{g_1, g_2, \dots, g_n\}$.
Položme $\mathbf{M} = (g_i(\alpha_j))$. Potom $\mathbf{M}\mathbf{M}^T = (\text{Tr}_{U|T}(\alpha_i \alpha_j))$ a tedy
 $\Delta(\alpha_1, \alpha_2, \dots, \alpha_n) = \det \mathbf{M}^2$.*

Tvrzení 4.5 (II.5.6)

- Zobrazení $(\alpha, \beta) \mapsto \text{Tr}_{U|T}(\alpha\beta)$ je nedegenerovanou symetrickou bilineární formou $U \times U \rightarrow T$;
- Jsou-li $\alpha_1, \alpha_2, \dots, \alpha_n$ a $\beta_1, \beta_2, \dots, \beta_n$ dvě báze U nad T a $\mathbf{P} = (p_{ij})$, kde $\beta_j = \sum p_{ij} \alpha_i$, platí
$$\Delta(\beta_1, \beta_2, \dots, \beta_n) = (\det \mathbf{P})^2 \Delta(\alpha_1, \alpha_2, \dots, \alpha_n) \neq 0.$$

Lemma 4.6 (II.5.4)

$$\begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ \vdots & \vdots & \dots & \vdots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \dots & \alpha_n^{n-1} \end{vmatrix} = \prod_{i < j} (\alpha_j - \alpha_i).$$

Tvzení 4.7 (II.5.7)

Bud' $T \leq T(\gamma)$ separabilní rozšíření stupně n . Potom

- ① $\Delta(1, \gamma, \dots, \gamma^{n-1}) = \prod_{g \neq h} (g(\gamma) - h(\gamma))^2$, kde g, h probíhají všechny homomorfismy z tělesa $T(\gamma)$ do jeho algebraického uzávěru;
- ② $\Delta(1, \gamma, \dots, \gamma^{n-1}) = (-1)^{\binom{n}{2}} N_{U|T}(m'_{\gamma, T}(\gamma)).$

Lemma 4.8 (II.6.1)

Bud' $T \leq U$ rozšíření. Pro každou podmnožinu $M \subseteq U$ platí, že $T(M)$ sestává právě ze všech prvků tvaru $p(\alpha_1, \alpha_2, \dots, \alpha_n)/q(\beta_1, \beta_2, \dots, \beta_n)$, kde $q(\beta_1, \beta_2, \dots, \beta_n) \neq 0$, $p, q \in T[x_1, x_2, \dots, x_n]$ a $\alpha_i, \beta_i \in M$.

Definice

- 1 Podmnožinu $M \subseteq U$ nazveme **algebraicky nezávislou** (nad T) jestliže $p(\alpha_1, \alpha_2, \dots, \alpha_n) \neq 0$ pro každé po dvou různé $\alpha_1, \alpha_2, \dots, \alpha_n$ a každý polynom $p(x_1, x_2, \dots, x_n) \in T[x_1, x_2, \dots, x_n]$.
- 2 Prvek $\beta \in U$ nazveme **algebraicky závislý na M** (nad T) je-li algebraický nad $T(M)$.

Lemma 4.9 (II.6.2)

Množina $M \subseteq U$ je algebraicky nezávislá právě když žádné $\beta \in M$ není algebraicky závislé na $M \setminus \{\beta\}$.

Definice

Necht' M_1, M_2 jsou podmnožiny U . Množina M_2 je **algebraicky závislá** na množině M_1 (nad T) jestliže je každý prvek z M_2 algebraicky závislý na M_1 .

Lemma 4.10 (II.6.3)

Necht' M_1, M_2, M_3 jsou podmnožiny U . Je-li M_3 algebraicky závislá na M_2 a M_2 algebraicky závislá na M_1 , je M_3 algebraicky závislá na M_1 .

Definice

Podmnožiny M_1, M_2 tělesa U nazveme **algebraicky ekvivalentní** (nad T) jestliže je M_1 algebraicky závislá na M_2 a zároveň M_2 algebraicky závislá na M_1 .

Lemma 4.11 (II.6.4)

Bud' M podmnožina U . Každou algebraicky nezávislou podmnožinu M_0 množiny M lze rozšířit na algebraicky nezávislou podmnožinu M_1 množiny M , která je s M algebraicky ekvivalentní.

Lemma 4.12 (O výměně - II.6.5)

Nechť M_1, M_2 jsou podmnožiny U takové, že M_1 je algebraicky nezávislá a algebraicky závislá na M_2 . Potom pro každé $\alpha \in M_1 \setminus M_2$ existuje $\beta \in M_2 \setminus M_1$ tak, že množina $(M_2 \setminus \{\beta\}) \cup \{\alpha\}$ je algebraicky ekvivalentní M_2 .

Tvrzení 4.13 (II.6.6)

Nechť $T \leq U$ a M_1, M_2 jsou podmnožiny U takové, že M_1 je algebraicky nezávislá nad T a je algebraicky závislá na M_2 na T . Potom je mohutnost M_1 nejvýše rovna mohutnosti M_2 .

Důsledek 4.14 (II.6.7)

Každé dvě algebraicky nezávislé algebraicky ekvivalentní podmnožiny U mají stejnou mohutnost.

Definice

Bud' $T \leq U$ rozšíření.

- Algebraicky nezávislou množinu, která je algebraicky ekvivalentní U nazveme **transcendentní bazí**.
- Mohutnost transcendentní báze (podle Tvzení 4.13 ji mají všechny stejné) nazveme **stupněm transcendence** U nad T a označíme $[U : T]_{\text{tr}}$.

Tvrzení 4.15 (II.6.8)

Nechť $T \leq U \leq V$ je posloupnost rozšíření. Potom platí

$$[V : T]_{\text{tr}} = [V : U]_{\text{tr}} + [U : T]_{\text{tr}}.$$

- Bud' R okruh. Okruh S spolu s (okruhovým) homomorfismem $f: R \rightarrow S$ nazveme **R -algebrou**.
- Zobrazení f nazveme **strukturní homomorfismus**.
- Níže budeme vždy předpokládat, že R -algebry jsou komutativní.

Lemma 5.1 (II.7.1)

Bud' S komutativní R -algebra se strukturním homomorfismem $f: R \rightarrow S$. Potom je S jako R -algebra konečně generovaná právě když lze f rozšířit na okruhový epimorfismus $R[x_1, \dots, x_n] \rightarrow S$.

Důsledek 5.2 (II.7.2)

Je-li R noetherovský, je také každá konečně generovaná R -algebra noetherovská.

Tvrzení 5.3 (II.7.3)

Nechť $S_0 \leq S_1$ jsou dvě R -algebry. Jestliže množina A generuje S_0 jako R -algebru a množina B generuje S_1 jako S_0 -algebru, potom sjednocení $A \cup B$ generuje S_1 jako R -algebru.

Důsledek 5.4 (II.7.4)

Bud' R noetherovský a $S_0 \leq S_1 \leq S_2$ posloupnost R -algeber, že

- S_0 je konečně generovaná R -algebra;*
- S_2 je konečně generovaný S_0 -modul;*

Potom je S_1 konečně generovanou R -algebrou.

Tvrzení 5.5 (II.7.5)

Bud' R noetherovský okruh. Necht' $S_1 \leq S_2$ jsou R -algebry splňující:

- S_2 je konečně generovaný S_1 -modul;*
- S_2 je konečně generovaná R -algebra;*

Potom je také S_1 konečně generovanou R -algebrou.

Důkaz.

- Budeme hledat množinu S_0 tak, aby byly splněny předpoklady Důsledku 5.4.
- Bud' M množina generátorů S_2 jako S_1 -modulu a C množina generátorů S_2 jako R -algebry.
- Pro každé $c \in C$ a $m \in M$ necht'

$$cm = \sum_{m' \in M} s_{cm, m'} m',$$

kde $s_{cm, m'}$ jsou prvky S_1 .



Dokončení důkazu Tvzení 5.5.

- Označme S_0 R -algebru generovanou prvky $s_{cm,m'}$ a buď S_3 S_0 -modul generovaný množinou M . Ukážeme, že $S_3 = S_2$.
- Označme $C^* = \{c_1 c_2 \cdots c_k \mid k \in \mathbb{N} \text{ a } c_i \in C\}$. Stačí ukázat, že $C^* \subseteq S_3$.
- Protože $1 \in M$, je $c = \sum s_{c1,m'} m' \in S_3$ a tedy $C \subseteq S_3$.
- Mějme $c_1, c_2, \dots, c_k \in C$ a předpokládejme, že $a = c_1 c_2 \cdots c_{k-1} \in S_3$.
- Potom je $a = \sum s_m m$, pro nějaké $s_m \in S_0$.
- Odtud $c_1 c_2 \dots c_k = a c_k = \sum_m s_m c_k m =$

$$= \sum_m s_m \left(\sum_{m'} s_{c_k m, m'} m' \right) = \sum_{m'} \underbrace{\left(\sum_m s_m s_{c_k m, m'} \right)}_{\in S_0} m' \in S_3.$$



Lemma 5.6 (II.7.6)

Bud' T těleso. Okruh $T(x_1, \dots, x_n)$ není jako T -algebra konečně generovaný.

Důkaz.

- Pro spor předpokládejme, že $T(x_1, \dots, x_n)$ je konečně generováno prvky $g_1, \dots, g_k$.
- Bud' $g_i = p_i/q_i$, kde $p_i, q_i \in T[x_1, \dots, x_n]$.
- Alespoň jeden z polynomů q_i je nenulového stupně, jinak by $g_1, \dots, g_k \in T[x_1, \dots, x_n]$ a T -algebry $T[x_1, \dots, x_n]$ a $T(x_1, \dots, x_n)$ by se rovnaly.
- Potom lze každý prvek $T(x_1, \dots, x_n)$ vyjádřit ve tvaru $a/(q_1^{\alpha_1} \cdots q_k^{\alpha_k})$ pro nějaké $a \in T[x_1, \dots, x_n]$ a $\alpha_i \in \mathbb{N}_0$.
- Speciálně $(q_1 \cdots q_n + 1)^{-1} = a/(q_1^{\alpha_1} \cdots q_k^{\alpha_k})$, odkud $q_1^{\alpha_1} \cdots q_k^{\alpha_k} = a(q_1 \cdots q_n + 1)$.
- Proto $(q_1 \cdots q_n + 1) \mid q_1^{\alpha_1} \cdots q_k^{\alpha_k}$ což je **spor**. □

Definice

Bud' T těleso. Konečně generovanou T -algebru budeme nazývat **afinní T -algebrou**.

Lemma 5.7 (II.7.7)

Je-li afinní T -algebra tělesem, je rozšířením konečného stupně.

Lemma 5.8 (II.7.8)

Bud' T těleso a $\alpha_1, \dots, \alpha_n \in T$. Potom

- ❶ *ideál $M = (x_1 - \alpha_1, \dots, x_n - \alpha_n)$ je v $T[x_1, \dots, x_n]$ maximální.*
- ❷ *polynom $f \in T[x_1, \dots, x_n]$ leží v ideálu $M = (x_1 - \alpha_1, \dots, x_n - \alpha_n)$ právě když $f(\alpha_1, \dots, \alpha_n) = 0$.*

Důkaz Lemmatu 5.8.

- Buď $f \in T[x_1, \dots, x_n]$. Položme $f_n = f$.
- Použijeme-li algoritmus pro dělení polynomů se zbytkem, dostaneme: $f_n = g_n(x_n - \alpha_n) + f_{n-1}$, kde $g_n \in T[x_1, \dots, x_n]$ a $f_{n-1} \in T[x_1, \dots, x_{n-1}]$.
- Podobně dostaneme $f_{n-1} = g_{n-1}(x_{n-1} - \alpha_{n-1}) + f_{n-2}$, kde $g_{n-1} \in T[x_1, \dots, x_{n-1}]$ a $f_{n-2} \in T[x_1, \dots, x_{n-2}]$.
- Postupujeme-li podobně dále, dostaneme nakonec, že $f = \sum g_i(x_i - \alpha_i) + f_0$, kde $f_0 \in T$.
- Odtud snadno plyne dokazované.



Věta 5.9 (Hilbertova o nulách – II.7.9)

Nechť K je algebraicky uzavřené těleso a $S = K[x_1, \dots, x_n]$. Potom

- ① *Ideál M okruhu S je maximální právě když existují $\alpha_1, \dots, \alpha_n$ tak, že*

$$M = (x_1 - \alpha_1, \dots, x_n - \alpha_n);$$

- ② *Pro každý vlastní ideál J okruhu S je množina*

$$\mathbb{V}(J) = \{(\alpha_1, \dots, \alpha_n) \mid f(\alpha_1, \dots, \alpha_n) = 0 \text{ pro všechna } f \in J\}$$

neprázdná a platí, že

$$\sqrt{J} = \{g \mid g(\alpha_1, \dots, \alpha_n) = 0 \text{ pro všechna } g \in \mathbb{V}(J)\}.$$

Důsledek 5.10

Bud' K algebraicky uzavřené těleso. Potom je každý prvoideál okruhu $K[x_1, \dots, x_n]$ průnikem maximálních ideálů.

Důkaz Věty 5.9.

- Buď M maximální ideál okruhu S a $\pi: S \rightarrow S/M$ kanonická projekce.
- Podle Tvzení 5.7 je rozšíření $K \leq S/M$ konečného stupně, tedy algebraické. Protože je K algebraicky uzavřené, je $K = S/M$.
- Položme $\pi(x_i) = \alpha_i$. Potom $x_i - \alpha_i \in M$ a tedy

$$(x_1 - \alpha_1, \dots, x_n - \alpha_n) \subseteq M.$$

- Podle Lemmatu 5.8 je $(x_1 - \alpha_1, \dots, x_n - \alpha_n)$ maximální a tedy rovno M .
- Buď J ideál S . Potom, opět podle Lemmatu 5.8,

$$(\alpha_1, \dots, \alpha_n) \in \mathbb{V}(J) \text{ právě když } J \subseteq (x_1 - \alpha_1, \dots, x_n - \alpha_n).$$



Pokračování důkazu Věty 5.9.

