Předmluva

Následující text pokrývá přednášku *Komutativní okruhy* a částečně ji přesahuje. V současné podobě má šest částí. Do přednášky původně patřilo:

- Část I celá bez kapitoly 6
- Část II celá
- Část III bez kapitol 5 a 6
- Část VI pouze kapitoly 1 a 2

Tyto partie by neměly obsahovat již příliš mnoho chyb a překlepů. Ostatní partie jsou pravděpodobně v nepříliš dokonalém stavu. Protože se ukázalo, že kapitola 1 části VI není v následných přednáškách nutná, lze ji vynechat.

Text do budoucna dozná změn. Mezi současnou část II a III bude vložena nová samostatná část, která bude obsahovat mimo jiné současnou kapitolu VI.2 (lokalizace). Dále v této nové části bude pojednán v obecnosti tenzorový součin a bude vysvětlena jeho souvislost se současnými speciálními konstrukcemi tenzorového součinu, které jsou uvedeny jednak v části I (volné moduly), jednak v části VI (lokalizace). V samotné přednášce obecně pojatý tenzorový součin přednášet nemíním, neboť ho považuji pro daný účel za zbytečné abstraktní.

Kapitola VI.1 (normalizace) dozná určitých změn, které odstraní několikeré opakovaní podobných obratů v důkazech tím, že tyto obraty vyjádří formou předběžných lemmat.

Ostatní části, které jsou mimo rámec přednášky, budou do budoucna pozměněny a výrazně rozšířeny. Do textu by měla být zařazena většina obecnějších algebraických výsledků, které jsou postupně referovány na Semináři z matematiky inspirované kryptografií (takzvaný SMIK, jehož některé studijní texty lze nalézt na `http://www.karlin.mff.cuni.cz/~krypto/seminar.php`).

Rád bych v dohledné době dokončil samostatný úvodní text z obecné algebry, který je do značné míry hotov a přístupný na síti. Po jeho dokončení bude toto pojednání doplněno odkazy do zmíněného úvodního textu. Stejně tak v budoucnu naroste i počet odkazů mezi jednotlivými kapitolami uvnitř pojednání. Současný stav do jisté míry odráží skutečnost, že při psaní některých kapitol jsem neměl vždy k dispozici text předcházejících částí. Rovněž značení bude v budoucnu více sjednoceno.

V Praze 13. srpna 2006 Aleš Drápal

Obsah

I Základní tvrzení o komutativních okruzích

I.1 Základní pojmy související s dělitelností

V dalším se předpokládá znalost pojmů jako jsou okruh, obor integrity, ideál, hlavní ideál, homomorfismus okruhů a jádro homomorfismu. Rovněž se nebudeme vracet k základním větám o homomorfismu a isomorfismu (posledně jmenované jsou tři).

Soustředíme se zejména na komutativní okruhy; v některých případech se může stát, že budeme pro komutativní okruhy formulovat tvrzení, jež platí pro výrazně větší třídu okruhů. Je to daň za snahu podat o oblasti komutativních okruhů co nejširší přehled.

Nejvýznamnějšími třídami okruhů pro nás budou Gaussovy obory a obory hlavních ideálů. V anglosaské literatuře se běžně objevují pod zkratkou UFD a PID, kde UFD značí Unique Factorization Domain, zatímco pod zkratkou PID se skrývá Principal Ideal Domain. Zkratka UFD je sdělnější než námi používaný pojem Gaussův obor, neboť s ní je asociována ta nejzákladnější vlastnost těchto oborů. V dalším budeme považovat za samozřejmou znalost faktu, že obor integrity, ve kterém je každý řetězec vlastních dělitelů konečné délky, bude Gaussův, pokud každé dva jeho prvky mají největšího společného dělitele. Alternativou této podmínky je přitom podmínka, že každý ireducibilní prvek je prvočinitel.

Ať R je obor integrity. Jeho prvek a dělí $b \in R$ právě když $bR \subseteq aR$. Intuitivně máme sklon na dělitele pohlížet jako na prvek, který je menší než dělenec. Vztahy inkluze hlavních ideálů tuto závislost obracejí (alespoň zdánlivě), a je třeba se s tímto faktem sžít. Při práci s obory integrity, které nejsou obory hlavních ideálů, je totiž nutné uvažovat dělitelnost ideálů, a nikoliv pouze dělitelnost prvků (které jsou reprezentovány hlavními ideály). Přitom ideál J dělí ideál I právě když ho obsahuje.

