Komutativní okruhy
Teorie těles a její aplikace

Pavel Růžička

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

Zimní Semestr, 2008

Teorie těles a její aplikace

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:

Eukleidův obor
$\Downarrow$
Obor hlavních ideálů (PID) $\Longrightarrow$ *Dedekindův obor*
$\Downarrow$ $\Downarrow$
Gaussův obor (UFD) Noetherovský obor

Buď 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

Buď 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 $N\colon R \to \mathbb{N}_0$ 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 $N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2$;
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 neprázdná 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 $a_1, a_2, \ldots, a_n$ budeme značit $(a_1, a_2, \ldots, a_n)$.

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

1. 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;
2. Obor $\mathbb{Z}[\sqrt{-2}] = \{\alpha = a + \sqrt{-2}b \mid a, b \in \mathbb{Z}\}$ s normou $N(\alpha) = \alpha\overline{\alpha} = a^2 + 2b^2$ je Eukleidův;
3. Obor $\mathbb{Z}[\zeta] = \{\alpha = a + \zeta b \mid a, b \in \mathbb{Z}\}$, kde $\zeta = e^{i\frac{2\pi}{3}}$ s normou $N(\alpha) = \alpha\overline{\alpha} = a^2 + ab + b^2$ je Eukleidův;
4. Obor $\mathbb{Z}[\beta]$, kde $\beta = \frac{1}{2}(1 + \sqrt{-19})$ je obor hlavních ideálů, ale není Eukleidův;
5. 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)

Buď 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 $\{1, 2, \ldots, n\}$ taková, že $b_i \sim c_{\sigma(i)}$ pro každé $i \in \{1, 2, \ldots, n\}$.

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)

Buď 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 sestrojit následující posloupnost polynomů:
  - $f_0 = 0$;
  - f_{n+1} je polynom nejmenšího stupně z polynomů v (neprázdné) množině $I \setminus (f_0, f_1, \ldots, f_n)$;
- Označme a_n vedoucí koeficient polynomu f_n a s_n jeho stupeň.
- Z konstrukce plyne, že $s_0 \leq s_1 \leq s_2 \leq \ldots$.

Dokončení důkazu Věty 1.10.

- Označme $J_n = (a_0, a_1, \ldots, a_n)$.
- Protože $J_0 \subseteq J_1 \subseteq J_2 \subseteq \ldots$ a R je dle předpokladu noetherovský, existuje k tak, že $J_k = J_{k+1}$.
- To znamená, že $a_{k+1} \in (a_0, a_1, \ldots, a_k)$, 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 $(f_0, f_1, \ldots, f_k)$.
- To je spor.

□

Důsledek 1.11 (I.2.2)

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

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 $R[x_1, x_2, \ldots, x_n]$ 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.

Buď R Gaussův obor a T jeho podílové těleso. Nechť $p \in R$ 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 $f = a_n x^n + \cdots + a_1 x + a_0$ položíme $\mathbf{c}_p(f) = \min\{\mathbf{v}_p(a_i) \mid i = 0, 1, \ldots, n\}$.

Lemma 1.15 (I.2.3)

Buď R Gaussův obor, T jeho podílové těleso a p ∈ R nerozložitelný prvek. Pro nenulové u ∈ T a f ∈ 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

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

Tvrzení 1.18 (I.2.6)

Buď 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 Tvrzení 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 Tvrzení 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 $g = a \in R$.
- Buď $p \in R$ 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.

- Buď $(f_1) \subseteq (f_2) \subseteq \dots$ 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

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

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 $\pi\colon R/I \times R/J \to R/(I+J) \times R/(I+J)$.
- 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 $I_1, I_2, \ldots, I_n$ 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 $I_1, I_2, \ldots, I_n$ jsou ideály okruhu R. Uvažme homomorfismus

$$\varphi\colon R \to (R/I_1) \times (R/I_2) \times \cdots \times (R/I_n),$$

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

Potom

1. *φ je na právě když jsou ideály $I_1, I_2, \ldots, I_n$ po dvou komaximální;*
2. $\ker \varphi = I_1 \cap I_2 \cap \cdots \cap I_n$;

Důkaz.