- Zřejmě $\mathbb{V}(J) = \mathbb{V}(\sqrt{J})$. Zbývá ukázat, že pokud $f(\alpha) = 0$ pro každé $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{V}(J)$, tak $f \in \sqrt{J}$.
- Uvažme okruh $U = S[y]$ a v něm ideály $A = JU$ a $B = (1 - fy)U$.
- Pro spor předpokládejme, že ideály A, B nejsou komaximální. Potom existují $\alpha \in K^n$ a $\beta \in K$ tak, že $f(\alpha) = 0$ a zároveň $1 - f(\alpha)\beta = 0$ což je spor.
- Okruh S je noetherovský a tedy ideál J je generován konečně mnoha polynomy, $g_1, \dots, g_k$.
- Protože $A + B = S[y]$, existují $h_1, \dots, h_k$ a $h \in S[y]$ tak, že

$$1 = \sum h_i g_i + (1 - fy)h.$$



Dokončení důkazu Věty 5.9.

- Uvažme homomorfismus $\phi: S[y] \rightarrow K(x_1, \dots, x_n, y)$ rozšiřující identitu na S o dosazení $y \mapsto 1/f$. (Lze předpokládat $f \neq 0$).
- Dostaneme

$$1 = \sum \phi(h_i)g_i + (1 - \frac{f}{f})h = \sum \phi(h_i)g_i.$$

- Obrazy $\phi(h_i)$ jsou zlomky tvaru t_i/f^{γ_i} , kde $t_i \in S$.
- Vynásobíme-li společným jmenovatelem, dostaneme

$$f^\delta = \sum f^{\varepsilon_i} t_i g_i.$$

- Dostáváme $f^\delta \in J$, odkud plyne, že $f \in \sqrt{J}$.



Definice

- Pro $J \subseteq T[x_1, \dots, x_n]$ položme

$$\mathbb{V}(J) = \{\alpha \in T^n \mid f(\alpha) = 0 \text{ pro všechna } f \in J\}.$$

Podmnožiny T^n tvaru $\mathbb{V}(J)$, kde $J \subseteq T[x_1, \dots, x_n]$ se nazývají **algebraické**.

- Pro $C \subset T^n$ položme naopak

$$\mathbb{I}(C) = \{f \in T[x_1, \dots, x_n] \mid f(\alpha) = 0 \text{ pro všechna } \alpha \in C\}.$$

Podmnožiny $T[x_1, \dots, x_n]$ tvaru $\mathbb{I}(C)$ jsou ideály tohoto okruhu. Tyto ideály nazývám **uzavřené**.

Lemma 5.11 (V.1.1)

1

- $\mathbb{I}(\bigcup C_i) = \bigcap \mathbb{I}(C_i);$
- $\mathbb{V}(\bigcup J_i) = \bigcap \mathbb{V}(J_i);$

2

- $C' \subseteq C \implies \mathbb{I}(C) \subseteq \mathbb{I}(C');$
- $J' \subseteq J \implies \mathbb{V}(J) \subseteq \mathbb{V}(J');$

3

- $J \subseteq \mathbb{IV}(J);$
- $C \subseteq \mathbb{VI}(C);$

Důsledek 5.12 (V.1.2)

Zobrazení $\mathbb{I}$ a $\mathbb{V}$ tvoří Galoisovu korespondenci mezi podmnožinami K^n a podmnožinami $K[x_1, \dots, x_n]$.

Lemma 5.13 (V.1.3)

$$\mathbb{V}(J_1 J_2) = \mathbb{V}(J_1) \cup \mathbb{V}(J_2).$$

Důsledek 5.14

*Algebraické množiny tvoří systém uzavřených množin v topologii na K^n . Tato topologie se nazývá **Zariského** topologie.*

Definice

Algebraická množina je nerozložitelná pokud nelze vyjádřit jako sjednocení vlastních algebraických podmnožin.

Lemma 5.15 (V.1.4)

Každou algebraickou množinu C lze jednoznačně vyjádřit ve tvaru $C = \bigcup_{i=1}^n C_i$, kde C_i jsou nerozložitelné algebraické množiny a žádnou z množin C_i nelze vynechat.

Lemma 5.16 (V.1.5)

Neprázdná algebraická množina je nerozložitelná právě když je $\mathbb{I}(C)$ prvoideál.

Věta 5.17 (V.1.6)

Bud' T algebraicky uzavřené těleso. Potom pro každý vlastní ideál J okruhu $S = T[x_1, \dots, x_n]$ platí, že

$$\mathbb{IV}(J) = \sqrt{J} = \bigcap \{M \mid M \text{ je maximální ideál } S \text{ a } J \subseteq M\}.$$

Část III

Celistvost a Dedekindovy obory

Tvrzení 6.1 (III.2.2)

Nechť $R \leq S$ jsou okruhy a I je ideál R . Nechť M je S -modul, který je jako R -modul generovaný n -ticí prvků. Platí-li pro $s \in S$, že $sM \subseteq IM$, existují $a_i \in I^{n-i}$ tak, že

$$s^n + a_{n-1}s^{n-1} + \cdots + a_1s + a_0 \in \text{Ann}(M).$$

Důkaz.

- Nechť $g_1, \dots, g_n$ jsou generátory R -modulu M .
- Uvažme matici $\mathbf{B} = (b_{ij})$ takovou, že $sg_i = \sum b_{ij}g_j$.
- Položme $\mathbf{C} = s\mathbf{I} - \mathbf{B}$. Potom $\mathbf{C}\mathbf{g}^T = 0$, kde $\mathbf{g} = (g_1, \dots, g_n)$.
- Buď $\mathbf{D}$ matice adjungovaná k matici $\mathbf{C}$. Potom $\mathbf{DC} = (\det \mathbf{C})\mathbf{I}$, odkud $\det \mathbf{C} \in \text{Ann}(M)$.
- Z definice determinantu dostaneme, že $\det \mathbf{C}$ je polynom hledaného tvaru.



Definice

Necht' $R \leq S$ jsou okruhy.

- 1 Prvek $u \in S$ nazveme **celistvým** nad R jestliže je kořenem monického polynomu $f \in R[x]$.
- 2 Okruh S je **celistvý** nad R , je-li každý prvek z S celistvý nad R .
- 3 Homomorfismus $f: R \rightarrow S$ je **celistvý**, je-li S celistvý nad $f(R)$.

Tvrzení 6.2 (III.2.4)

Necht' $R \leq S$ jsou okruhy a $u \in S$. Potom je ekvivalentní:

- 1 u je celistvé nad R ;
- 2 $R[u]$ je konečně generovaný jako R -modul;
- 3 existuje podokruh S obsahující $R[u]$, který je konečně generovaný jako R -modul;
- 4 existuje věrný $R[u]$ -modul, který je jako R -modul konečně generovaný;

Důkaz Tvzení 6.2.

- $(1 \implies 2)$ Je-li u kořenem monického polynomu f stupně n , je R -modul $R[u]$ generován mocninami $1, u, \dots, u^{n-1}$;
- $(2 \implies 3)$ a $(3 \implies 4)$ je triviální;
- $(4 \implies 1)$ Buď M věrný $R[u]$ -modul generovaný n -prvky.
- Použijeme Tvzení 6.1 pro $s = u$, $S = R[u]$ a $I = R$. Je totiž $uM \subseteq M = RM$ a tedy $f(a) \in \text{Ann}M$ pro vhodný monický polynom z $R[x]$ stupně n .
- Protože je M věrný $R[u]$ -modul, je pak $f(u) = 0$.



Tvrzení 6.3 (III.2.5)

Buď R podokruh okruhu S . Jsou-li $u_1, \dots, u_n$ celistvé nad R je okruh $R[u_1, \dots, u_n]$ celistvý nad R a jako R -modul konečně generovaný.

Důsledek 6.4 (III.2.6)

Nechť $R \leq S$ jsou okruhy. Pak prvky $u \in S$, které jsou celistvé nad R , tvoří podokruh S obsahující R .

Tento podokruh budeme nazývat **celistvý uzávěr** R v S .

Tvrzení 6.5 (III.2.7)

Nechť $R \leq S \leq U$ jsou okruhy takové, že S je celistvé nad R . Je-li $u \in U$ celistvé nad S je celistvé již nad R .

Důsledek 6.6 (III.2.8)

Nechť $R \leq S \leq U$ jsou okruhy takové, že S je celistvé nad R . Potom jsou celistvé uzávěry okruhů R a S v U shodné.

Tvrzení 6.7 (III.2.9)

Bud' $R \leq T \leq U$, kde R je okruh a T, U jsou tělesa. Je-li $\alpha \in U$ celistvé nad R , jsou nad R celistvé také všechny kořeny a koeficienty polynomu $m_{\alpha, T}$.

Důkaz.

- Lze předpokládat, že U je rozkladovým nadtělesm $m_{\alpha, T}$. Bud' K algebraický uzávěr U .
- α je celistvé nad R a tedy je kořenem nějakého monického polynomu $c \in R[x]$. V $T[x]$ potom platí, že $m_{\alpha, T} \mid c$.
- Je-li β kořen $m_{\alpha, T}$, je pak také kořenem c , tedy je celistvý nad $R[x]$.
- Koeficienty polynomu $m_{\alpha, T}$ leží v okruhu generovaném jeho kořeny, proto jsou také celistvé.



Důsledek 6.8 (III.2.10)

Necht' $R \leq T \leq U$, kde R je okruh a $T \leq U$ je rozšíření těles konečného stupně. Je-li $\alpha \in U$ celistvé nad R , pak jsou nad R celistvé také $N_{U|T}$ a $\text{Tr}_{U|T}$.

Tvrzení 6.9 (III.2.11)

Necht' $R \leq S$ jsou obory a S je celitvé nad R . Potom je R tělesem právě když je S tělesem.

Tvrzení 6.10 (III.2.12)

Necht' $R \leq S$ jsou obory a S je celitvé nad R . Ideál P okruhu S je maximální právě když je maximální ideál $R \cap P$.

Definice

- Nechť $R \leq S$ jsou okruhy. Řekneme, že R je **celistvě uzavřené** v S je-li rovno svému celistvému uzávěru.
- Obor R je **celistvě uzavřený**, je-li celistvě uzavřený ve svém podílovém tělese.

Tvrzení 6.11 (III.3.1)

Bud' R celistvě uzavřený obor integrity a T jeho podílové těleso. Bud' $T \leq U$ algebraické rozšíření těles. Potom pro celistvé α platí, že

- 1 *minimální polynom $m_{\alpha, T}$ padne do $R[x]$;*
- 2 *je-li $T \leq U$ konečného stupně, potom $N_{U|T}(\alpha)$ a $\text{Tr}_{U|T}(\alpha)$ padnou do R .*

Tvzení 6.12 (III.2.3)

Gaussův obor je celitvě uzavřený.

Důkaz Tvzení 6.12.

- Buď R Gaussův obor, T jeho podílové těleso a necht' $u \in T$ je celitvý nad R .
- Potom $u^n + a_{n-1}u^{n-1} + \dots + a_1u + a_0 = 0$ pro vhodná $a_i \in R$.
- Buď $u = s/t$, kde $s, t \in R$ jsou nesoudělné. Dostaneme

$$s^n + a_{n-1}s^{n-1}t + \dots + a_1st^{n-1} + a_0t^n = 0,$$

odkud $s^n = -t(a_{n-1}s^{n-1} + \dots + a_1st^{n-2} + a_0t^{n-1})$.

- Pak ale $t \mid s^n$. Protože jsou s, t nesoudělné, je nutně t invertibilní. To znamená, že $u \in R$.



Uvažme nyní následující situaci:

- R je celistvě uzavřený obor integrity a T je jeho podílové těleso;
- $T \leq U$ je separabilní rozšíření těles konečného stupně n ;
- S je celistvý uzávěr R v U ;

Tvrzení 6.13 (III.3.2)

Předpokládejme, že rozšíření $T \leq U$ je navíc normální a necht' $\alpha \in S$. Potom je α invertibilní právě když je $N_{U|T}(\alpha)$ invertibilní v R .

Lemma 6.14 (III.3.3)

Pro libovolná $\alpha_1, \dots, \alpha_k \in U$ existuje $r \in R$ tak, že $r\alpha_i \in S$.

Definice

Báze $\alpha_1, \dots, \alpha_n$ tělesa U nad T se nazývá **celistvá**, jestliže $\alpha_i \in S$ a každý prvek $s \in S$ lze vyjádřit ve tvaru $s = \sum r_i \alpha_i$, kde $r_i \in R$.

Tvrzení 6.15 (III.3.4)

Nechť prvky $\alpha_1, \dots, \alpha_n \in S$ tvoří bázi U nad T . Položme $\Delta = \Delta(\alpha_1, \dots, \alpha_n)$. Potom $\Delta S \subseteq \sum R\alpha_i$.

Důkaz.

- Místo $\text{Tr}_{U|T}$ pišme jen Tr a označme $\mathbf{T} = (\text{Tr}(\alpha_i \alpha_j))$.
- Pro $\alpha \in U$ necht' $\alpha = \sum t_i \alpha_i$. Potom pro každé $\beta \in U$ platí $\text{Tr}(\alpha \beta) = \text{Tr}((\sum t_i \alpha_i) \beta) = \sum t_i \text{Tr}(\alpha_i \beta)$.
- Dostaneme, že vektor (t_i) je řešením soustavy rovnic $\mathbf{T}(x_i) = (\text{Tr}(\alpha \alpha_i))$.
- Podle Tvrzení 4.5 je $\Delta \neq 0$.
- Podle Cramerova pravidla je toto řešení tvaru r_i/Δ , kde r_i je determinant matice vzniklé nahrazením i -tého sloupce matice $\mathbf{T}$ sloupcem $(\text{Tr}(\alpha \alpha_i))$.
- Speciálně tedy $r_i \in R$ a $\Delta \alpha = \sum r_i \alpha_i$.



Důsledek 6.16 (III.3.6)

Je-li R noetherovský je také S noetherovský.

Tvrzení 6.17 (III.3.7)

Je-li R obor hlavních ideálů má U celistvou bázi.

Důkaz.