Ideál I okruhu R se nazývá *maximální*, jestliže pro žádný ideál J neplatí $I \subsetneq J \subsetneq R$ a současně je $I \neq R$. V oboru hlavních ideálů zjevně platí, že $a \in R$ je ireducibilní právě když aR je maximální ideál. Obecně ovšem může pro ireducibilní prvek a komutativního okruhu R existovat ideál I takový, že je $aR \subsetneq I \subsetneq R$. Pak ovšem I není hlavní ideál.

Přidržíme se konvence v komutativní algebře obvyklé, totiž že za *vlastní* se považuje každý ideál R různý od R (tedy neobsahující prvek 1). Nyní budeme směřovat k vyložení popisu prvočinitele v řeči ideálů. Připomeneme nejprve, že pro ideály I a J okruhu R se jejich součin značí IJ. Rozumí se jím množina všech součtů tvaru $\sum a_i b_i$, $1 \leq i \leq n$, kde $a_i \in I$ a $b_i \in J$. Je zřejmé, že IJ je rovněž ideál R a že platí $IJ \subseteq I \cap J$.

Ideál P okruhu R se nazývá *prvoideál*, jestliže je $P \neq R$ a současně pro libovolné dva ideály I a J okruhu R platí implikace

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

Připomeňme, že v komutativním okruhu R se nazývá prvek $p \in R$ *prvočinitelem*, jestliže není invertibilní a současně pro libovolné dva prvky $a, b \in R$ splňuje implikaci

$$p \text{ dělí } ab \Rightarrow p \text{ dělí } a \text{ nebo } p \text{ dělí } b.$$

I.1.1 Lemma. *Ideál $P \neq R$ komutativního okruhu R je prvoideál právě když pro každé dva prvky $a, b \in R$ splňuje implikaci*

$$ab \in P \Rightarrow a \in P \text{ nebo } b \in P.$$

Důkaz. Z $ab \in P$ plyne $(ab)R \subseteq P$ a současně je $(aR)(bR) = (ab)R$. Je-li P prvoideál, tak musí být $aR \subseteq P$ nebo $bR \subseteq P$, a tedy $a \in P$ nebo $b \in P$.

Předpokládejme nyní, že P splňuje podmínku lemmatu, a že pro ideály I a J okruhu R platí $IJ \subseteq P$. Ať například existuje $b \in J \setminus P$. Pak pro každé $a \in I$ máme $ab \in P$, a tedy $a \in P$, takže je $I \subseteq P$. □

Z lemmatu I.1.1 okamžitě vidíme, že prvek p komutativního okruhu R je prvočinitel právě když pR je prvoideál. Níže ověříme, že maximální ideály jsou v komutativních okruzích vždy prvoideály, což nabízí (alternativní) důkaz, že v oborech hlavních ideálů jsou ireducibilní prvky vždy prvočiniteli. (Prvek $a \in R$ je *ireducibilní* právě když nemá vlastního dělitele a není invertibilní. To nastane právě když $aR \neq R$ a z $aR \subseteq bR$ plyne $bR = R$ nebo $bR = aR$, pro každé $b \in R$. V oborech hlavních ideálů je tedy $a \in R$ ireducibilní právě když aR je maximální ideál.)

Nejprve ale připomeneme, že pro ideály I a J okruhu R je množina $I + J = \{a + b;\ a \in I \text{ a } b \in J\}$ rovněž ideálem R. Je to zjevně nejmenší ideál, který obsahuje $I \cup J$. V komutativním okruhu R je proto ideál $M \neq R$ maximální právě když pro každé $a \in R \setminus M$ platí $R = M + aR$, tedy když pro každé $a \in R \setminus M$ existuje $m \in M$ a $r \in R$ takové, že $1 = m + ar$.

I.1.2 Lemma. *V komutativním okruhu je každý maximální ideál prvoideálem.*

Důkaz. Ať je M maximální ideál okruhu R a ať platí $ab \in M$. Předpokládejme $a \notin M$. Potom $1 = m + ar$ pro nějaká $m \in M$, $r \in R$, takže $b = b \cdot 1 = bm + rab \in M$. □

Předchozí fakt lze ovšem nahlédnout elegantněji. Stačí totiž použít následující tvrzení (jeho důkaz bezprostředně vyplývá z charakterizace ideálů faktorokruhu jakožto kvocientů ideálů původního okruhu; pro jistotu je však důkaz uveden).

I.1.3 Tvrzení. *Buď I vlastní ideál komutativního okruhu R. Potom*

(i) ideál I je maximální právě když R/I je těleso,

(ii) ideál I je prvoideál právě když R/I je obor integrity.