Indukcí s využitím Lemmatu 1.20 a Tvrzení 1.21. □

Důsledek 1.23 (I.3.3)

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

$$f\colon R \to (R/I_1) \times (R/I_2) \times \cdots \times (R/I_n),$$

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

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

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

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

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 $n_1, n_2, \ldots, n_k$ a nezáporná celá čísla $r_1, r_2, \ldots, r_k$ taková, že $r_i < n_i$. Potom má soustava rovnic

$$\begin{aligned} x &\equiv r_1 \pmod{n_1} \\ x &\equiv r_2 \pmod{n_2} \\ &\vdots \\ x &\equiv r_k \pmod{n_k} \end{aligned}$$

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 nazýva multiplikativní podmnožina R.

Tvrzení 1.27 (I.3.7)

Buď 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 (I.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

$$\mu\colon \bigoplus M_i \to M, \quad (m_i) \mapsto \sum m_i.$$

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);*

Nechť 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 $f\colon B \to M$ existuje právě jeden homomorfismus $\varphi\colon F \to M$ 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)

Buď 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 $\iota\colon R^{(B)} \to F$ rozšiřující identické vnoření $i\colon B \to F$ je izomorfismus.*

Tvrzení 2.5 (I.4.11)

Buď 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 $e_1, e_2, \ldots, e_n$ volná báze F a $a = \sum r_i e_i$;
- Označme $C(a)$ ideál R generovaný prvky $r_1, r_2, \ldots, r_n$.
- 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 $e_1, e_2, \ldots, e_n$ 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 Tvrzení 2.6.

- Tvrzení ukážeme indukcí podle n. Pro $n = 1$ není co dokazovat.
- Buď $a = \sum r_i e_i$ a položme $b = a - r_1 e_1$.
- Podle indukčního předpokladu existuje báze $e_1, f_2, f_3, \ldots, f_n$ 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 $xu + yv = 1$.
- Položme $g_1 = ue_1 + vf_2$, $g_2 = -ye_1 + xf_2$ a $g_j = f_j$ pro $j = 3, \ldots, n$.
- Potom je $g_1, g_2, \ldots, g_n$ volná báze F taková, že $a = sg_1$.

□

Důkaz Tvrzení 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 Tvrzení 2.6 existuje báze $e_1, e_2, \ldots, e_n$ 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 $a = xc + yb = xse_1 + y \sum r_i e_i = te_1 + y \sum_{i=2} r_i e_i$.
- 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 $i = 2, \ldots, n$.
- Zároveň ale $t \in (s)$ a tedy $(s) = (t) = (s, r_1)$. Proto také $r_1 \in (s)$.

Definice

Buď R okruh a M modul nad R.

- Pro $a \in M$ položme

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

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

- Množina

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

  tvoří podmodul M, který nazveme torzní část M.

Definice

Buď R obor integrity. Modul M nazveme

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

Lemma 2.8 (I.5.2)

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

Tvrzení 2.9 (I.5.4)

Konečně generovaný beztorzní modul nad oborem hlavních ideálů je volný.

Důkaz.

- Existuje projekce $\varphi\colon F \to M$ 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 Tvrzení 2.6 existují báze $e_1, e_2, \ldots, e_n$ a $s \in R$ tak, že $c = se_1$. Protože $c \neq 0$ je také $s \neq 0$.
- Pak ale $s \in \mathrm{Ann}\varphi(e_1)$, odkud plyne $\varphi(e_1) = 0$. To vede ke sporu s minimalitou n. □

Důsledek 2.10 (I.5.6)

Buď 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 definujme

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

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 Tvrzení 2.11.