- Buď $\alpha_1, \dots, \alpha_n \in S$ báze U nad T . Podle Tvrzení 6.15 je $\Delta S \subseteq \sum R\alpha_j$.
- $\sum R\alpha_j$ je volný R modul s bazí $\alpha_1, \dots, \alpha_n$. Podle Důsledku 2.16 je ΔS volný modul hodnosti nejvýše n .
- R -moduly S a ΔS jsou izomorfní a S obsahuje volný modul $\sum R\alpha_j$ hodnosti n .
- Proto je S volný R -modul hodnosti n a tedy U má celistvou bázi.



Věta 6.18 (III.3.8)

Bud' R obor hlavních ideálů. Potom je každý nenulový konečně generovaný S -podmodul tělesa U volným R -modul hodnosti $[U : T]$.

- Uvažme případ, kdy $R = \mathbb{Z}$, $T = \mathbb{Q}$ a U je algebraické rozšíření tělesa $\mathbb{Q}$ konečného stupně.
- Bud' $\overline{\mathbb{Q}}$ algebraický uzávěr $\mathbb{Q}$ a označme $\mathbb{Z}_{\overline{\mathbb{Q}}}$ celistvý uzávěr $\mathbb{Z}$ v $\overline{\mathbb{Q}}$. Prvky $\mathbb{Z}_{\overline{\mathbb{Q}}}$ budeme nazývat **algebraická celá čísla**.
- Celistvý uzávěr okruhu $\mathbb{Z}$ v U budeme značit $\mathbb{Z}_U$. Máme $\mathbb{Z}_U = \mathbb{Z}_{\overline{\mathbb{Q}}} \cap U$.

Definice

Obor R nazveme **Dedekindův**, je-li

- 1 celistvě uzavřený;
- 2 noetherovský;
- 3 každý jeho prvoideál je maximální;

Věta 6.19 (III.4.1)

Bud' R Dedekindův obor, T jeho podílové těleso. Je-li $T \leq U$ rozšíření konečného stupně, je celistvý uzávěr S okruhu R v U také Dedekindův.

Důkaz.

- Z Důsledku 6.16 plyne, že S je noetherovský.
- Je-li P prvoideál v S , je $P \cap R$ prvoideál R .
- $P \cap R$ je neprázdný: Buď $s \in P$ a

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in R[x]$$

polynom jehož je s kořenem minimálního stupně. Pak je nutně $a_0 \neq 0$ a $a_0 \in P \cap R$.

- Protože je R Dedekindův, je $P \cap R$ maximální. Podle Tvrzení 6.10 je také P maximální.
- Podle Lemmatu 6.14 je U podílové těleso S .
- Potom je S podle Důsledku 6.6 celistvě uzavřený.



Lemma 6.20 (III.4.2)

Bud' R noetherovský okruh. Potom pro každý ideál I okruhu R existují prvoideály $P_1, \dots, P_k$ tak, že $I \supseteq P_1 \cdots P_k$.

Necht' R je Dedekindův obor a T jeho podílové těleso.

- Pro podmnožinu A tělesa T značme

$$(R :_T A) = \{t \in T \mid tA \subseteq R\}.$$

- Pro prvoideál P oboru R položíme $P^{-1} = (R :_T P)$.

Lemma 6.21 (III.4.3)

Bud' P prvoideál Dedekindova oboru R . Potom pro každý nenulový ideál I oboru R platí

$$I \subsetneq IP^{-1} = \left\{ \sum a_i p_i \mid a_i \in I, p_i \in P^{-1} \right\}.$$

Důkaz Lemmatu 6.21.

- Z definice plyne, že $R \subseteq P^{-1}$ a tedy $I \subseteq IP^{-1}$.
- Zbývá ukázat nerovnost. Nejprve ukážeme, že $R \subsetneq P^{-1}$.
- Buď a nenulový prvek P a necht' $P_1 \cdots P_k \subseteq aR$, kde P_i jsou prvoideály a k je nejmenší možné.
- Potom $P_1 \cdots P_k \subseteq P$, odkud plyne, že pro některé i je $P_i \subseteq P$.
- Je-li například $P_1 \subseteq P$, je $P_1 = P$ neboť P_1 je prvoideál a tedy maximální.
- Z minimality k plyne $P_2 \cdots P_k \not\subseteq aR$; Zvolme $b \in P_2 \cdots P_k \setminus aR$. Potom $b/a \notin R$.
- Zároveň, protože $P = P_1$, ale $a^{-1}bP \subseteq a^{-1}aR = R$, odkud plyne, že $b/a \in P^{-1}$.



Dokončení důkazu Lemmatu 6.21.

- Pro spor předpokládejme, že $IP^{-1} = I$.
- Bud' $\alpha_1, \dots, \alpha_n$ množina generátorů I a zvolme $\alpha \in P^{-1} \setminus R$.
- Uvažme translaci $I \rightarrow I$ danou přiřazením $\beta \mapsto \alpha\beta$ a bud' $\mathbf{A}$ matice této translace vzhledem k posloupnosti $\alpha = (\alpha_1, \dots, \alpha_n)$.
- Potom $(\alpha\mathbf{I} - \mathbf{A})\alpha = 0$.
- Bud' $f(x) = \det(x\mathbf{I} - \mathbf{A})$. Pak $f(\alpha)A = 0$, odkud $f(\alpha) = 0$ (jsme v oboru integrity).
- Přitom f je monický polynom nad R , tedy α je celistvý nad R .
- Protože R je Dedekindův a tedy celitvě uzavřený je nutně $\alpha \in R$
-spor.



Lemma 6.22

Bud' R Dedekindův obor a P jeho prvoideál. Potom $PP^{-1} = R$.

Věta 6.23 (III.4.4)

Každý vlastní ideál Dedekindova oboru lze jednoznačně, až na pořadí, vyjádřit jako součin prvoideálů.

Důkaz.

- Bud' R Dedekindův obor a předpokládejme, že existují ideály R , které nejsou součiny prvoideálů. Protože R je noetherovský existuje maximální takový ideálů, označme jej I .
- Bud' P prvoideál obsahující I . Potom je $IP^{-1} \subseteq PP^{-1} = R$.
- V případě rovnosti by $I = IR = IP^{-1}P = PP^{-1}P = PR = P$, což neplatí a tedy, vzhledem k Lemmatu 6.14, $I \subsetneq IP^{-1} \subsetneq R$.
- Vzhledem k maximalitě I je $IP^{-1} = P_2 \cdots P_k$, odkud $I = PP_2 \cdots P_k$
- spor.



Dokončení důkazu Věty 6.23.

- Ukážeme jednoznačnost. Necht' $I = P_1 \cdots P_k = Q_1 \cdots Q_l$.
- Potom $P_1 \cdots P_k \subseteq Q_1$ a tedy jeden z ideálů P_i je obsažen v Q_1 . Vzhledem k jeho maximalitě jsou si oba ideály rovny a tedy například $P_1 = Q_1$.
- Potom $P_1^{-1}I = P_2 \cdots P_k = Q_2 \cdots Q_l$ a jednoznačnost ukážeme indukcí.



Definice

Buď R Dedekindův obor a T jeho podílové těleso. **Lomeným ideálem** rozumíme konečně generovaný R -podmodul T .

Lemma 6.24 (III.4.5)

Nenulový R -podmodul A tělesa T je lomeným ideálem právě když existuje nenulové $c \in R$ tak, že cA je ideál R .

Věta 6.25 (III.4.6)

Lomené ideály Dedekindova oboru tvoří grupu.

Důkaz.

- Buď R Dedekindův obor a T jeho podílové těleso. Snadno nahlédneme, že lomené ideály s operací násobení tvoří komutativní monoid.
- Pro lomený ideál A položme $A^{-1} = \{t \in T \mid tA \subseteq R\}$. Zřejmě je A^{-1} podmodul T a pro nenulové $a \in A$ je $aA^{-1} \subseteq R$, odkud vidíme, že A^{-1} je lomený ideál.
- Z definice plyne, že $AA^{-1} \subseteq R$. Ukážeme, že platí rovnost. K tomu stačí ukázat, že existuje lomený ideál B tak, že $AB \supseteq R$.
- Je-li $A = P$ prvoideál, je $PP^{-1} = R$ podle Lemmatu 6.22.
- Buď A ideál a $A = \prod P_i$ jeho vyjádření v součin prvoideálů. Potom pro $B = \prod P_i^{-1}$ platí, že $AB = R$.
- Je-li A lomený ideál a $cA \subseteq R$, je pro $B = c(cA)^{-1}$, $AB = R$. □

Tvrzení 6.26 (III.4.7)

Každý lomený ideál A lze jednoznačně, až na pořadí, vyjádřit ve tvaru $A = \prod P_i^{\alpha_i}$, kde P_i jsou po dvou různé prvoideály a α_i jsou nenulová celá čísla.

- Označme $\mathcal{I}_T$ grupu všech lomených ideálů.
- Lomený ideál tvaru tR , kde $t \in T^*$ nazveme hlavní. Hlavní idály tvoří podgrupu grupy $\mathcal{I}_T$, kterou označíme $\mathcal{P}_T$.
- Položme $\mathcal{C}\ell_T = \mathcal{I}_T / \mathcal{P}_T$. Gupu $\mathcal{C}\ell_T$ nazveme **třídová grupa R** .
- Zřejmě je $\mathcal{C}\ell_T = 1$ právě když je R obor hlavních ideálů.

Důsledek 6.27 (III.4.8)

Grupa $\mathcal{I}_T$ je izomorfní volné abelově grupě s bazí tvořenou všemi prvoideály.

Definice

- Bud' V reálný vektorový prostor dimenze n . Podgrupu L Abelovy grupy $(V, +)$ nazveme **mříží**, jestliže existují lineárně nezávislé vektory $e_1, \dots, e_m$ tak, že

$$L = \left\{ \sum k_i e_i \mid k_i \in \mathbb{Z} \right\}.$$

- Je-li $m = n$, nazveme mříž **úplnou**.
- Základní buňkou** mříže L , vzhledem k lineárně nezávislé volné bázi $e_1, \dots, e_m$, nazveme množinu

$$B = \left\{ \sum \lambda_i e_i \mid 0 \leq \lambda_i < 1 \right\}.$$

Definice

Podgrupa D Abelovy grupy $(V, +)$ se nazývá **diskrétní**, je-li každý její bod izolovaný.

Lemma 7.1 (III.5.1)

Diskrétní podgrupa D vektorového prostoru V je uzavřená.

Důkaz.

- Pro spor předpokládejme, že existuje $x \in \text{Cl}(D) \setminus D$.
- Buď U libovolné okolí bodu 0. Zvolme okolí $U' \subseteq U$ tak, že pokud $a, b \in U'$, tak $a - b \in U$.
- Zvolme různé $x_1, x_2 \in x + U'$. Potom $0 \neq x_1 - x_2 \in U \cap D$.
- Vidíme, že v každém okolí bodu nula leží nějaký nenulový bod z D . Proto je 0 hromadným bodem D a tedy D není diskretní - **spor**.



Tvrzení 7.2 (III.5.2)

Nechť V je konečně dimenzionální reálný vektorový prostor. Podgrupa $(V, +)$ je diskrétní právě když je mříží.

Důkaz.

- Každá mříž je evidentně diskrétní podgrupou V .
- Bud' D diskrétní podgrupa V . Ukážeme, že D je mříží.
- Zvolme v D maximální lineárně nezávislou posloupnost vektorů $e_1, \dots, e_m$ a označme L podgrupu D jimi generovanou.
- Bud' B zkladní buňka mříže L vzhledem k $e_1, \dots, e_m$.



Dokončení důkazu Tvzení 7.2.

- Množina $\text{Cl}(B)$ je uzavřená a omezená. Proto je kompaktní.
- Podle Lemmatu 7.1 je $B \cap D$ podmnožina $\text{Cl}(B)$ bez hromadného bodu. Proto tedy je konečná.
- Snadno nahlédneme, že $|B \cap D| = [D : L]$.
- Proto je grupa D/L konečná, odkud plyne, že D je konečně generovaná beztorzní Abelova grupa.
- Podle Tvzení 2.9) je D volná. Buď $e'_1, \dots, e'_n$ její volná báze.
- Položme $[D : L] = k$. Potom jsou $ke'_i \in L$ a tedy násobky $ke'_1, \dots, ke'_n$ generují volnou podgrupu L . Protože je L volná Abelova grupa hodnosti m , je $n \leq m$.
- Protože L je podgrupou D , je naopak $m \leq n$ a tedy $m = n$.
- Dimenze podprostoru generovaného L je $n = m$, odkud plyne, že $e'_1, \dots, e'_m$ jsou lineárně nezávislé. Proto je D mříží. □

Lemma 7.3 (III.5.3)

Nechť L je mříží ve V . Potom je L úplná právě když lze nalézt omezenou množinu $B \subseteq V$ tak, že $V = L + B$.

Důkaz.

- Je-li L úplná, můžeme za B volit její základní buňku.
- Předpokládejme, že $V = L + B$ pro nějakou omezenou množinu B .
- Označme U vektorový prostor generovaný L . Ukážeme, že $U = V$.
- Bud' $x \in V$. Pro každé $k \in \mathbb{N}$ existují $u_k \in U$, $b_k \in B$ tak, že $kx = u_k + b_k$, odkud $x = u_k/k + b_k/k$.
- Protože je B omezená, je

$$\lim_{k \rightarrow \infty} b_k/k = 0, \text{ odkud } \lim_{k \rightarrow \infty} u_k/k = x.$$

- Protože je U podprostor V , je to jeho uzavřená podmnožina. Proto $x \in U$ a tedy $U = V$. □

Míra určená mříží

- Bud' V reálný vektorový prostor s danou bazí $\mathbf{e} = \{\mathbf{e}_1, \dots, \mathbf{e}_n\}$. Pak báze $\mathbf{e}$ určuje skalární součin

$$\langle \mathbf{u} \mid \mathbf{v} \rangle = \sum u_i v_i,$$

kde $\mathbf{u} = \sum u_i \mathbf{e}_i$, $\mathbf{v} = \sum v_i \mathbf{e}_i$.