Důkaz. Prvek $a \in R$ je invertibilní právě když $aR = R$. Jinými slovy, prvek je invertibilní právě když neleží v žádném vlastním ideálu. Všechny nenulové prvky R/I jsou tedy invertibilní právě když R/I nemá vlastní nenulový ideál. Všechny ideály R/I mají tvar J/I, $R \supseteq J \supseteq I$. Odsud (i).

Pro $a, b \in R$ je $(a+I)(b+I) = ab + I$ rovno $0_{R/I} = I$ právě když $ab \in I$. Okruh R/I je proto oborem integrity právě když z $ab \in I$ vyplývá $a + I = I$ nebo $b + I = I$, čili právě když z $ab \in I$ vyplývá $a \in I$ nebo $b \in I$. Takový požadavek podle lemmatu I.1.1 říká, že I je prvoideál. $\square$

Část (ii) lze samozřejmě dokázat pouze v řeči ideálů. Je užitečné si takový důkaz sestavit.

Podobných obratů, kdy se důkaz zdánlivě založený na výpočtu stane vhodnou strukturní úvahou zřejmý, je v komutativní algebře mnoho.

Je dobré si také uvědomit, jak součet ideálů, $I + J$, odpovídá pojmu největšího společného dělitele. Vskutku, pokud $I = aR$ a $J = bR$, R komutativní, tak z $I + J = cR$ plyne, že c dělí a i b. Současně pro každý společný dělitel d prvků a a b máme $dR \supseteq (aR) \cup (bR)$, a tedy $dR \supseteq aR + bR = I + J$. Z $I + J = cR$ tedy plyne, že c je největším společným dělitelem a a b. Vidíme, že v oborech integrity hlavních ideálů je korespondence mezi součty ideálů a největšími společnými děliteli jednoznačná. V Gaussových oborech ovšem $I + J$ nemusí být vždy hlavní ideál; existence největšího společného dělitele obecně totiž znamená existenci nejmenšího hlavního ideálu, který ideál $I + J$ obsahuje.

Obraťme se nyní k další základní vlastnosti okruhů známé z definice Gaussových oborů. Konečností řetězce vlastních dělitelů se rozumí neexistence posloupnosti $a_0, a_1, a_2, \dots$ takové, že a_{i+1} dělí a_i pro každé $i \geq 0$, přičemž a_i není nikdy s a_{i+1} asociováno (tedy a_i nikdy nedělí a_{i+1}). Jinými slovy, požaduje se, aby neexistoval nekonečný řetězec $I_0 \subsetneq I_1 \subsetneq \dots$ hlavních ideálů.

Komutativní okruh R se nazývá *noetherovský*, jestliže neobsahuje nekonečný řetězec $I_0 \subsetneq I_1 \subsetneq \dots$ svých ideálů. Říkává se také, že R je noetherovský, jestliže splňuje *podmínku rostoucího řetězce* (ascending chain condition, ACC) pro ideály. Tato podmínka se obvykle definuje tak, že v každé rostoucí posloupnosti ideálů $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ existuje $k \geq 0$ takové, že $I_j = I_k$ pro každé $j \geq k$.

Pro nekomutativní okruhy je definice obdobná, avšak místo ideálů se uvažují levé nebo pravé ideály (a pak se hovoří o okruzích zleva či zprava noetherovských).

Je-li $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$ rostoucí posloupnost ideálů, je $I = \bigcup(I_j;\, j \geq 0)$ rovněž ideál. Tento fakt budeme v dalším používat jako samozřejmý. V oborech hlavních ideálů si řetězce vlastních dělitelů a rostoucí posloupnosti ideálů odpovídají jednoznačně. Připomeneme to opakováním známého faktu:

I.1.4 Lemma. *Obory hlavních ideálů jsou noetherovské.*

Důkaz. Postupujme sporem. Ať $I_0 \subsetneq I_1 \subsetneq \dots$ je rostoucí řetězec ideálů. Ať $a_0, a_1, \dots \in R$ jsou taková, že $I_j = a_j R$, $j \geq 0$. Ideál $I = \bigcup(I_j;\, j \geq 0)$ je roven nějakému aR. Buď $k \geq 0$ nejmenší takové, že $a \in I_k$. Pak $I = aR \subseteq I_{k'} \subseteq I$ pro každé $k' \geq k$, odkud $I_{k'} = I_k$, ve sporu s naším předpokladem. $\square$

Některé základní vlastnosti noetherovských okruhů je účelnější sledovat na noetherovských modulech.