- Nejprve ukážeme, že $M = \sum \tau_P(M)$.
- Zvolme $u \in M$ a buď $r \in \mathrm{Ann}(u)$ 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 $P \subseteq \mathrm{Ann}(M_{n+1}^p/M_n^p)$ a na M_{n+1}^p/M_n^p lze nahlížet jako na vektorový prostor nad R/P.

Tvrzení 2.12 (I.5.7)

Buď 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.

- Buď M konečně generovaný p-modul. Buď k nejmenší takové, že $M = M_k^p$.
- Je-li $k = 0$ je i 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 $u_1, u_2, \ldots, u_s$ 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 $r_i u_i \in M_1^p$.
- Buď $r_i = p^{m_i} x_i$, 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 indučního 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 $p_i^m x_i u_i = 0$ podle Tvrzení 2.12.
- Buď $M_1^p = (N \cap M_1^p) \oplus K$.
- 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 bež k je roven dimenzi M^p_{k+1}/M^p_k. □

Věta 2.14 (I.5.11)

Buď 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 $e_1, e_2, \ldots, e_n$ modulu F a klesající posloupnost ideálů $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n$ 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 $f_1, f_2, \ldots, f_n$ 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 $e_2, \ldots, e_n$ modulu F' a prvky $s_2, \ldots, s_n$ okruhu R splňující $(s_2) \supseteq \cdots \supseteq (s_n)$ tak, že $M' = \bigoplus Rs_ie_i$.
- 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 $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n$ a $M = \bigoplus I_ie_i$.

□

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 $e_1, e_2, \ldots, e_n$ modulu F a prvky $r_1, r_2, \ldots, r_n$ okruhu R spňující $r_i \mid r_j$ pro $i \leq j$ takové, že $M = \bigoplus Rr_ie_i$.

Je-li k největší takové, že $r_k \neq 0$, tvoří prvky $r_1e_1, r_2e_2, \ldots, r_ke_k$ 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)

Buď 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 $(I_i : J) = (J_i : J)$ pro každé $i = 1, \ldots, n$.
- Protože J je největší z ideálů I_i, J_j, jsou podle Lemmatu 2.18 $I_i = J_i$.

□

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;
- Buď $T \leq U$ rozšíření. Množina

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

  tvoří těleso nazývané algebraický uzávěr T v U.
- Těleso ja algebraicky uzavřené nemá-li vlastní algebraické rozšíření.
- Algebraický uzávěr tělesa je jeho algebraické, algebraicky uzavřené rozšíření.

Definice

Buď $T \leq U$ 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.

- Buď $T \leq U$, $T \leq V$ dvojice rozšíření. Homomorfismus $f : U \to V$, 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

Buď $T \leq U$ 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.*
- *Algebrackés uzávěry tělesa T jsou T-izomorfní.*

Prvotěleso

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

Konečná charakteristika

- Je-li T těleso konečné charakterisitiky p, určuje přiřazení $x \mapsto x^p$ endomorfisus 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.

Nechť $T \leq U$, $T \leq V$ jsou rozšíření. Množinu všech T-homomorfismů z U do V budeme značit $\hom_T(U, V)$.

Definice

Nechť $T \leq U \leq W$ jsou algebraická rozšíření, kde W je algebraicky uzavřené. Mohutnost množiny $\hom_T(U, W)$ nazveme stupeň separability U nad T a označíme $[U : T]_S$.

Lemma 3.4

Nechť $T \leq U \leq W$ jsou algebraická rozšíření a W je algebraicky uzavřené. Potom

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

Lemma 3.5 (II.2.1)

Nechť $T \leq U \leq V \leq W$ je posloupnost algebraických rozšíření těles, přičemž W je algebraicky uzavřené. Pro každé $\varphi \in \hom_T(U, W)$ zvolme rozšíření $\overline{\varphi} \in \hom_T(W, W)$ (které existuje a je automorfismem podle předcházejícího lemmatu). Potom přiřazení $(\psi, \varphi) \mapsto \overline{\varphi} \circ \psi$ určuje bijekci

$$\hom_U(V, W) \times \hom_T(U, W) \to \hom_T(V, W).$$

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)

Buď $T \leq U$ 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.