- Z tohoto součinu odvodíme Lebesgueovu míru $\text{vol}_{\mathbf{e}}$ na V .
- Uvažme vektory $\mathbf{v}_1, \dots, \mathbf{v}_n \in V$. Tyto vektory určují rovnoběžnostěn

$$A(\mathbf{v}_i) = \{\sum \alpha_j \mathbf{v}_j \mid 0 \leq \alpha_j \leq 1\}.$$

Je-li $\mathbf{v}_i = \sum a_{ij} \mathbf{e}_j$ a $\mathbf{A} = (a_{ij})$, potom platí

$$\text{vol}_{\mathbf{e}}(A(\mathbf{v}_i)) = |\det \mathbf{A}| = \sqrt{|\det(\langle \mathbf{v}_i \mid \mathbf{v}_j \rangle)|}.$$

(Je totiž $(\langle \mathbf{v}_i \mid \mathbf{v}_j \rangle) = \mathbf{A} \mathbf{A}^T$.)

- Je-li $\mathbf{a} = \{\mathbf{a}_1, \dots, \mathbf{a}_n\}$ báze, pak pro měřitelnou M platí

$$\text{vol}_{\mathbf{a}}(M) = \text{vol}_{\mathbf{e}}(M) \text{vol}_{\mathbf{e}}(\mathbf{A})^{-1}$$

- Fixujeme bázi $\mathbf{e}$ a položíme $\text{vol} = \text{vol}_{\mathbf{e}}$.

Lemma 7.4 (III.5.4)

Bud' L úplná mříž ve V . Necht' $\mathbf{a} = \{a_1, \dots, a_n\}$ a $\mathbf{b} = \{b_1, \dots, b_n\}$ jsou báze V takové, že $L = \{\sum k_i a_i \mid k_i \in \mathbb{Z}\} = \{\sum k_i b_i \mid k_i \in \mathbb{Z}\}$. Jsou-li A , resp. B , základní buňky vzhledem k bázím $\mathbf{a}$, resp. $\mathbf{b}$, potom $\text{vol}(A) = \text{vol}(B)$.

- Položíme $\text{vol}(L) = \text{vol}(A) = \text{vol}(B)$.

Věta 7.5 (Minkovského o mřížovém bodě - (III.5.5))

Bud' L úplná mříž v reálném vektorovém prostoru dimenze n . Potom každá konvexní středově souměrná množina $M \subseteq V$, (tedy $M = -M$), která splňuje

$$\text{vol}(M) > 2^n \text{vol}(L)$$

obsahuje alespoň jeden mřížový bod.

Důkaz Věty 7.5.

- Nejprve sporem ukážeme, že existují různé $x_1, x_2 \in L$ tak, že $(x_1 + \frac{1}{2}M) \cap (x_2 + \frac{1}{2}M) \neq \emptyset$.
- Buď A základní buňka L . Množiny $A \cap (x + \frac{1}{2}M)$, $x \in L$ jsou po dvou disjunktní a tedy

$$\text{vol}(A) \geq \sum_{x \in L} \text{vol}(A \cap (x + \frac{1}{2}M)).$$

- Posunutím o $-x$ dostaneme $\text{vol}(A \cap (x + \frac{1}{2}M)) = \text{vol}((A - x) \cap \frac{1}{2}M)$.
- Odtud plyne

$$\text{vol}(A) \geq \sum_{x \in L} \text{vol}((A - x) \cap \frac{1}{2}M) = \text{vol}(\frac{1}{2}M) = \frac{1}{2^n}(\text{vol}M),$$

což je **spor**.



Dokončení důkazu Věty 7.5.

- Nechť pro $x_1 \neq x_2$ z L platí $x_1 + \frac{1}{2}y_1 = x_2 + \frac{1}{2}y_2$, kde $y_i \in M$.
- Potom $x_1 - x_2 = \frac{1}{2}(y_2 - y_1)$, což je střed úsečky spojující body $-y_1$ a y_2 .
- Protože je M konvexní, leží tento bod v M . Protože $x_1 - x_2 \in L$, leží tento bod v $M \cap L$.



Malé opakování

- Komutativní těleso K je **číselným tělesem** je-li konečným rozšířením $\mathbb{Q}$.
- Prvky těles K jsou algebraická komplexní čísla. Ty z nich, která jsou kořenem monického polynomu ze $\mathbb{Z}[x]$ nazveme **algebraická celá čísla**. Tyto prvky tvoří celistvý uzávěr $\mathbb{Z}$ v K , který značíme $\mathbb{Z}_K$.
- $\mathbb{Z}_K$ je volný $\mathbb{Z}$ modul hodnosti $n = [K : \mathbb{Q}]$. To plyne z existence celivé báze. Přitom hodnota diskriminantu $\Delta(\mathbb{Z}_K)$ nezávisí na volbě celivé báze.
- Buď I nenulový ideál okruhu $\mathbb{Z}_K$. Pro libovolné nenulové $c \in \mathbb{Z}_K$ je zobrazení $x \mapsto cx$ izomorfismem $\mathbb{Z}$ -modulů $\mathbb{Z}_K$ a $c\mathbb{Z}_K$. Proto mají oba tyto volné $\mathbb{Z}$ -moduly stejnou hodnost. Přitom, pokud $c \in I$, je $c\mathbb{Z}_K \subseteq I \subseteq \mathbb{Z}_K$. Proto je I volný $\mathbb{Z}$ -modul hodnosti n . Speciálně má I n -prvkou celistvou bázi.

Absolutní norma lomeného ideálu

- Uvažujme dále o nenulovém ideálu I okruhu $\mathbb{Z}_K$. V $\mathbb{Z}_K$ existuje celistvá báze $e_1, \dots, e_n$ tak, že $m_1 e_1, \dots, m_n e_n$ je, pro vhodná kladná celá čísla m_i , celistvá báze I . Potom $|\mathbb{Z}_K : I| = \prod m_i$ a

$$\Delta(I) = |\mathbb{Z}_K : I|^2 \Delta(\mathbb{Z}_K).$$

- Víme, že $\mathbb{Z}_K$ je Dedekindův obor. Podle Lemmatu 6.24 jsou lomené ideály oboru $\mathbb{Z}_K$ volnými $\mathbb{Z}$ -moduly hodnosti n . Podobně jako celé ideály tak mají celistvou bázi a pro dvojici $I \leq J$ lomených ideálů je

$$\Delta(J) = |J : I| \Delta(I).$$

- Speciálně pro lomený ideál I oboru $\mathbb{Z}_K$ označíme $\mathcal{N}(I)$ index $|\mathbb{Z}_K : I|$ a nazveme jej **absolutní normou** I .

Lemma 7.6 (IV.1.1)

Bud' $I = \alpha \mathbb{Z}_K$ hlavní ideál okruhu $\mathbb{Z}_K$. Potom

$$\mathcal{N}(I) = |\mathbb{Z}_K : I| = |\mathbf{N}_{K|\mathbb{Q}}(\alpha)|.$$

Důkaz.

- Je-li $\mathbf{e}: e_1, \dots, e_n$ celistvá báze, potom je $\alpha e_1, \dots, \alpha e_n$ n -prvková množina generátorů volného $\mathbb{Z}$ -modulu I hodnosti n a tedy je to jeho volná báze.
- Potom dle definice pro matici $\mathbf{M}_{\mathbf{e}}(\alpha) = (a_{ij})$, kde $\alpha e_i = \sum a_{ij} e_j$, platí, že

$$\mathbf{N}_{K|\mathbb{Q}}(\alpha) = \det \mathbf{M}_{\mathbf{e}}(\alpha).$$

- Podle Lematu 6.17 existuje celistvá báze $\mathbf{e}: e_1, \dots, e_n$ tělesa K .
- Pak existují celá kladná čísla $m_1, \dots, m_n$ tak, že $m_1 e_1, \dots, m_n e_n$ tvoří bázi I jako volného $\mathbb{Z}$ -modulu.



Dokončení důkazu.

- Uvědomme si, že sloupce matice $\mathbf{M}_{\mathbf{e}}(\alpha)$ stejně jako sloupce diagonální matice s prvky $m_1, \dots, m_n$ na diagonále jsou tvořeny souřadnicemi (vzhledem k bázi $\mathbf{e}$) volných bazí $\mathbb{Z}$ -modulu I .
- Matice přechodu mezi celistvými bazemi mají celočíselné souřadnice a jsou regulární. Proto je absolutní jejich determinantů rovna jedné.
- Odtud plyne, že

$$|\det \mathbf{M}_{\mathbf{e}}(\alpha)| = |\prod m_i|.$$

- Protože.

$$|\mathbb{Z}_K : I| = |\prod m_i|,$$

plyne z předchozí formule dokazované.



Lemma 7.7 (III.6.1)

Bud' R Dedekindův obor a P jeho prvoideál. Potom, pro každé $n \geq 0$, je P^n/P^{n+1} jednodimenzionální vektorový prostor nad tělesem R/P .

Důkaz.

- Protože je $P \cdot P^n = P^{n+1}$, je $P \subseteq \text{Ann}(P^n/P^{n+1})$. Proto můžeme P^n/P^{n+1} chápat jako R/P -modul a vzhledem k tomu, že R/P je těleso, jako R/P -vektorový prostor.
- Podle Věty 6.23 má P^n jednoznačný rozklad v součin prvoideálů, a tedy $P^{n+1} \subsetneq P^n$.
- Stačí ukázat, že R -modul P^n/P^{n+1} je cyklický. Zvolme proto libovolné $\alpha \in P^n \setminus P^{n+1}$ a položme $J = \alpha R + P^{n+1}$.
- Protože $\alpha \notin P^{n+1}$, máme $P^{n+1} \subsetneq J \subseteq P^n$. Vynásobíme ideály v tomto řetězci lomeným ideálem P^{-n} , dostaneme $P \subsetneq JP^{-n} \subseteq R$.
- Vzhledem k maximalitě P je $JP^{-n} = R$, odkud $J = P^n$ a tedy $(R/P)(\alpha + P^{n+1}) = P^n/P^{n+1}$.



Tvrzení 7.8 (IV.1.2)

Necht' $I = P_1^{j_1} \cdots P_k^{j_k}$ je faktorizace ideálu I okruhu $\mathbb{Z}_K$ na prvoideály. Potom

$$\mathcal{N}(I) = \mathcal{N}(P_1)^{j_1} \cdots \mathcal{N}(P_k)^{j_k}.$$

Důkaz.

- Nejprve předpokládejme, že $I = P^j$. Potom

$$\mathcal{N}(P^j) = |\mathbb{Z}_K : P^j| = |\mathbb{Z}_K : P| \cdot |P : P^2| \cdots |P^{j-1} : P^j|.$$

- Podle Lemmatu 7.7 jsou $|\mathbb{Z}_K : P| = |P^{i-1} : P^i|$, odkud dostáváme, že $\mathcal{N}(P^j) = \mathcal{N}(P)^j$.
- Podle Čínské věty o zbytcích (Lemma 1.22) je $\mathbb{Z}_K/I \simeq \bigoplus \mathbb{Z}_K/P_i^{j_i}$, odkud plyne

$$\mathcal{N}(I) = \prod \mathcal{N}(P_i^{j_i}) = \prod \mathcal{N}(P_i)^{j_i}.$$



Lemma 7.9

Bud' R Dedekindův okruh a necht' $a \in R$. Necht' $aR = P_1^{j_1} \cdots P_k^{j_k}$ je rozklad aR v součin prvoideálů. Potom pro libovolný prvoideál P , $a \in P$ právě když $P = P_i$ pro některé $i \leq k$.

Důkaz.

- $aR \subseteq P_i$ a tedy $a \in P_i$, pro každé $i = 1, \dots, k$.
- Je-li P prvoideál takový, že $a \in P$, je $\prod P_i^{j_i} \subseteq P$ a tedy $P_i \subseteq P$ pro některé i .
- Protože v Dedekindově okruhu jsou prvoideály maximální, je potom $P_i = P$.



Tvzení 7.10 (IV.1.3)

Pro každou konstantu $c > 0$ existuje jen konečně mnoho ideálů I okruhu $\mathbb{Z}_K$ takových, že $\mathcal{N}(I) \leq c$.

Důkaz Tvzení 7.10.

- Nechť P je prvoideál v $\mathbb{Z}_K$. Potom je $P \cap \mathbb{Z}$ prvoideál v $\mathbb{Z}$ (Tvzení 6.10), a tedy $P \cap \mathbb{Z} = p\mathbb{Z}$ pro vhodné prvočíslo.
- Podle Lemmatu 7.9 je pak $p \in P$ a $\mathbb{Z}_K/P$ je konečný $\mathbb{Z}_p$ modul. Proto je

$$\mathcal{N}(P) = |\mathbb{Z}_K : P| = p^{t_P}.$$

- Pokud je $p \in P$, vyskytuje se prvoideál P v rozkladu ideálu $p\mathbb{Z}_K$. Takových prvoideálů je jen konečně mnoho.
- Protože je jen konečně mnoho prvočísel menších nebo rovných c , dostáváme odtud dokazované.



Lemma 7.11 (IV.2.1)

Označme $\mathbb{D} = \{(a_1, a_2) \in \mathbb{C}^2 \mid a_1 = \overline{a_2}\}$ a definujme zobrazení $G: \mathbb{D} \rightarrow \mathbb{R}^2$ předpisem $(a_1, a_2) \mapsto (x, y)$ pro $a_1 = x + iy$. Potom je G isomorfismus reálných vektorových prostorů a pro $(a_1, a_2), (b_1, b_2) \in \mathbb{D}$ je

$$\langle G(a_1, a_2) \mid G(b_1, b_2) \rangle = (a_1 \overline{b_1} + a_2 \overline{b_2})/2.$$

- Nechť dále značí K číselné těleso stupně n nad $\mathbb{Q}$.
- Označme $K_{\mathbb{C}}$ komplexní vektorový prostor $\{(u_g) \mid g \in \text{hom}(K, \mathbb{C})\}$.
- Protože je rozšíření $\mathbb{Q} \leq K$ separabilní, je množina $\text{hom}(K, \mathbb{C})$ n -prvková a tedy $\dim(K_{\mathbb{C}}) = [K: \mathbb{Q}] = n$.
- Pro $g \in \text{hom}(K, \mathbb{C})$ definujme $\overline{g}: \alpha \mapsto \overline{g(\alpha)}$.
- Uvažme jednak komplexní skalární součin $\langle \mathbf{u} \mid \mathbf{v} \rangle_{\mathbb{C}} = \sum u_g \overline{v_g}$, jednak zobrazení $F: K_{\mathbb{C}} \rightarrow K_{\mathbb{C}}$ takové, že pro $F(\mathbf{u}) = \mathbf{v}$ je $v_g = \overline{u_{\overline{g}}}$.