Modul M nad okruhem R (stručně R–modul) bude zde, jak je obvyklé, Abelova grupa se zadaným skalárním násobením λu pro každé $\lambda \in R$ a $u \in M$, jež splňuje

$$\lambda(u+v) = \lambda u + \lambda v,\ \lambda(\nu u) = (\lambda\nu)u,\ (\lambda+\nu)u = \lambda u + \nu u,\ 1u = u$$

pro všechna $u, v \in M$ a všechna $\lambda, \nu \in R$.

Všimněte si, že zobrazení $u \mapsto \lambda u$ je pro každé pevně vybrané λ endomorfismem Abelovy grupy $M(+,-,0)$. Definice modulu je stanovena tak, aby přiřazením takového zobrazení každému prvku $\lambda \in R$ vznikl homomorfismus z okruhu R do okruhu endomorfismů Abelovy grupy M.

Přesně vzato bychom předchozí definici měli považovat za definici levého modulu. Definice pravého modulu je symetrická, rozdíl je v tom, že se skalární násobení píše zprava. Pokud je R komutativní, tak ovšem není mezi levými a pravými moduly třeba rozlišovat.

Pojmy jako podmodul a faktormodul jistě není třeba vysvětlovat. Podobně lze považovat za známou platnost vět o homomorfismu a isomorfismu pro moduly.

Okruh R lze považovat za modul nad sebou samým. Podmoduly takového modulu zjevně odpovídají pro R komutativní ideálům R.

Modul M nad R se nazývá *noetherovský*, jestliže splňuje podmínku rostoucích řetězců pro podmoduly (tj. neexistuje nekonečná posloupnost $M_0 \subsetneq M_1 \subsetneq \dots$ podmodulů M).

Je-li $X \subseteq M$, kde M je R–modul, tak všechny prvky tvaru $\sum r_i x_i$, kde $x_i \in X$, $r_i \in R$ a $1 \le i \le k$, tvoří podmodul M. Je to nejmenší podmodul M, který obsahuje X a nazýváme ho podmodulem *generovaným* X. Je-li tento podmodul roven M, říkáme, že X generuje modul M. O tomto modulu řekneme, že je *konečně generovaný* právě když lze nalézt konečnou množinu, jež ho generuje.

Za zmínku stojí, že podmodul N modulu M, který je generovaný podmoduly $M_i \subseteq M$, $i \in I$, je roven

$$\sum(M_i;\ i \in I) = \{\sum_{j \in J} m_j;\ J \subseteq I \text{ je konečná a } m_j \in M_j \text{ pro každé } j \in J\}.$$

I.1.5 Tvrzení. *Modul M je noetherovský právě když je každý jeho podmodul konečně generovaný.*

Důkaz. Uvažme nějakou posloupnost $A_0 \subseteq A_1 \subseteq \dots$ podmodulů M. Potom je $A = \bigcup(A_i;\ i \ge 0)$ rovněž podmodul M. Je-li A konečně generovaný, s generátory $a_1, \dots, a_n$, musí existovat $k \ge 0$ takové, že A_k obsahuje všechny tyto generátory. Pak ovšem $A_i = A$ pro každé $i \ge k$. Jestliže A není konečně generovaný, lze položit $B_0 = 0$ a volit $B_i \subsetneq A$ a $b_i \in A$ tak, že $b_i \notin B_i$ a $B_{i+1} = B_i + Rb_i$. Pak je $B_0 \subsetneq B_1 \subsetneq \dots$, takže M není noethoerovský. $\square$

Je zřejmé, že podmoduly a faktormoduly noetherovských modulů jsou opět noetherovské. Lze snadno dokázat i opak, totiž že z noetherovskosti faktormodulu a příslušného podmodulu plyne noetherovskost celého modulu:

I.1.6 Lemma. *Ať M je modul s podmodulem N. Pokud N a M/N jsou noetherovské, je noetherovský i modul M.*

Důkaz. Ať M_0 je podmodul M. Položme $N_0 = M_0 \cap N$. Podle předpokladu existují $a_1, \dots, a_n$, která generují N_0. Modul $(M_0 + N)/N$ je rovněž noetherovský; nechť je generován prvky $b_1 + N, \dots, b_m + N$, kde $b_1, \dots, b_m \in M_0$. Potom pro každé $c \in M_0$ existují $r_1, \dots, r_m \in R$ taková, že $c \equiv \sum r_i b_i \bmod N$. Pak $c - \sum r_i b_i$ leží v $M_0 \cap N = N_0$. Vidíme, že $\{a_1, \dots, a_n\} \cup \{b_1, \dots, b_m\}$ generuje M_0. $\square$

Komutativní okruh R je noetherovský právě když je noetherovský jako R–modul. Faktorokruhy noetherovských komutativních okruhů jsou zřejmě také noetherovské.