Buď $T \leq U$ 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 buď $\alpha \in U$ zvoleno tak, že je stupeň $[T(\alpha) : T]$ maximální. Pro spor předpokládejme, že existuje $\beta \in U \setminus T(\alpha)$. Označme $V = T(\alpha, \beta)$.
- Buď $\hom_T(V, K) = \{f_1, f_2, \ldots, f_n\}$. 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

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

  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 $f \in \hom_T(U, W)$, 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.

Buď $\mathcal{M} \subset T[x]$ 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)

Buď $T \leq U$ rozšíření. Uvažme mezitěleso 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.

Buď $T \leq U$ algebraické rozšíření. Označme

$$\mathrm{Gal}(U, T) = \hom_T(U, U).$$

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

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

Tvrzení 3.17 (II.3.7)

Buď $T \leq U$ rozšíření a $G \subseteq \mathrm{Aut}(U)$. Potom

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

Lemma 3.18 (II.3.2)

Buď U těleso a nechť G je n-prvková podgrupa grupy $\mathrm{Aut}(U)$. Potom je U separabilní rozšíření tělesa $\mathrm{Fix}(U, G)$ stupně n a platí, že

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

Důkaz.

- Označme $T = \mathrm{Fix}(U, G)$. 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

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

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

Lemma 3.19 (II.3.8)

Buď $T \leq U$ Galoisovo rozšíření. Potom

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

Důkaz.

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

Lemma 3.20 (II.3.9)

Buď U těleso a nechť $G \leq \mathrm{Aut}(U)$. Potom pro každé $f \in \mathrm{Aut}(U)$ platí

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

Důkaz.

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

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

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

- Podobně platí

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

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

Definice

- Mějme uspořádané množiny A, B. Zobrazení $\alpha\colon A \to B$ 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 $\alpha\colon A \to B$ a $\beta\colon B \to A$ 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)

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

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

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

2. *Normální rozšíření T odpovídají normálním podgrupám grupy $\mathrm{Gal}(U, T)$.*

3. *Je-li $T \leq V (\leq U)$ normální rozšíření, platí*

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

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 $g \in \mathrm{Gal}(U, T)$ je potom $g^{-1}(V) = V$.
- Proto pro libovolná $h \in \mathrm{Gal}(U, V)$ a $v \in V$ platí $ghg^{-1}(v) = gg^{-1}(v) = v$ a tedy $ghg^{-1} \in \mathrm{Gal}(U, V)$. To znamená, že $\mathrm{Gal}(U, V) \trianglelefteq \mathrm{Gal}(U, T)$.
- Buď $G \trianglelefteq \mathrm{Gal}(U, T)$. Pro libovolné $f \in \mathrm{Gal}(U, T)$ pak máme podle Lemmatu 3.20 $f(\mathrm{Fix}(U, G)) = \mathrm{Fix}(U, fGf^{-1}) = \mathrm{Fix}(U, G)$.
- Z normality U nad T pak plyne normalita $\mathrm{Fix}(U, G)$ nad T.
- Přiřazení $f \mapsto f \restriction V$ určuje homomorfismus z $\mathrm{Gal}(U, T)$ na $\mathrm{Gal}(V, T)$ jehož jádrem je právě grupa $\mathrm{Gal}(U, V)$. 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 $\mathrm{Gal}(U, T)$ Abelova.

Důkaz.

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

Lemma 3.26

Buď T těleso, $a \in T$ a nechť U je rozkladové nadtěleso polynomu $x^n - a$. Pokud T obsahuje rozkladové nadtěleso polynomu $x^n - 1$, je grupa $\mathrm{Gal}(U, T)$ Abelova.

Důkaz.