Lemma 7.12 (IV.2.2)

Nechť $\mathbf{u}, \mathbf{v} \in K_{\mathbb{C}}$. Potom platí, že

$$\langle F(\mathbf{u}) \mid F(\mathbf{v}) \rangle_{\mathbb{C}} = \overline{\langle \mathbf{u} \mid \mathbf{v} \rangle_{\mathbb{C}}}.$$

Důsledek 7.13

Nechť $\mathbf{u}, \mathbf{v} \in K_{\mathbb{C}}$. Je-li $F(\mathbf{u}) = \mathbf{u}$ a zároveň $F(\mathbf{v}) = \mathbf{v}$, potom $\langle \mathbf{u} \mid \mathbf{v} \rangle_{\mathbb{C}} \in \mathbb{R}$.

- Pohlížíme-li na $K_{\mathbb{C}}$ jako na reálný prostor, je F jeho automorfismus. Pevné bodu tohoto zobrazení tvoří reálný podprostor $K_{\mathbb{C}}$, který označíme jako $K_{\mathbb{R}}$. Navíc restrikce hermitovského skalárního součinu na prostor $K_{\mathbb{R}}$ na něm definuje reálný skalární součin.
- Prostor $K_{\mathbb{R}}$ s tímto skalárním součinem nazveme **Minkovského prostor**. Metriku odvozenou od tohoto skalárního součinu budeme nazývat **kanonickou** a označíme ji **vol**.

Značení

- Označme $r = |\text{hom}(K, \mathbb{R})|$, tj. počet homomorfismů z $\text{hom}(K, \mathbb{C})$, jejichž hodnoty jsou reálné a s počet dvojic komplexně sdružených homomorfismů z $\text{hom}(K, \mathbb{C}) \setminus \text{hom}(K, \mathbb{R})$. Zřejmě je $n = r + 2s$.
- Označme $K_{\mathbb{C}}^{\mathbb{R}} = \{(a_g) \mid g \in \text{hom}(K, \mathbb{C}) \text{ a } a_g \in \mathbb{R}\}$ - množinu všech reálných posloupností z $\text{hom}(K, \mathbb{C})$.

Lemma 7.14 (IV.2.4)

Bud' Σ podmnožina $\text{hom}(K, \mathbb{C})$ obsahující $\text{hom}(K, \mathbb{R})$ a navíc z každé dvojice komplexně sdružených nereálných homomorfismů právě jeden. Definujme $G: K_{\mathbb{R}} \rightarrow K_{\mathbb{C}}^{\mathbb{R}}$, tak, že $G(a_g) = a_g$, pro $g \in \text{hom}(K, \mathbb{R})$ a $a_g = G(a_g) + iG(a_{\bar{g}})$ pro $g \in \Sigma \setminus \text{hom}(K, \mathbb{R})$. Dále položme $\tau_g = 1$ pro $g \in \text{hom}(K, \mathbb{R})$ a $\tau_g = 2$ pro $g \in \text{hom}(K, \mathbb{C}) \setminus \text{hom}(K, \mathbb{R})$. Na $K_{\mathbb{C}}^{\mathbb{R}}$ definujme $\langle \mathbf{a} \mid \mathbf{b} \rangle = \sum \tau_g a_g b_g$. Potom je G isomorfismus, který zachovává skalární součin.

Důsledek 7.15 (IV.2.5)

Bud' vol_0 standardní míra na $K_{\mathbb{C}}^{\mathbb{R}} \simeq \mathbb{R}^{r+2s}$. Pak pro každou měřitelnou množinu $M \subseteq K_{\mathbb{R}}$ platí, že $\text{vol}(M) = 2^s \text{vol}_0(G(M))$.

Definice

- Pro $\mathbf{u} = (u_g) \in K_{\mathbb{C}}$ definujme stopu $\text{Tr}(\mathbf{u}) = \sum u_g$. Snadno nahlédeme, že jde o lineární formu $\text{Tr}: K_{\mathbb{C}} \rightarrow \mathbb{C}$, která navíc splňuje $\text{Tr}(F(\mathbf{u})) = \overline{\text{Tr}(\mathbf{u})}$. Speciálně restrikce tohoto zobrazení na $K_{\mathbb{R}}$ dává lineární formu $\text{Tr}: K_{\mathbb{R}} \rightarrow \mathbb{R}$.
- Definujme $f: K \rightarrow K_{\mathbb{C}}$ tak, že $f(\alpha) = (g(\alpha))_{g \in \text{hom}(K, \mathbb{C})}$. Snadno nahlédneme, že $F(f(\alpha)) = f(\alpha)$ pro každé $\alpha \in K$.

Lemma 7.16 (IV.2.6)

Pro každé $\alpha \in K$ je $\text{Tr}(f(\alpha)) = \text{Tr}_{K|\mathbb{Q}}(\alpha)$.

Tvrzení 7.17 (IV.2.7)

Je-li I nenulový ideál v $\mathbb{Z}_K$, pak je $f(I) = \{f(\alpha) \mid \alpha \in I\}$ úplnou mříží v $K_{\mathbb{R}}$ a platí, že

$$\text{vol}(f(I)) = \sqrt{|\Delta(I)|}.$$

Důkaz.

- Bud' $\alpha_1, \dots, \alpha_n$ celistvá báze ideálu I . Potom

$$f(I) = \left\{ \sum n_i \alpha_i \mid n_i \in \mathbb{Z} \right\}.$$

- Podle Tvrzení 4.4 je

$$\Delta(I) = \Delta(\alpha_1, \dots, \alpha_n) = \det^2(g_i(\alpha_j)),$$

- Podle Tvrzení 4.5 je $\Delta(I) \neq 0$. Sloupce matice $(g_i(\alpha_j))$, tvořeny vektory $f(\alpha_j)$, jsou pak lineárně nezávislé. Dle definice je $f(I)$ mříží.
- Pak je $\text{vol}(f(I)) = |\det(g_i(\alpha_j))| = \sqrt{|\Delta(I)|}$.



Lemma 7.18 (IV.2.8)

Bud' I nenulový ideál v $\mathbb{Z}_K$ a necht' c_g , pro $g \in \text{hom}(K, \mathbb{C})$, jsou kladná čísla taková, že $c_g = c_{\bar{g}}$. Je-li

$$\left(\frac{2}{\pi}\right)^s \sqrt{|\Delta(I)|} \leq \prod c_g,$$

potom existuje $\alpha \in I$, $\alpha \neq 0$, tak, že pro všechna $g \in \text{hom}(K, \mathbb{C})$ platí $|g(\alpha)| < c_g$.

Důkaz.

- Definujme $M = \{\mathbf{u} \in K_{\mathbb{R}} \mid |u_g| < c_g \text{ pro všechna } g \in \text{hom}(K, \mathbb{C})\}$.
- Uvažme výběr Σ a zobrazení $G: K_{\mathbb{R}} \rightarrow K_{\mathbb{C}}^{\mathbb{R}}$ jako v Tvzení 7.14.
- Potom

$$G(M) = \left\{ (a_g) \in K_{\mathbb{C}}^{\mathbb{R}} \mid \begin{cases} |a_g| < c_g & \text{pro } g \in \text{hom } K, \mathbb{R} \\ a_g^2 + \bar{a}_g^2 < c_g^2 & \text{pro } g \in \Sigma \end{cases} \right\}.$$



Dokončení důkazu Lemmatu 7.18.

- Z definice odvodíme

$$\text{vol}(G(M)) = \prod_{g: K \rightarrow \mathbb{R}} (2c_g) \prod_{g \in \Sigma} (\pi c_g^2) = 2^r \pi^s \prod_{g: K \rightarrow \mathbb{C}} c_g.$$

- Podle Důsledku 7.15 a Tvrzení 7.17 je pak

$$\text{vol}(M) = 2^s \text{vol}(G(M)) = 2^n \left(\frac{\pi}{2}\right)^s \prod_{g: K \rightarrow \mathbb{C}} c_g > 2^n \text{vol}(f(I)).$$

- Podle Věty 7.5 (Minkovského o mřížovém bodě) existuje nenulové $\alpha \in I$ tak, že

$$(g(\alpha))_{g \in \text{hom}(K, \mathbb{C})} = f(\alpha) \in M,$$

odkud $|g(\alpha)| < c_g$ pro každé $g \in \text{hom}(K, \mathbb{C})$.



Tvrzení 7.19 (IV.2.9)

Nechť I je nenulový ideál okruhu $\mathbb{Z}_K$ v číselném tělese K . Pak existuje $\alpha \in I$, $\alpha \neq 0$, takové, že

$$|N_{K|\mathbb{Q}}(\alpha)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta(I)|}.$$

Důkaz.

- Pro každé $\varepsilon > 0$ zvolme $c_g \in \mathbb{R}^+$, kde $g \in \text{hom}(K, \mathbb{C})$, $c_g = c_{\bar{g}}$ tak, že

$$\prod c_g = \varepsilon + \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta(I)|}.$$

- Z Tvrzení 7.18 plyne existence nenulového $\alpha \in I$ tak, že $|g(\alpha)| < c_g$ pro každé $g \in \text{hom}(K, \mathbb{C})$.
- Podle Tvrzení 7.2 je $N_{K|\mathbb{Q}}(\alpha) = \prod g(\alpha)$ a tedy

$$|N_{K|\mathbb{Q}}(\alpha)| = \prod |g(\alpha)| < \prod c_g = \varepsilon.$$

- Podle Tvrzení 6.11 je $N_{K|\mathbb{Q}}(\alpha)$ celé číslo pro každé $\alpha \in \mathbb{Z}_K$, odkud dostáváme dokazované, neboť ε lze volit libovolně malé. □

Lemma 7.20

Bud' K číselné těleso a položme $c = (2/\pi)^s \sqrt{|\Delta(\mathbb{Z}_K)|}$. Potom v každém nenulovém ideálu I oboru $\mathbb{Z}_K$ existuje nenulové α tak, že $\mathcal{N}(\alpha\mathbb{Z}_K) \leq c\mathcal{N}(I)$.

Důkaz.

- Z úvah na začátku předcházející kapitoly (připomeňme, že značíme $\mathcal{N}(I) = |\mathbb{Z}_K : I|$) plyne, že pro nenulový ideál I okruhu $\mathbb{Z}_K$ platí

$$\sqrt{|\Delta(I)|} = \sqrt{|\Delta(\mathbb{Z}_K)|} |\mathbb{Z}_K : I| = \sqrt{|\Delta(\mathbb{Z}_K)|} \mathcal{N}(I)$$

- Podle Tvrzezení 7.19 existuje nenulové $\alpha \in I$ tak, že

$$|\mathcal{N}_{K|\mathbb{Q}}(\alpha)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta(I)|} = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta(\mathbb{Z}_K)|} \mathcal{N}(I) = c\mathcal{N}(I).$$

- Podle Lemmatu 7.6 je $\mathcal{N}(\alpha\mathbb{Z}_K) = |\mathcal{N}_{K|\mathbb{Q}}(\alpha)|$ odkud dostáváme, že $\mathcal{N}(\alpha\mathbb{Z}_K) \leq c\mathcal{N}(I)$. □

Věta 7.21 (IV.2.10)

Třídová grupa Cl_K číselného tělesa K je konečná.

Důkaz.

- Buď A nenulový lomený ideál $\mathbb{Z}_K$. Pak je A^{-1} také lomený ideál a podle Lemmatu 6.24 existuje nenulové $\gamma \in \mathbb{Z}_K$ tak, že $J = \gamma A^{-1}$ je celistvý ideál.
- Podle Lemmatu 7.20 existuje nenulové $\alpha \in J$ tak, že $\mathcal{N}(\alpha \mathbb{Z}_K) \leq c\mathcal{N}(J)$. Položme $I = \alpha J^{-1}$.
- Nejprve ukážeme celistvost I : Je $\alpha \in \gamma A^{-1}$ a $J^{-1} = \gamma^{-1} A$. Proto $I = \alpha J^{-1} \subseteq \gamma A^{-1} \gamma^{-1} A = A A^{-1} = \mathbb{Z}_K$, odkud plyne celistvost αJ^{-1} .



Důkaz Věty 7.21 - část 2.

- Nyní ukážeme, že $\mathcal{N}(I) \leq c$:
- Dle předchozího jsou ideály $\alpha\mathbb{Z}_K$, J a αJ^{-1} celistvé.
- Nechť $\alpha\mathbb{Z}_K = P_1^{\mu_1} \cdots P_k^{\mu_k}$ a $J = P_1^{\nu_1} \cdots P_k^{\nu_k}$ jsou rozklady ideálů $\alpha\mathbb{Z}_K$ a J v součin prvoideálů. Potom $\alpha J^{-1} = \prod P_i^{\mu_i - \nu_i}$ a, protože je ideál αJ^{-1} celistvý, jsou $\mu_i - \nu_i$ nezáporné.
- Podle Tvzení 8.2 pak platí, že $\mathcal{N}(\alpha\mathbb{Z}_K) = \prod \mathcal{N}(P_i)^{\mu_i}$, $\mathcal{N}(J) = \prod \mathcal{N}(P_i)^{\nu_i}$ a $\mathcal{N}(\alpha J^{-1}) = \prod \mathcal{N}(P_i)^{\mu_i - \nu_i}$.
- Protože $\mathcal{N}(\alpha\mathbb{Z}_K) \leq c\mathcal{N}(J)$, platí $\prod \mathcal{N}(P_i)^{\mu_i} \leq c \prod \mathcal{N}(P_i)^{\nu_i}$, odkud $\mathcal{N}(I) = \mathcal{N}(\alpha J^{-1}) = \prod \mathcal{N}(P_i)^{\mu_i - \nu_i} \leq c$.
- Protože $\gamma J = A^{-1}$, je

$$A = \gamma J^{-1} = \frac{\gamma}{\alpha} I \in \mathcal{P}_K I.$$

- Přitom $\mathcal{N}(I) \leq c$ a takových ideálů je vzhledem k Tvzení 7.10 jen konečně mnoho. Odtud plyne konečnost grupy Cl_K . □

Lemma 8.1

Pro $n \in \mathbb{N}$ a každou konečnou množinu posloupností $(i_0, \dots, i_{n-1})$ nezáporných celých čísel existuje přirozené číslo t tak, že pro každou dvojici posloupností $(i_0, \dots, i_{n-1})$ a $(j_0, \dots, j_{n-1})$ z této množiny

$$i_0 + i_1 t + \dots + i_{n-1} t^{n-1} = j_0 + j_1 t + \dots + j_{n-1} t^{n-1}$$

právě když $(i_0, \dots, i_{n-1}) = (j_0, \dots, j_{n-1})$.