I.2 Polynomy nad noetherovskými okruhy a Gaussovými obory

V této kapitole budeme pod okruhem rozumět komutativní okruh. Někdy budeme používat bez bližšího upozornění zápis obvyklý v komutativní algebře, kdy $(a_1, \dots, a_k)$ označuje ideál generovaný prvky $a_1, \dots, a_k$. V okruhu hlavních ideálů se prvky identifikují se svými hlavními ideály, takže v takovém případě $(a_1, \dots, a_k)$ může znamenat i největší společný dělitel prvků $a_1, \dots, a_k$.

Okruh polynomů $R[x_1, \dots, x_k]$ v proměnných $x_1, \dots, x_k$ je definován známým způsobem na množině formálních součtů $a = \sum a_{\varepsilon_1, \dots, \varepsilon_k} x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k}$, kde $\varepsilon_1 \geq 0, \dots, \varepsilon_k \geq 0$, přičemž $a_{\varepsilon_1, \dots, \varepsilon_k} \neq 0$ jen v konečně mnoha případech. Definicí formálního součtu se zde zabývat nebudeme; z hlediska formálního popisu je nejsnazší říci, že polynom a ztotožňujeme se zobrazením $a \colon \mathbb{N}_0^k \to R$, kde $a(\varepsilon_1, \dots, \varepsilon_k) = a_{\varepsilon_1, \dots, \varepsilon_k}$.

Za samozřejmé rovněž budeme považovat ztotožnění $R[x_1, \dots, x_k, x_{k+1}] \cong (R[x_1, \dots, x_k])[x_{k+1}]$. Upozorněme dále, že leckdy se místo $x_1, \dots, x_k$ proměnné označují velkými písmeny, například $X_1, \dots, X_k$.

Některé vlastnosti okruhu R jsou zachovány i při přechodu k okruhu polynomů $R[x]$. Cílem této kapitoly je ukázat, že takovými vlastnostmi je vlastnost být noetherovským okruhem a být Gaussovým oborem.

I.2.1 Věta (Hilbertova o bázi). *Okruh R je noetherovský právě když je noetherovský okruh $R[x]$.*

Důkaz. Předpokládejme, že okruh R je noetherovský a okruh $R[x]$ noetherovský není. Potom existuje ideál I okruhu $R[x]$, který není konečně generovaný. Můžeme proto vytvořit posloupnost polynomů $a_0, a_1, \dots$, které leží v I, takovou, že $a_0 \in I \cap R$ a že a_{i+1} je některý z polynomů nejmenšího stupně obsažených v $I \setminus (a_0, \dots, a_i)$. Stupně těchto polynomů zřejmě tvoří neklesající posloupnost. Označme J_i ideál okruhu R generovaný vedoucími koeficienty polynomů $a_0, \dots, a_i$. Pak $J_0 \subseteq J_1 \subseteq \dots$, takže pro nějaké $k \geq 0$ máme $J_{k+1} = J_k$. Označme h stupeň polynomu a_{k+1}. Vynásobením polynomů a_i, $0 \leq i \leq k$, vhodným jednočlenem x^s, $s \geq 0$, dostaneme polynomy $\overline{a_i} \in I$ stupně h, jejichž vedoucí koeficienty generují J_k. Proto existují $r_0, \ldots, r_k \in R$ taková, že polynom $a = \sum r_i \overline{a_i} \in I$ má stejný vedoucí koeficient jako polynom a_{k+1}. Pak ovšem $a_{k+1} - a$ padne do $I \setminus (a_0, \ldots, a_k)$, přičemž má menší stupeň než a_{k+1}. Tím jsme obdrželi hledaný spor. □

I.2.2 Důsledek. *Je-li R noetherovský okruh, je jím i $R[x_1, \ldots, x_k]$.*

Obraťme nyní svou pozornost ke Gaussovým oborům. Každý prvek a Gaussova oboru R lze zapsat jako $up_1^{\varepsilon_1} \cdots p_k^{\varepsilon_k}$, kde u je prvek invertibilní a $p_1, \ldots, p_k$ jsou prvočinitele. Přitom se předpokládá, že prvočinitelé p_i a p_j, $1 \leq i < j \leq k$, nejsou asociováni, tedy že generují různé hlavní ideály. Zápis je jednoznačný až na volbu pořadí a záměnu asociovanými prvočiniteli. Můžeme též psát

$$(a) = (p_1)^{\varepsilon_1} \cdots (p_k)^{\varepsilon_k}.$$

Tento zápis již jednoznačný je (až na pořadí), neboť v něm figurují (po dvou různé) hlavní ideály, nikoliv jejich (ne nutně jednoznačně určené) generátory.