- Buď 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 $\alpha \mapsto \beta\alpha$.
- Nechť $\varphi\colon \alpha \mapsto \beta\alpha$ a $\psi\colon \alpha \mapsto \gamma\alpha$ 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 $\mathrm{Gal}(U, T)$ 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 $G_0, \ldots, G_n$ 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

Buď $T \leq U$, kde U je rozkladové nadtěleso polynomu $x^n - a$ nad T. Pokud charakteristika tělesa T nedělí n, je $\mathrm{Gal}(U, T)$ 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.
- Nechť $\alpha_1, \ldots, \alpha_n$ 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.
- Buď 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 $\mathrm{Gal}(U, V)$ Abelova.
- Podle lemmatu 3.25 je grupa $\mathrm{Gal}(V, T)$ Abelova.
- Podle Věty 3.23 je $\mathrm{Gal}(U, V) \trianglelefteq \mathrm{Gal}(U, T)$ a platí

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

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

Definice

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

Lemma 3.30

Normální uzávěr radikálového rozšíření je opět radikálové rozšíření.

Důkaz.

- Buď $T \leq T(\alpha_1, \ldots, \alpha_m)$ radikálové a U jeho normální uzávěr.
- Důkaz provedeme indukcí podle m. Označme ještě V normální uzávěr rošíření $T \leq T(\alpha_1, \ldots, \alpha_{m-1})$. 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.
- Prototože $\alpha_m^{n_m} \in V$, 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 $T \leq U = T(\alpha_1, \ldots, \alpha_n)$, kde $\alpha_j^{n_j} \in T(\alpha_1, \ldots, \alpha_{j-1})$, normální radikálové rozšíření a charakteristika T nedělí n_j, je grupa $\mathrm{Gal}(U, T)$ řešitelná.

Důkaz.

- Tvrzení 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 $U = V(\alpha_2, \ldots, \alpha_n)$ normální radikálové rozšíření a dle indukčního předpokladu je grupa $\mathrm{Gal}(U, V)$ řešitelná.
- Podle Lemmatu 3.29 je grupa $\mathrm{Gal}(V, T)$ řešitelná a podle Věty 3.23 je $\mathrm{Gal}(U, V) \trianglelefteq \mathrm{Gal}(U, T)$ a platí

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

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

Definice

Nechť 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

Nechť T je těleso, $f \in T[x]$ a U rozkladové nadtěleso f. Galoisovou grupou polynomu f (nad T) rozumíme grupu $\mathrm{Gal}(U, T)$.

Věta 3.32

Buď 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 $\mathrm{Gal}(V : T)$ řešitelná.
- Rozšíření $T \leq U$ je normální a tedy podle Věty 3.23 je

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

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

Definice

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

Lemma 3.33

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

Věta 3.34

Buď $f \in \mathbb{Q}[x]$ 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 $x^5 - npx + p = 0$ pro $n > 1$ není řešitelná pomocí radikálů.

- Uvažme rozšíření $T \leq U$ konečného stupně n a zvolme bázi $\mathbf{e} = (e_1, e_1, \ldots, e_n)$ 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 $\mathbf{M_e}(\alpha)$.

Definice

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

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

$$c_\alpha = \det(x\mathbf{I}_n - \mathbf{M_e}(\alpha)) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0.$$

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

Tvrzení 4.1 (II.5.1)

Buď $T \leq U$ rozšíření konečného stupně n a nechť $\alpha \in U$. Potom

1. $c_\alpha = m_{\alpha,T}^d$, *kde* $d = [U : T(\alpha)]$;
2. $\mathrm{N}_{U|T}(\alpha) = (-1)^n c_0 = (-1)^n a_0^d = (\mathrm{N}_{T(\alpha)|T}(\alpha))^d$;
3. $\mathrm{Tr}_{U|T}(\alpha) = -c_{n-1} = d\mathrm{Tr}_{T(\alpha)|T}(\alpha)$;

Tvrzení 4.2 (II.5.2)

Buď $T \leq U$ separabilní rozšíření a $\alpha \in U$. Potom

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

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

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

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

Máme tak grupové homomorfismy $\mathrm{N}_{U|T} \colon (U^*, .) \to (T^*, .)$ a $\mathrm{Tr}_{U|T} \colon (U, +) \to (T, +)$.