Důkaz.

- Je $\sum_{k=0}^{n-1} i_k t^k = \sum_{k=0}^{n-1} j_k t^k$ právě když $\sum_{k=0}^{n-1} (i_k - j_k) t^k = 0$.
- Dostáváma tak jen konečného polynomů a proto existuje přirozené číslo t , které není kořenem žádného z nich. Toto t vyhovuje podmínkám lemmatu. □

Lemma 8.2 (IV.1.2)

Nechť K je komutativní těleso a necht' $y_0 \in K[x_0, \dots, x_{n-1}]$ je nekonstatní polynom. Potom existují polynomy $y_1, \dots, y_{n-1} \in K[x_0, \dots, x_{n-1}]$ s následujícími vlastnostmi:

- ❶ $K[x_0, y_1, \dots, y_{n-1}] = K[x_0, \dots, x_{n-1}]$;
- ❷ *existuje $m \in \mathbb{N}$, konstanta $c \in K$ a $f_0, \dots, f_{m-1} \in K[y_1, \dots, y_{n-1}]$ tak, že*

$$y_0 = cx_0^m + \sum_{i < m} f_i x_0^i.$$

Důkaz Lemmatu 8.2.

- Bud' $y_0(x_0, \dots, x_{n-1}) = \sum a_{i_0, \dots, i_{n-1}} x_0^{i_0} \dots x_{n-1}^{i_{n-1}}$.
- $a_{i_0, \dots, i_{n-1}} \neq 0$ jen pro konečně mnoho $(i_0, \dots, i_{n-1})$. Bud' t přirozené číslo splňující podmínky Lemmatu 8.1 vzhledem k těmto posloupnostem.
- Položme $y_i = x_i - x_0^{t^i}$, pro $1 \leq i \leq n-1$.

- Protože je $x_i = y_i + x_0^{t^i}$, máme

$$K[x_0, x_1, \dots, x_{n-1}] = K[x_0, y_1, \dots, y_{n-1}] \text{ a}$$

$$y_0 = \sum a_{i_0, \dots, i_{n-1}} (x_0^t + y_1)^{i_1} \dots (x_0^{t^{n-1}} + y_{n-1})^{i_{n-1}} x_0^{i_0}.$$

odkud po roznásobení dostaneme vyjádření y_0 v požadovaném tvaru.

- Rozmyslete si ještě, že lze volit

$$m = \max\{\sum_{k=0}^{n-1} i_k t^k \mid a_{i_0, \dots, i_{n-1}} \neq 0\}.$$



Tvrzení 8.3 (VI.1.3)

Nechť K je komutativní těleso a $A = K[x_0, \dots, x_{n-1}]$. Nechť $y_0 \in A$ je nekonstantní polynom a označme I ideál generovaný y_0 . Potom lze nalézt $y_1, \dots, y_{n-1} \in K[x_0, \dots, x_{n-1}]$ takové, že

- ① A je celistvé nad $K[y_0, \dots, y_{n-1}]$;
- ② $y_0, \dots, y_{n-1}$ jsou algebraicky nezávislé nad K ;
- ③ $I \cap K[y_0, \dots, y_{n-1}] = y_0 K[y_0, \dots, y_{n-1}]$;

Důkaz.

- Zvolme $y_1, \dots, y_n$ jako v předchozím lemmatu. Potom

$$y_0 = cx_0^m + \sum_{i < m} f_i x_0^i$$

pro $f_i \in K[y_1, \dots, y_{n-1}]$ a tedy x_0 je celistvé nad $K[y_0, \dots, y_{n-1}]$.

- Protože podle Lemmatu 8.2 navíc platí, že

$$K[x_0, y_1, \dots, y_{n-1}] = K[x_0, \dots, x_{n-1}],$$

je A celistvé nad $K[y_0, \dots, y_{n-1}]$.



Dokončení důkazu Tvzení 8.3.

- Podle Tvzení 4.15 je

$$[K(y_0, \dots, y_{n-1}) : K]_{\text{tr}} = [K(x_0, \dots, x_{n-1}) : K]_{\text{tr}} = n.$$

- Maximální algebraicky nezávislá podmnožina množiny $y_0, \dots, y_{n-1}$ pak musí být n -prvková a tedy $y_0, \dots, y_{n-1}$ jsou algebraicky nezávislé nad K .
- Zbývá ukázat, že $I \cap K[y_0, \dots, y_{n-1}] = y_0 K[y_0, \dots, y_{n-1}]$. Nechť tedy pro nějaké $u \in A$ platí $w = y_0 u \in K[y_0, \dots, y_{n-1}]$. Potom (protože A je celistvé nad $K[y_0, \dots, y_{n-1}]$) existují $k \in \mathbb{N}$ a $g_0, \dots, g_{k-1} \in K[y_0, \dots, y_{n-1}]$, tak, že $u^k + \sum_{i=0}^{k-1} g_i u^i = 0$.
- Odtud

$$0 = y_0^k \left(u^k + \sum_{i=0}^{k-1} g_i u^i \right) = w^k + \sum_{i=0}^{k-1} g_i y_0^{k-i} w^i.$$

- Z algebraické nezávislosti $y_0, \dots, y_{n-1}$ plyne, že $K[y_0, \dots, y_{n-1}]$ je Gaussův obor. Máme $y_0 \mid w^k$ a protože je y_0 prvočinitel dostáváme, že $y_0 \mid w$. Odtud $w \in y_0 K[y_0, \dots, y_{n-1}]$. □

Tvrzení 8.4 (VI.1.4)

Bud' I vlastní ideál okruhu $A = K[x_0, \dots, x_{n-1}]$. Potom existují $y_0, \dots, y_{n-1} \in K[x_0, \dots, x_{n-1}]$ a nezáporné $d \leq n$ tak, že

- ❶ $y_0, \dots, y_{n-1}$ jsou nad K algebraicky nezávislé;
- ❷ A je celistvé rozšíření $K[y_0, \dots, y_{n-1}]$;
- ❸ $I \cap K[y_0, \dots, y_{n-1}] = \sum_{i < d} y_i K[y_0, \dots, y_{n-1}]$;

Důkaz.

- V případě, že $I = 0$ stačí položit $d = 0$ a $y_i = x_i$. Předpokládejme, že $I \neq 0$.
- Tvrzení ukážeme indukcí podle n . V případě, že $n = 1$, je A obor hlavních ideálů a tvrzení plyne z Tvrzení 8.3 (nebo lze snadno nahlédnout přímo).
- Předpokládejme, že $n > 1$ a tvrzení platí pro každou menší hodnotu.



Důkaz Tvzení 8.4 - část 2.

- Zvolme nenulové $z_0 \in I$ a aplikujme Tvzení 8.3. Dostaneme, že existují $z_1, \dots, z_{n-1} \in A$ tak, že
 - 1 $z_0, \dots, z_{n-1}$ jsou nad K algebraicky nezávislé;
 - 2 A je celistvým rozšířením $K[z_0, \dots, z_{n-1}]$;
 - 3 $z_0 A \cap K[z_0, \dots, z_{n-1}] = z_0 K[z_0, \dots, z_{n-1}]$;
- $J = I \cap K[z_1, \dots, z_{n-1}]$ je vlastním ideálem $B = K[z_1, \dots, z_{n-1}]$. Podle indukčního předpokladu existují $y_1, \dots, y_{n-1} \in B$ tak, že pro vhodné kladné $d \leq n$
 - 1 $y_1, \dots, y_{n-1}$ jsou nad K algebraicky nezávislé;
 - 2 B je celistvým rozšířením $K[y_1, \dots, y_{n-1}]$;
 - 3 $J \cap B = \sum_{1 \leq j < d} y_j K[y_1, \dots, y_{n-1}]$;
- Položme $y_0 = z_0$. Ukážeme, že $y_0, \dots, y_{n-1}$ vyhovují pro zvolené d podmínkám tvrzení.
- Okruh $K[z_0, \dots, z_{n-1}]$ je celistvý nad $K[z_0, y_1, \dots, y_{n-1}]$. Protože $z_0 = y_0$ a A je celistvé nad $K[z_0, \dots, z_{n-1}]$, je A celistvé také nad $K[y_0, \dots, y_{n-1}]$.



Důkaz Tvzení 8.4 – část 3.

- Protože $z_0, \dots, z_{n-1}$ jsou algebraicky nezávislé nad K , je

$$[K(z_0, \dots, z_{n-1}) : K]_{\text{tr}} = n.$$

Protože je $K[z_0, \dots, z_{n-1}]$ celistvým rozšířením $K[y_0, \dots, y_{n-1}]$, je podle Tvzení 4.15

$$n = [K(z_0, \dots, z_{n-1}) : K]_{\text{tr}} = [K(y_0, \dots, y_{n-1}) : K]_{\text{tr}}.$$

- To znamená, že $y_0, \dots, y_{n-1}$ jsou nad K algebraicky nezávislé.
- Protože $y_i \in I$ pro či $i < d$, zbývá ukázat, že $I \cap K[y_0, \dots, y_{n-1}] \subseteq \sum_{i < d} K[y_0, \dots, y_{n-1}]$.
- Buď $w \in I \cap K[y_0, \dots, y_{n-1}]$. Rozložme $w = y_0 w_0 + w_1$, kde $w_0 \in K[y_0, \dots, y_{n-1}]$ a $w_1 \in K[y_1, \dots, y_{n-1}]$.
- Protože platí $y_0 \in I$, je $w_1 \in I$ a tedy $w_1 \in I \cap K[y_1, \dots, y_{n-1}]$.
- To podle předchozího znamená, že $w_1 \in \sum_{1 \leq j < d} y_j K[y_1, \dots, y_{n-1}]$, odkud plyne dokazované. □

Připomenutí

Připomeňme, že afinní K -algebrou (kde K je těleso) rozumíme komutativní K -algebru jež je konečné dimenze nad K .

Lemma 8.5 (VI.1.1)

Bud' $\varphi: A \rightarrow B$ surjektivní homomorfismus K -algeber. Necht' $z_0, \dots, z_{m-1}$ jsou prvky takové, že

- ❶ $z_0, \dots, z_{m-1}$ jsou nad K algebraicky nezávislé;
- ❷ A je konečně generovaný $K[z_0, \dots, z_{m-1}]$ -modul;
- ❸ pro nějaké nezáporné $n \leq m$ platí

$$\ker(\varphi) \cap K[z_0, \dots, z_{m-1}] = \sum_{n \leq j} z_j K[z_0, \dots, z_{m-1}].$$

Potom jsou prvky $\varphi(z_0), \dots, \varphi(z_{n-1}) \in B$ algebraicky nezávislé nad K a B je jako $K[\varphi(z_0), \dots, \varphi(z_{n-1})]$ -modul konečně generovaný.

Důkaz Lemmatu 8.5 - část 1.

- Nejprve ukážeme, že B je konečně generovaný $K[\varphi(z_0), \dots, \varphi(z_{m-1})]$ -modul.
- A je dle předpokladu jako $K[z_0, \dots, z_{m-1}]$ -modul konečně generovaný; nechť $a_1, \dots, a_k$ je nějaká množina jeho generátorů. To znamená, že pro každé $a \in A$ existují polynomy $f_1^a, \dots, f_k^a \in K[z_0, \dots, z_{m-1}]$ tak, že

$$a = \sum f_i^a a_i.$$

- Potom, vzhledem k tomu, že $\varphi(z_j) = 0$, pro $n \leq j$ (tyto prvky leží v jádru), dostaneme, že $\varphi(f_i^a) \in K[\varphi(z_0), \dots, \varphi(z_{n-1})]$ a zřejmě platí

$$\varphi(a) = \sum \varphi(f_i^a) \varphi(a_i) \in \sum \varphi(a_i) K[\varphi(z_0), \dots, \varphi(z_{n-1})].$$

- Protože je φ surjektivní, je B konečně generován nad $K[\varphi(z_0), \dots, \varphi(z_{n-1})]$ prvky $\varphi(a_i)$.



Důkaz Lemmatu 8.5 - část 2.

- Nyní ověříme, že $\varphi(z_0), \dots, \varphi(z_{n-1})$ jsou nad K algebraicky nezávislé.
- Pro spor předpokládejme, že $\varphi(f) = 0$ pro nějaké nenulové $f \in K[z_0, \dots, z_{n-1}]$.
- Potom $f \in \ker \varphi$, odkud plyne, že

$$f = \sum_{n \leq j} z_j g_j$$

pro vhodné $g_j \in K[z_0, \dots, z_{m-1}]$.

- Z algebraické nezávislosti $z_0, \dots, z_{m-1}$ však plyne, že

$$f - \sum_{n \leq j} z_j g_j \neq 0,$$

což je spor.