Je-li p prvočinitel, tak pro $(p) = (p_i)$, $1 \leq i \leq k$, položme $v_p(a) = \varepsilon_i$. Pokud se (p) mezi ideály (p_i) nevyskytuje, položíme $v_p(a) = 0$. Hodnotě $v_p(a)$ se říká *p–valuace* prvku a. Lze ji zjevně použít i pro prvky podílového tělesa T Gaussova oboru R, kde klademe $v_p(a/b) = v_p(a) - v_p(b)$. Korektnost takové definice je zřejmá. Nenulový prvek $a \in T$ zjevně padne do R právě když $v_p(a) \geq 0$ pro každý prvočinitel p. Pokud potřebujeme vyjádřit $v_p(0)$, definujeme ho jako ∞.

Buď R i nadále Gaussův obor s podílovým tělesem T. Polynom $a \in R[x]$ se nazývá *primitivní*, jestliže jeho koeficienty jsou nesoudělné (a tedy generují R) a jestliže je nenulový.

Pro nenulový polynom $a = \sum a_i x^i \in T[x]$ a pro prvočinitele p položme $c_p(a) = \min\{v_p(a_i);\ 0 \leq i \leq \deg a\}$. Vidíme, že $a \in R[x]$ je primitivní právě když $c_p(a) = 0$ pro každý prvočinitel p. Zřejmě platí

I.2.3 Lemma. *Je-li $u \in T^*$, $p \in R$ prvočinitel a $a \in T[x]$, $a \neq 0$, je $c_p(ua) = v_p(u) + c_p(a)$.*

Vidíme, že nenulový polynom a z $T[x]$ leží v $R[x]$ právě když $c_p(a) \geq 0$ pro každý prvočinitel p.

Připomeňme, že pro každý homomorfismus okruhů $f\colon R \to S$ existuje jediný homomorfismus $f_x : R[x] \to S[x]$, který rozšiřuje f a zobrazuje x na x. Zde budeme uvažovat homomorfismus π_x daný přirozenou projekcí $\pi\colon R \to R/(p)$, p prvočinitel.

I.2.4 Lemma (Gaussovo). *Ať $a, b \in R[x]$ jsou primitivní. Pak je primitivní i polynom ab.*

Důkaz. Budeme dokazovat, že pro každý prvočinitel p z platnosti $c_p(a) = 0 = c_p(b)$ plyne $c_p(ab) = 0$. Okruh $R/(p)$ je obor integrity, a proto je oborem integrity i okruh $R/(p)[x]$. Máme $\pi_x(ab) = \pi_x(a)\pi_x(b)$, přičemž podmínka $c_p(a) = 0$ je shodná s podmínkou $\pi_x(a) \neq 0$. Z $\pi_x(a) \neq 0$ a $\pi_x(b) \neq 0$ plyne $\pi_x(ab) \neq 0$, a tedy i $c_p(ab) = 0$. □

Důkaz Gaussova lemmatu lze samozřejmě provést i bez faktorizace úvahou vycházející ze vzorce pro koeficienty násobku polynomů.

I.2.5 Důsledek. *Pro všechny nenulové polynomy $a, b \in T[x]$ a všechny prvočinitele $p \in R$ platí $c_p(ab) = c_p(a) + c_p(b)$*

Důkaz. Položme $u = \prod p^{-c_p(a)}$ a $v = \prod p^{-c_p(b)}$ (kde součin probíhá přes prvočinitele p, z nichž žádné dva nejsou asociovány). Pak $a_1 = ua$ i $b_1 = vb$ jsou primitivní polynomy z $R[x]$, dle lemmatu I.2.3. Z $c_p(a_1b_1) = 0 = c_p(a_1) + c_p(b_1)$ plyne $c_p(ab)+v_p(uv) = c_p(a)+v_p(u)+c_p(b)+v_p(v)$, odkud $c_p(ab)-c_p(a)-c_p(b) = v_p(uv) - v_p(u) - v_p(v) = 0$. □