Tvrzení 4.3

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

1. $\mathrm{Tr}_{V|T} = \mathrm{Tr}_{U|T} \circ \mathrm{Tr}_{V|U}$;
2. $\mathrm{N}_{V|T} = \mathrm{N}_{U|T} \circ \mathrm{N}_{V|U}$;

Definice

Buď $T \leq U$ separabilní rozšíření stupně n a $\alpha_1, \alpha_2, \ldots, \alpha_n \in U$.
Definujeme diskriminant jako $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det(\mathrm{Tr}_{U|T}(\alpha_i\alpha_j))$.

Lemma 4.4 (II.5.5)

Buď W algebraický uzávěr U a $\hom_T(U, W) = \{g_1, g_2, \ldots, g_n\}$.
Položme $\mathbf{M} = (g_i(\alpha_j))$. Potom $\mathbf{M}\mathbf{M}^T = (\mathrm{Tr}_{U|T}(\alpha_i\alpha_j))$ a tedy
$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det \mathbf{M}^2$.

Tvrzení 4.5 (II.5.6)

- *Zobrazení $(\alpha, \beta) \mapsto \mathrm{Tr}_{U|T}(\alpha\beta)$ je nedegenerovanou symetrickou bilineární formou $U \times U \to T$;*
- *Jsou-li $\alpha_1, \alpha_2, \ldots, \alpha_n$ a $\beta_1, \beta_2, \ldots, \beta_n$ dvě báze U nad T a $\mathbf{P} = (p_{ij})$, kde $\beta_j = \sum p_{ij}\beta_i$, platí*

$$\Delta(\beta_1, \beta_2, \ldots, \beta_n) = (\det \mathbf{P})^2 \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0.$$

Lemma 4.6 (II.5.4)

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

Tvrzení 4.7 (II.5.7)

Buď $T \leq T(\gamma)$ 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. $\Delta(1, \gamma, \dots, \gamma^{n-1}) = (-1)^{\binom{n}{2}} \mathrm{N}_{U|T}(m'_{\gamma,T}(\gamma))$.

Lemma 4.8 (II.6.1)

Buď $T \leq U$ rozšíření. Pro každou podmnožinu $M \subseteq U$ platí, že $T(M)$ sestává právě ze všech prvků tvaru $p(\alpha_1, \alpha_2, \ldots, \alpha_n)/q(\beta_1, \beta_2, \ldots, \beta_n)$, kde $q(\beta_1, \beta_2, \ldots, \beta_n) \neq 0$, $p, q \in T[x_1, x_2, \ldots, x_n]$ a $\alpha_i, \beta_i \in M$.

Definice

1. Podmnožinu $M \subseteq U$ nazveme algebraicky nezávislou (nad T) jestliže $p(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$ pro každé po dvou různé $\alpha_1, \alpha_2, \ldots, \alpha_n$ a každý polynom $p(x_1, x_2, \ldots, x_n) \in T[x_1, x_2, \ldots, x_n]$.
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

Nechť 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)

Nechť 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)

Buď 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

Buď $T \leq U$ rozšíření.

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

Tvrzení 4.15 (II.6.8)

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

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

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

Lemma 5.1 (II.7.1)

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

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)

Buď 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)

Buď R noetherovský okruh. Nechť $S_1 \leq S_2$ 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.
- Buď M množina generátorů S_2 jako S_1-modulu a C množina generátorů S_2 jako R-algebry.
- Pro každé $c \in C$ a $m \in M$ nechť

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

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

Dokončení důkazu Tvrzení 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 $c_1, c_2, \ldots, c_k \in C$ 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 $c_1 c_2 \ldots c_k = a c_k = \sum_m s_m c_k m =$

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

Lemma 5.6 (II.7.6)

Buď T těleso. Okruh $T(x_1, \ldots, x_n)$ není jako T-algebra konečně generovaný.