Věta 8.6 (O normalizaci - VI.1.5)

Bud' A netriviální afinní algebra nad komutativním tělesem K a I její vlastní ideál I . Potom existuje n -tice $y_0, \dots, y_{n-1} \in A$ a nezáporné $d \leq n$ tak, že

- ❶ $y_0, \dots, y_{n-1}$ jsou algebraicky nezávislé nad K ;
- ❷ A je celistvým rozšířením $K[y_0, \dots, y_{n-1}]$;
- ❸ $I \cap K[y_0, \dots, y_{n-1}] = \sum_{i < d} y_i K[y_0, \dots, y_{n-1}]$;

Definice

Prvky $y_0, \dots, y_{n-1}$ netriviální afinní algebry A tvoří **noetherovskou normalizaci** jestliže platí, že

- ❶ A je celistvým rozšířením $K[y_0, \dots, y_{n-1}]$;
- ❷ $y_0, \dots, y_{n-1}$ jsou nad K algebraicky nezávislé;

Důkaz Věty 8.6.

- Pro dostatečně velké m existuje surjektivní homomorfismus

$$\varphi: K[x_0, \dots, x_{m-1}] \rightarrow A.$$

- Podle Tvzení 8.4 existují $z_0, \dots, z_{m-1} \in K[x_0, \dots, x_{m-1}]$ a nezáporné $n \leq m$ tak, že
 - $z_0, \dots, z_{m-1}$ jsou algebraicky nezávislé nad K ;
 - $K[x_0, \dots, x_{m-1}]$ je celistvé rozšíření $K[z_0, \dots, z_{m-1}]$;
 - $\ker \varphi \cap K[z_0, \dots, z_{m-1}] = \sum_{n \leq j} z_j K[z_1, \dots, z_{m-1}]$;
- Podle Tvzení 8.5 jsou $\varphi(z_0), \dots, \varphi(z_{n-1})$ algebraicky nezávislé nad K a algebra A je celistvá nad $K[z_0, \dots, z_{n-1}]$;
- Podle Tvzení 8.4 existují $y_0, \dots, y_{n-1} \in K[\varphi(z_0), \dots, \varphi(z_{n-1})]$ tak, že pro vhodné nezáporné $d \leq n$ platí
 - $z_0, \dots, z_{m-1}$ jsou algebraicky nezávislé nad K ;
 - $K[\varphi(z_0), \dots, \varphi(z_{n-1})]$ je celistvé nad $K[y_0, \dots, y_{n-1}]$;
 - $I \cap K[y_0, \dots, y_{n-1}] = \sum_{i < d} y_i K[y_0, \dots, y_{n-1}]$;
- Celistvost A nad $K[y_0, \dots, y_{n-1}]$ plyne z tranzitivity celistvosti. □

Lemma 8.7 (VI.3.1)

Bud' S celistvé rozšíření oboru R . Potom pro každou multiplikativní podmnožinu U oboru R je $U^{-1}S$ celistvé rozšíření $U^{-1}R$.

Lemma 8.8 (VI.3.2)

Bud' S rozšíření okruhu R a U multiplikativní množina v R . Označme $\overline{R}$ celistvý uzávěr R v S . Potom je $U^{-1}\overline{R}$ celistvým uzávěrem $U^{-1}R$ v $U^{-1}S$.

Důkazu Lemmatu 8.8.

- Podle Lemmatu 8.7 je $U^{-1}\overline{R}$ celistvé nad $U^{-1}R$.
- Nechť je $s/u \in U^{-1}S$ celistvé nad $U^{-1}R$. Potom existují $r_i/u_i \in U^{-1}R$ tak, že

$$\left(\frac{s}{u}\right)^n + \frac{r_{n-1}}{u_{n-1}} \left(\frac{s}{u}\right)^{n-1} + \cdots + \frac{r_1}{u_1} \frac{s}{u} + \frac{r_0}{u_0} = 0.$$

- Položme $v = u_0 \cdots u_{n-1}$ a vynásobíme získanou rovnost $(u^n v^n)/1$. Dostaneme $t_0, \dots, t_{n-1} \in R$ takové, že

$$\frac{(vs)^n + t_{n-1}(vs)^{n-1} + \cdots + t_1(vs) + t_0}{1} = 0.$$

- Dostáváme, že $w((vs)^n + t_{n-1}(vs)^{n-1} + \cdots + t_1(vs) + t_0) = 0$ pro vhodné $w \in U$.
- Potom je $s/u = wvs/wvu$ a wvs celistvé nad R a tedy $wvs \in \overline{R}$.



Lemma 8.9 (VI.2.7)

Necht' $M \leq N$ jsou R -moduly. Potom je $M = N$ právě když $M_Q = N_Q$ pro každý maximální ideál Q okruhu R .

Důkaz.

- Předpokládejme, že $M < N$ a zvolme $n \in N \setminus M$.
- Položme $I = \{a \in R \mid an \in M\}$ a buď Q nějaký maximální ideál R obsahující I .
- Ukážeme, že $n \notin M_Q$.
- Kdyby platilo, že $n \in M$, existovalo by $b \in R \setminus Q$ tak, že $bn \in M$, což neplatí neboť $b \notin I$.



Tvzení 8.10 (VI.3.3)

Pro obor integrity R je ekvivalentní:

- ❶ *R je celistvě uzavřený;*
- ❷ *R_P je celistvě uzavřený pro každý prvoideál P oboru R ;*
- ❸ *R_Q je celistvě uzavřený pro každý maximální ideál Q oboru R ;*

Důkaz Tvzení 8.10.

- Bud' T podílové těleso oboru R . Potom pro každý prvoideál P oboru R platí $R \leq R_P \leq T$.
- Označme S celistvý uzávěr R v T . Podle Lemmatu 8.8 je S_P celistvý uzávěr R_P v T a z $R = S$ plyne $R_P = S_P$.
- Ukázali jsme $(1) \implies (2) \implies (3)$.
- Implikace $(3) \implies (1)$ plyne z Lemmatu 8.9.



Lemma 8.11 (VI.2.3)

Bud' U multiplikativní množina okruhu R . Pak přiřazení $P \mapsto U^{-1}P$ určuje vzájemně jednoznačnou korepondenci mezi prvoideály R disjunktními s U a prvoideály okruhu $U^{-1}R$.

Důkaz.

- Bud' P prvoideál disjunktní s U . Necht' $(a/u)(b/v) \in U^{-1}P$, tj., pro vhodné $c/w \in U^{-1}P$:

$$\frac{a}{u} \frac{b}{v} = \frac{c}{w}$$

- Odtud plyne, že existuje $x \in U$ tak, že $x(wab - uvc) = 0$, odkud $xwab \in P$.
- Protože P je prvoideál disjunktní s U a $xw \in U$, je $a \in P$, nebo $b \in P$, tj., $a/u \in U^{-1}P$, nebo $b/v \in U^{-1}P$.
- Je-li Q prvoideál R je $\{a \in R \mid \exists u \in U: a/u \in Q\}$ prvoideál v R disjunktní s U a $U^{-1}P = Q$.



Lemma 8.12 (VI.3.4)

Bud' S celistvé rozšíření okruhu R . Jsou-li Q_1, Q_2 prvoideály okruhu S takové, že $Q_1 \cap R = Q_2 \cap R$, potom $Q_1 = Q_2$.

Důkaz.

- Položme $Q = Q_1 \cap Q_2$ a označme $P = Q \cap R$ a $U = R \setminus P$.
- Potom $U^{-1}Q$ je prvoideál $U^{-1}S$ a $U^{-1}Q \cap R_P = PR_P$.
- Podle Lemmatu 8.8 je $U^{-1}S$ celistvý nad $U^{-1}R$ a PR_P je jediný maximální ideál okruhu R_P .
- Odtud plyne, že $U^{-1}Q$ je maximální ideál $U^{-1}S$.
- Z maximality $U^{-1}Q$ plyne, že $U^{-1}Q = U^{-1}Q_1 = U^{-1}Q_2$.
- Podle Lemmatu 8.11 to znamená, že $Q = Q_1 = Q_2$.



Tvrzení 8.13 (VI.3.5)

Bud' S celistvé rozšíření okruhu R . Pro každý prvoideál P okruhu R existuje prvoideál Q okruhu S tak, že $P = Q \cap R$.

Důkaz.

- Označme $U = R \setminus P$. V $U^{-1}S$ zvolme nějaký maximální ideál; podle Lemmatu 8.11 je tvaru $U^{-1}Q$ pro vhodný prvoideál Q okruhu R .
- Podle Lemmat 8.8 a 6.10 je $(U^{-1}Q) \cap R_P$ maximální v R_P . To však znamená, že $(U^{-1}Q) \cap R_P = PR_P = U^{-1}P$.
- Protože $(U^{-1}Q) \cap R_P = U^{-1}(Q \cap R)$, odvodíme z Lemmatu 8.8, že $P = Q \cap R$.



Tvrzení 8.14 (VI.3.6)

Nechť S je celistvé rozšíření okruhu R . Necht' $P_0 \subsetneq P_1$ jsou prvoideály okruhu R a Q_0 je prvoideál S takový, že $Q_0 \cap R = P_0$. Potom existuje prvoideál Q_1 okruhu S tak, že $Q_1 \cap R = P_1$.

Důkaz.

- S/Q_0 je celistvý nad $(R + Q_0)/Q_0 \simeq R/P_0$.
- Podle Tvrzení 8.13 existuje prvoideál Q_1 tak, že

$$Q_1/Q_0 \cap ((R + Q_0)/Q_0) = (P_1 + Q_0)/Q_0.$$

- Odtud plyne, že $P_1 + Q_0 = Q_1 \cap (R + Q_0)$.
- Proto

$$P_1 = R \cap (P_1 + Q_0) = R \cap (Q_1 \cap (R + Q_0)) = Q_1 \cap R.$$



Lemma 8.15 (VI.3.7)

Nechť S je celistvé rozšíření okruhu R . Potom

$$\sqrt{IS} = \{s \in S \mid s^n + \sum_{i=0}^{n-1} a_i s^i = 0, \text{ kde } a_i \in I\}.$$

Důkaz.

- Je-li $s^n + \sum_{i=0}^{n-1} a_i s^i = 0$, je $s^n = -\sum_{i=0}^{n-1} a_i s^i \in IS$ a proto $s \in \sqrt{IS}$.
- Předpokládejme naopak, že $s \in \sqrt{IS}$.
- Potom pro vhodné k je $s^k = \sum_{i < l} b_i t_i$, kde $b_i \in I$ a $t_i \in S$. Položme $A = R[s, t_0, \dots, t_{l-1}]$. Protože je A celistvý nad R je podle Tvzení 6.3 konečně generovaný jako R -modul.
- Navíc $s^k A = (\sum b_i t_i) A \in IA^2 = IA$ a zřejmě je A věrný R -modul. Podle Tvzení 6.1 existují $c_0, \dots, c_{m-1} \in I$ tak, že

$$(s^k)^m + \sum c_i (s^k)^i = 0.$$



Tvrzení 8.16 (VI.3.8)

Bud' R celistvě uzavřený okruh a S jeho celistvé rozšíření. Bud' I ideál okruhu R a označme T podílové těleso R . Potom je každé $s \in IS$ algebraické nad T a všechny koeficienty (mimo vedoucího) minimálního polynomu s leží v $\sqrt{I}$;

Důkaz.

- Protože je S celistvé nad R , je každý prvek $z \in S$ algebraický nad T .
- Bud' $m_{T,s} = \sum a_i x^i$ minimální polynom s nad T . Nejprve ukážeme, že všechny koeficienty tohoto polynomu jsou celistvé nad R a tedy, vzhledem k celistvé uzavřenosti R , $m_{T,s} \in R[x]$.
- Nechť $s_0, \dots, s_{k-1}$ jsou všechny kořeny $m_{T,s}$. Aplikací Lemmatu 8.15 ukážeme, že tyto kořeny jsou celistvé nad R .
- Odtud vyplývá, že $A = R[s_0, \dots, s_{k-1}]$ je konečně generovaný R -modul a všechny koeficienty $m_{T,s}$ padnou do A . Proto jsou nad R celistvé.



Dokončení důkazu Tvzení 8.16.

- Podle Lemmatu 8.15 leží všechny kořeny polynomu $m_{T,s}$ v $\sqrt{IA}$.
- Odtud plyne, že také všechny koeficienty (kromě vedoucího) polynomu $m_{T,s}$ padnou do $\sqrt{IA}$.
- Opět podle Lemmatu 8.15 jsou koeficienty a_i kořeny monických polynomů jejichž koeficienty (kromě vedoucího) leží v I .
- Protože a_i leží v R , leží (znovu podle Lemmatu 8.15) v $\sqrt{IR} = \sqrt{I}$.



Tvrzení 8.17

Bud' R celistvě uzavřený obor integrity, necht' S je celistvé rozšíření R . Necht' $P_0 \subsetneq P_1$ jsou prvoideály oboru R a Q_1 prvoideál S takový, že $Q_1 \cap R = P_1$. Potom existuje prvoideál $Q_0 \subsetneq Q_1$ oboru S takový, že $Q_0 \cap R = P_0$.

Důsledek 8.18 (VI.3.9)

Bud' R celistvě uzavřený obor a S jeho celistvé rozšíření. Necht'

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_{n-1} \subsetneq P_n$$

je řetězec prvoideálů oboru R a Q je prvoideál S takový, že $Q \cap R = P_n$. Potom lze sestavit řetězec

$$Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_{n-1} \subsetneq Q_n = Q$$

prvoideálů S takový, že $Q_j \cap R = P_j$.

Důkaz Tvzení 8.17 - část 1.

- Označme $U = S \setminus Q_1$, $V = R \setminus P_0$ a položme

$$W = \{uv \mid u \in U, v \in V\}.$$

Snadno nahlédneme, že W je multiplikativní množina v S .
Ukážeme, že $P_0 S \cap W = \emptyset$.

- Pro spor předpokládejme, že existuje $s \in P_0 S \cap W$.
- Označme T podílové těleso R . Protože je s celistvý nad R , je algebraický nad T ; buď

$$m_{T,s} = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$$

jeho minimální polynom. Podle Trzení 8.16 jsou $a_i \in \sqrt{P_0} = P_0$.

- Protože $s \in W$ je $s = uv$ pro nějaké $u \in U$ a $v \in V$. Potom $m_{T,s}(uv) = 0$, odkud, po vynásobení v^{-m} dostaneme, že

$$f(u) = u^m + \frac{a_{m-1}}{v}u^{m-1} + \cdots + \frac{a_1}{v^{m-1}}u + \frac{a_0}{v^m} = 0.$$



Důkaz Tvzení 8.17 – část 2.