I.2.6 Tvrzení. *Buď R Gaussův obor a ať je T jeho podílové těleso. Ireducibilní prvky okruhu $R[x]$ jsou jednak všechny prvočinitele oboru R, jednak všechny primitivní polynomy $a \in R[x]$, které jsou jakožto polynomy z $T[x]$ ireducibilní. Ke každému ireducibilnímu polynomu $b \in T[x]$ existuje $u \in T$ takové, že ub je ireducibilní prvek okruhu $R[x]$.*

Důkaz. Každý dělitel prvku z R (z hlediska dělitelnosti v $R[x]$) nutně leží v R, takže $a \in R$ je ireducibilní prvek okruhu $R[x]$ právě když je ireducibilním prvkem okruhu R. Ireducibilními prvky Gaussova oboru R jsou jeho prvočinitelé. Situace prvků z R je tedy zřejmá.

Ať $a \in R[x]$ je polynom stupně alespoň jedna. Pak $a = ua_1$, kde a_1 je primitivní a $u = \prod p^{c_p(a)}$, pro vhodné prvočinitele $p \in R$. Není-li a primitivní, je u jeho vlastním dělitelem. Můžeme tedy předpokládat, že a primitivní je.

Pokud $a = bc$ pro nějaká $b, c \in R[x]$, tak pro každý prvočinitel p podle důsledku I.2.5 máme $0 = c_p(a) = c_p(b) + c_p(c)$, odkud $c_p(b) = c_p(c) = 0$ pro všechny prvočinitele p. Je-li a ireducibilní prvek okruhu $T[x]$ (tedy to, co se běžně nazývá ireducibilní polynom), musí být b nebo c prvek okruhu $R = T \cap R[x]$, a z $c_p(b) = c_p(c) = 0$ plyne, že tento prvek je invertibilní (v R a tím i v $R[x]$), takže a je ireducibilní prvek $R[x]$.

Předpokládejme, že a není v $T[x]$ ireducibilní polynom. Pak $a = bc$, kde $0 < \deg(b) < \deg(a)$ a $b, c \in T[x]$. Položme $u = \prod p^{-c_p(b)}$ a $v = \prod p^{-c_p(c)}$, podobně jako v důkazu důsledku I.2.5. Dostaneme opět, že $b_1 = ub$ i $c_1 = vc$ jsou primitivní polynomy. Protože $0 = c_p(a) = c_p(b) + c_p(c) = c_p(b_1) = c_p(c_1)$ pro každý prvočinitel p, je vždy $v_p(u)+v_p(v) = 0$, a tedy $uv = 1$, takže $a = b_1c_1$ je v $R[x]$ součinem dvou polynomů menších stupňů, a tudíž není jako prvek $R[x]$ ireducibilní. □

I.2.7 Tvrzení. *Je-li R Gaussův obor, je i $R[x]$ Gaussův obor.*

Důkaz. Ať polynom a dělí v $R[x]$ polynom b. Pak vedoucí koeficient a dělí vedoucí koeficient b. Přitom $\deg(a) \leq \deg(b)$. Je-li $\deg(a) = \deg(b)$, je a vlastním dělitelem b právě když vedoucí koeficient a je vlastním dělitelem vedoucího koeficientu b. V nekonečné posloupnosti dělitelů prvků $R[x]$ se musí stupně polynomů od jistého místa shodovat. Ve zbylé části posloupnosti musí být od jistého místa asociovány všechny vedoucí koeficienty polynomů, a tím i celé polynomy. Proto jsou v $R[x]$ řetězce vlastních ideálů konečné. Zbývá ukázat, že každý ireducibilní prvek $a \in R[x]$ je v $R[x]$ prvočinitelem.

Ať a dělí bc, kde b a c jsou polynomy z $R[x]$. Je-li $a \in R$, můžeme například použít důsledek I.2.5, podle kterého $c_a(bc) = c_a(b) + c_a(c) \geq c_a(a) = 1$, takže $c_a(b) \geq 1$ nebo $c_a(c) \geq 1$, odkud plyne, že a dělí b nebo c.