Důkaz.

- Pro spor předpokládejme, že $T(x_1, \ldots, x_n)$ je konečně generováno prvky $g_1, \ldots, g_k$.
- Buď $g_i = p_i/q_i$, kde $p_i, q_i \in T[x_1, \ldots, x_n]$.
- Alespoň jeden z polynomů q_i je nenulového stupně, jinak by $g_1, \ldots, g_k \in T[x_1, \ldots, x_n]$ a T-algebry $T[x_1, \ldots, x_n]$ a $T(x_1, \ldots, x_n)$ by se rovnaly.
- Potom lze každý prvek $T(x_1, \ldots, x_n)$ vyjádřit ve tvaru $a/(q_1^{\alpha_1} \cdots q_k^{\alpha_k})$ pro nějaké $a \in T[x_1, \ldots, x_n]$ 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

Buď 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)

Buď T těleso a $\alpha_1, \ldots, \alpha_n \in T$. Potom

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

Důkaz Lemmatu 5.8.

- Buď $f \in T[x_1, \ldots, x_n]$. 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 $g_n \in T[x_1, \ldots, x_n]$ a $f_{n-1} \in T[x_1, \ldots, x_{n-1}]$.
- Podobně dostaneme $f_{n-1} = g_{n-1}(x_{n-1} - \alpha_{n-1}) + f_{n-1}$, kde $g_{n-1} \in T[x_1, \ldots, x_{n-1}]$ a $f_{n-2} \in T[x_1, \ldots, x_{n-2}]$.
- 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 $S = K[x_1, \ldots, x_n]$. Potom

1. *Ideál M okruhu S je maximální právě když existují $\alpha_1, \ldots, \alpha_n$ tak, že*
$$M = (x_1 - \alpha_1, \ldots, x_n - \alpha_n);$$
2. *Pro každý vlastní ideál J okruhu S je množina*
$$\mathbb{V}(J) = \{(\alpha_1, \ldots, \alpha_n) \mid f(\alpha_1, \ldots, \alpha_n) = 0 \text{ pro všechna } f \in J\}$$
neprázdná a platí, že
$$\sqrt{J} = \{g \mid g(\alpha_1, \ldots, \alpha_n) = 0 \text{ pro všechna } g \in \mathbb{V}(J)\}.$$

Důsledek 5.10

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

Důkaz Věty 5.9.

- Buď M maximální ideál okruhu S a $\pi\colon S \to S/M$ kanonická projekce.
- Podle Tvrzení 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

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

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

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

Pokračování důkazu Věty 5.9.

- Zřejmě $\mathbb{V}(J) = \mathbb{V}(\sqrt{J})$. Zbývá ukázat, že pokud $f(\boldsymbol{\alpha}) = 0$ pro každé $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{V}(J)$, 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 $\boldsymbol{\alpha} \in K^n$ a $\beta \in K$ tak, že $f(\boldsymbol{\alpha}) = 0$ a zároveň $1 - f(\boldsymbol{\alpha})\beta = 0$ což je spor.
- Okruh S je noetherovský a tedy ideál J je generován konečně mnoha polynomy, $g_1, \ldots, g_k$.
- Protože $A + B = S[y]$, existují $h_1, \ldots, h_k$ a $h \in S[y]$ tak, že

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

Dokončení důkazu Věty 5.9.

- Uvažme homomorfimus $\phi\colon S[y] \to K(x_1, \ldots, x_n, y)$ 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 $J \subseteq T[x_1, \ldots, x_n]$ 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 $J \subseteq T[x_1, \ldots, x_n]$ se nazývají algebraické.

- Pro $C \subset T^n$ položme naopak

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

Podmnožiny $T[x_1, \ldots, x_n]$ 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 $K[x_1, \ldots, x_n]$.

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)

Buď T algebraicky uzavřené těleso. Potom pro každý vlastní ideál J okruhu $S = T[x_1, \ldots, x_n]$ platí, že

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