- Zřejmě $f \in T[x]$ a přímým výpočtem ověříme, že f je nad T nerozložitelný. Proto $f = m_{T,u}$.
- Podle Tvzení 8.16 leží koeficienty f v R (lze také použít Tvzení 6.7).
- Označme $r_i = a_i/v^{m-i}$; koeficienty f . Potom $a_i = r_i v^{m-i} \in P_0$. Protože P_0 je prvoideál a $v \notin P_0$, je nutně $r_i \in P_0$.
- Potom podle Tvzení 8.16 $u \in \sqrt{P_0 S} \subseteq \sqrt{Q_1} = Q_1$, což je spor s tím, že $u \in U = S \setminus Q_1$. Ukázali jsme tak, že $P_0 S \cap W = \emptyset$.
- Podle Tvzení 1.27 existuje prvoideál Q_0 oboru S tak, že $Q_0 \cap W = \emptyset$ a $P_0 S \subseteq Q_0$, speciálně $P_0 \subseteq Q_0$.
- Zřejmě $1 \in U \cap V$, odkud plyne $U \cap V \subseteq W$. Odtud dostaneme, že $Q_0 \cap R = P_0$ a $Q_0 \subseteq Q_1$, přitom zde nenastane rovnost, protože $P_0 \neq P_1 = Q_1 \cap R$.



Definice

- Bud' P prvoideál okruhu R . **Výškou** prvoideálu P , značíme $\text{ht}_R P$ nebo jen $\text{ht} P$, nazvěme supremum délek všech řetězců

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = P$$

prvoideálů R .

- Dimenzi** okruhu R definujeme jako

$$\dim R = \sup\{\text{ht}_R P \mid P \text{ je prvoideál } R\}.$$

Lemma 8.19

Bud' P prvoideál okruhu R a U multiplikativní množina v R taková, že $P \cap U = \emptyset$. Potom platí

- ① $\text{ht} P + \dim R/P \leq \dim R$;
- ② $\text{ht} P = \dim R_P$;
- ③ $\text{ht} P = \text{ht} U^{-1} P$;

Tvrzení 8.20 (VI.4.1)

Je-li S celistvý nad okruhem R , platí $\dim R = \dim S$.

Důkaz.

- Je-li $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_n$ ostře rostoucí řetězec prvoideálů S , je podle Tvrzení 8.12 $(Q_0 \cap R) \subsetneq (Q_1 \cap R) \subsetneq \cdots \subsetneq (Q_n \cap R)$ ostře rostoucí řetězec prvoideálů R . Proto $\dim R \geq \dim S$.
- Naopak podle Tvrzení 8.13 a 8.14 je možné každý řetězec $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ prvoideálů R zvednout na řetězec $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_n$ prvoideálů S tak, že $Q_i \cap R = P_i$. Odtud $\dim R \leq \dim S$. □

Důsledek 8.21 (VI.4.2)

Je-li S celistvý nad okruhem R a I je vlastní ideál S , platí $\dim R/(R \cap I) = \dim S/I$.

Tvrzení 8.22 (VI.4.3)

Nechť R je celistvě uzavřený obor a S je jeho celistvé rozšíření. Potom pro každý prvoideál Q oboru S platí $\text{ht}_S Q = \text{ht}_R(Q \cap R)$.

Důkaz.

- Z Tvrzení 8.12 snadno plyne, že $\text{ht}_S Q \leq \text{ht}_R(Q \cap R)$.
- Bud'

$$P_0 \subseteq P_1 \subseteq \cdots \subseteq P_n = Q \cap R$$

řetězec prvoideálů v R . Podle Důsledku 8.18 lze tento řetězec zvednout na řetězec

$$Q_0 \subseteq Q_1 \subseteq \cdots \subseteq Q_n = Q$$

provoideálů S takový, že $Q_i \cap R = P_i$. Odtud plyne, že $\text{ht}_S Q \geq \text{ht}_R(Q \cap R)$.



Věta 8.23 (VI.4.4)

Bud' A netriviální afinní alebra nad nekomutativním tělesem K . Potom mají všechny noetherovské normalizace algebry A stejný počet prvků a ten je roven dimenzi A .

Důsledek 8.24 (VI.4.5)

Bud' A obor integrity, který je afinní K -algebrou, kde K je komutativní těleso. Označme T podlové těleso A . Potom

$$\dim A = [T : K]_{\text{tr}}.$$

Důkaz Věty 8.23 - část 1.

- Buď $y_0, \dots, y_{n-1}$ nějaká noetherovská normalizace A , tj., $y_0, \dots, y_{n-1}$ jsou nad K algebraicky nezávislé a A je celistvým rozšířením $K[y_0, \dots, y_{n-1}]$.
- Podle Tvrzení 8.20 je $\dim A = \dim K[y_0, \dots, y_{n-1}] \geq n$, neboť

$$0 \subsetneq (y_0) \subsetneq (y_0, y_1) \subsetneq \dots \subsetneq (y_0, \dots, y_{n-1})$$
 je řetězec prvoideálů v $K[y_0, \dots, y_{n-1}]$.
- Indukcí podle n ukážeme, že $n \geq \dim A$. V případě, že $n = 0$, je A celistvé nad K a $\dim A = \dim K = 0$, podle Tvrzení 8.20 (také lze použít Tvrzení 6.9).
- Předpokládejme, že $n > 0$ a dokazované platí pro každé nezáporné $n' < n$.
- Buď $P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_m$ řetězec prvoideálů v $K[y_0, \dots, y_{n-1}]$. Z indukčního předpokladu odvodíme, že $m \leq n$.



Důkaz Věty 8.23 - část 2.

- Podle Tvzení 8.4 existuje noetherovská normalizace $z_0, \dots, z_{n-1}$ okruhu $K[y_0, \dots, y_{n-1}]$ a nezáporné $d \leq n$ takové, že

$$P_1 \cap K[z_0, \dots, z_{n-1}] = \sum_{i < d} K[z_0, \dots, z_{n-1}].$$

- $K[y_0, \dots, y_{n-1}]$ je celistvé nad $K[z_0, \dots, z_{n-1}]$ a podle Tvzení 8.12 je tak $P_0 \cap K[z_0, \dots, z_{n-1}] \subsetneq P_1 \cap K[z_0, \dots, z_{n-1}]$, odkud plyne $P_1 \cap K[z_0, \dots, z_{n-1}] \neq 0$. Proto $0 < d$.
- Uvažme nyní přirozenou projekci "

$$\pi: K[y_0, \dots, y_{n-1}] \rightarrow K[y_0, \dots, y_{n-1}]/P_1.$$

- Z Lemmatu 8.5 plyne, že $\pi(z_d), \dots, \pi(z_{n-1})$ tvoří noetherovskou normalizaci faktoragebry $K[y_0, \dots, y_{n-1}]/P_1$. Zároveň v ní tvoří faktory $P_1/P_1 \subsetneq \dots \subsetneq P_m/P_1$ rostocí řetězec prvoideálů.
- Protože $0 < d$, plyne z indukčního předpokladu, že $m - 1 \leq n - d$, odkud dostáváme $m \leq n$. □

Definice

Řekneme, že prvoideál Q_1 **pokrývá** prvoideál Q_0 , jestliže $Q_0 \subsetneq Q_1$ a neexistuje prvoideál P takový, že $Q_0 \subsetneq P \subsetneq Q_1$.

Lemma 8.25

Bud' $y_0, \dots, y_{n-1}$ noetherovská normalizace afinní K -algebry A . Pokud Q_1 pokrývá prvoideál Q_0 , tak $Q_1 \cap K[y_0, \dots, y_{n-1}]$ pokrývá $Q_0 \cap K[y_0, \dots, y_{n-1}]$ v $K[y_0, \dots, y_{n-1}]$.

Věta 8.26

Bud' A obor integrity, který je n -dimenzionální afinní K -algebrou. Potom má každý maximální ostře rostoucí řetězec prvoideálů v K délku n .

Definice

- Okruh R nazveme **valuačním okruhem** tělesa T , jestliže pro každé $a \in T$ leží alespoň jeden z prvků a , a^{-1} v R .
- Obor integrity R je **valuační obor** je-li valuačním okruhem svého podílového tělesa.

Tvrzení 8.27 (VI.5.1)

Obor R je valuačním oborem nějakého tělesa právě když jsou jeho ideály lineárně uspořádány.

Důkaz.

- Necht' $J \not\subseteq I$ jsou ideály R . Zvolme $b \in J \setminus I$.
- Bud' $a \in I$ libovolné. Protože $b = a(b/a) \notin I$, platí $b/a \notin R$. Protože R je valuační obor, nutně $a/b \in R$, odkud $a = (a/b)b \in J$. Proto $I \subseteq J$.
- Naopak předpokládejme, že R je obor, a že jsou jeho ideály lineárně uspořádány. Bud' T podílové těleso R a $a = b/c \in T$ nenulový prvek.
- Je buďto $bR \subseteq cR$, nebo $cR \subseteq bR$. V prvním případě $a = b/c \in R$, ve druhém $a^{-1} = c/b \in R$. Proto je R valuační obor.



Lemma 8.28 (Nakayamovo lemma)

Nakayama Bud' M konečně generovaný R -modul takový, že $JM = M$, kde J je Jacobsonův radikál okruhu R . Potom je $M = 0$.

Důkaz.

- Protože M je konečně generovaný a $JM = M$, existuje podle Tvzení 6.1 prvek $a \in J$ tak, že $(1 - a)M = 0$.
- Podle Tvzení 1.29 je $1 - a$ invertibilní, odkud již plyne $M = 0$ □

Důsledek 8.29

Konečně generovaný modul M takový, že $QM = M$ pro každý maximální ideál Q je nulový.

Tvzení 8.30 (VI.5.3)

Bud' R valuační obor který není tělesem. Označme P jeho maximální ideál a položme $I = \bigcap P^n$. Předpokládejme, že P je konečně generovaný. Potom v řetězci

$$I \subsetneq \dots \subsetneq P^{n+1} \subsetneq P^n \subsetneq \dots \subsetneq P^2 \subsetneq P \subsetneq R$$

leží všechny ideály obsahující I . Je-li navíc I konečně generovaný, potom je $I = 0$.

Důkaz Tvrzení 8.30.

- Každý konečně generovaný ideál valuačního oboru je hlavní. Speciálně je P hlavní ideál; buď $P = aR$.
- Snadno nahlédneme, že $P^n = a^n R$ a že $a^n \notin a^{n+1} R$.
- Nechť $b \in a^n R \setminus a^{n+1} R$. Potom $b = ca^n$ pro nějaké c . Nutně $c \notin P$ a tedy c je invertibilní. Proto $a^n = c^{-1}b$ a $bR = a^n R$. Odtud plyne první část tvrzení.
- Je-li I konečně generovaný, je hlavní. Buď d jeho generátor. Protože $d \in P$, existuje e tak, že $d = ea$.
- Nutně je $e \in I$ (jinak by platilo, že $eR = P^n$ pro nějaké n a $I = P^{n+1}$). Proto $PI = I$, odkud podle Důsledku 8.29 $I = 0$.



Definice

Valuační obor nazveme **diskrétní** je-li jeho maximální ideál P konečně generovaný a ideál $\bigcap P^n$ nulový.

Poznámka

Z Tvrzení 8.30 plyne, že diskrétní valuační obory jsou právě valuační obory, které jsou noetherovské a, po krátkém zamyšlení, že to jsou právě právě valuační obory, které jsou Dedekindovy.

Definice

Buď T těleso. Uvažme zobrazení $\nu: T^* \rightarrow \mathbb{Z}$ a položme $\nu(0) = \infty$. Zobrazení ν nazveme **diskrétní valuací** jestliže je na a a platí

- ① $\nu(a + b) \geq \min\{\nu(a), \nu(b)\}$;
- ② $\nu(ab) = \nu(a) + \nu(b)$;

Tvrzení 8.31 (VI.5.5)

Bud' R diskretní valuační obor a T jeho podílové těleso. Bud' a generátor maximálního ideálu v R . Potom platí:

① *posloupnost*

$$0 \subsetneq \cdots \subsetneq a^n R \subsetneq \cdots \subsetneq a^m R \subsetneq \cdots \subsetneq T, \quad (n \geq m \vee \mathbb{Z})$$

je tvořena právě všemi R -podmoduly tělesa T ;

② *definujeme-li $\nu: T^* \rightarrow \mathbb{Z}$ tak, že $\nu(b) = n$ právě když $Rb = Ra^n$, je ν diskretní valuací tělesa T ;*

Důkaz.

- Nejprve ukážeme, že pro každé $b \in T^*$ existuje $i \in \mathbb{Z}$ tak, že $bR = a^i R$. Pro nenulové $b \in R$ je to zřejmé.
- Pokud $b \notin R$, je $b^{-1} \in R$ a $b^{-1}R = a^i R$ pro vhodné $i \in \mathbb{N}$. Potom $bR = ba^{-i}a^iR = ba^{-i}b^{-1}R = a^{-i}R$.
- Odtud snadno odvodíme (1). Druhá část tvrzení je snadná. □

Tvzení 8.32 (VI.5.6)

Bud' $\nu: T^* \rightarrow \mathbb{Z}$ diskretní valuace tělesa T . Potom je $R = \{a \in T \mid \nu(a) \geq 0\}$ diskretní valuační okruh a ν je jediná valuace, která jej takto určuje.

Důkaz.

- Z vlastností valuace snadno odvodíme, že R je okruh a že $\nu(1) = 0$.
- Odtud $\nu(a^{-1}) = -\nu(a)$ a $a \in T$ je invertibilní prvek R právě když $\nu(a) = 0$.
- Dále pro $a, b \in R$ platí, že $\nu(b) \geq \nu(a)$ právě když $bR \subseteq aR$.
- Navíc, protože je ν na, existuje $a \in R$ tak, že $\nu(a) = 1$. Potom je $\nu(a^n) = n$, $a^n R$, $n \geq 0$ jsou všechny nenulové ideály R a R je diskretní valuační okruh.



KONEC