Pro $\deg(a) \geq 1$ z ireducibility a v $T[x]$ plyne, že a dělí b nebo c v $T[x]$. Předpokládejme prvou možnost. Pak $b = aq$, kde $q \in T[x]$. Ovšem důsledek I.2.5 dává $c_p(b) = c_p(q)$ pro každé p, neboť a je podle tvrzení I.2.6 polynom primitivní. Z $b \in R[x]$ plyne $c_p(q) \geq 0$ pro každé p, takže q leží v $R[x]$. To znamená, že a dělí b nejen v $T[x]$, ale i v $R[x]$. □

V předchozích úvahách jsme místo obratů vyjadřujících nulovost $c_p(a)$ pro každý prvočinitel $p \in R$ mohli pracovat s invertibilitou prvku $c(a) = \prod p^{c_p(a)}$. Pro $a \in R[x]$ je ovšem $c(a)$ určeno jednoznačně až na násobek invertibilním prvkem. Jednoznačně určený je tedy pouze ideál $(c(a))$. Důsledek I.2.5 říká, že $(c(ab)) = (c(a))(c(b))$. Místo $c(a)$ se někdy píše $cont(a)$, kde *cont* je zkratkou za content, česky „obsah“.

I.3 Komaximální ideály, prvoideály, radikál

V této kapitole bude každý uvažovaný okruh komutativní.

Je dobré si uvědomit, že na množinu všech ideálů okruhu R lze pohlížet jako na komutativní monoid s operací násobení ideálů IJ. Jednotkovým prvkem tohoto monoidu je R; monoid přitom žádné další invertibilní prvky nemá. Na množině všech ideálů je také definována aditivní struktura s operací $I + J$, přičemž platí, jak lze snadno ověřit, distributivní zákon

$$I(J + K) = IJ + IK.$$

Obecně máme $I \cap J \supseteq IJ$, v některých důležitých situacích, jak nyní nahlédneme, však platí rovnost.

O ideálech I a J řekneme, že jsou *komaximální*, jestliže $I + J = R$.

I.3.1 Lemma. *Pro komaximální ideály platí $IJ = I \cap J$.*

Důkaz. Máme $I \cap J = (I \cap J)(I + J) = (I \cap J)I + (I \cap J)J \subseteq JI + IJ = IJ$. □

Ideály $I_1, \dots, I_n$ se nazývají *po dvou komaximální*, pokud I_j a I_k jsou komaximální kdykoliv $1 \leq j < k \leq n$.

I.3.2 Tvrzení. *Ať $I_1, \dots, I_n$ jsou po dvou komaximální ideály okruhu R, $n \geq 2$. Potom $I_1 \cap \dots \cap I_n = I_1 \cdots I_n$ a komaximální je i dvojice ideálů $I_1 \cap \dots \cap I_{n-1}$ a I_n.*

Důkaz. Vyjádříme-li R jako $(I_1+I_n)(I_2+I_n)\cdots(I_{n-1}+I_n)$, dostaneme okamžitě rovnost $I_1 \cdots I_{n-1} + I_n = R$. (Zapíšeme-li totiž $1 = 1_R$ jako $a_j + b_j$, kde $a_j \in I_j$ a $b_j \in I_n$, $1 \leq j < n$, dostaneme vynásobením těchto součtů vyjádření 1_R jako $a_1 \dots a_n + c$, kde $c \in I_n$.) Zbytek plyne indukcí založenou na lemmatu I.3.1. □

I.3.3 Lemma. *Ať $I_1, \dots, I_n$ jsou ideály okruhu R. Uvažme homomorfismus $f : R \to (R/I_1) \times \cdots \times (R/I_n)$, který zobrazuje každé r na $(r + I_1, \dots, r + I_n)$. Pak* $\mathrm{Ker}(f) = I_1 \cap \cdots \cap I_n$. *Homomorfismus f je surjektivní právě když ideály $I_1, \dots, I_n$ jsou po dvou komaximální.*

Důkaz. Tvrzení o jádru je zřejmé. Pro $1 \le i < j \le n$ uvažme přirozenou projekci $\pi: (R/I_1) \times \cdots \times (R/I_n) \to \big((R/I_i) \,/\, ((I_i + I_j)/I_i)\big) \times \big((R/I_j) \,/\, ((I_i + I_j)/I_j)\big) \cong R/(I_i + I_j) \times R/(I_i + I_j)$. Protože πf zobrazuje prvky R na diagonálu uvedeného součinu, plyne ze surjektivity f nutně komaximalita I_i a I_j. Předpokládejme, že pro všechna $1 \le i < j \le n$ jsou I_i a I_j komaximální a dokažme tvrzení nejprve pro $n = 2$.

Chceme ukázat, že pro $r_i \in R$, $i \in \{1, 2\}$, existuje $r \in R$ takové, že $r \equiv r_i \mod I_i$. Víme, že $1 = a_1 + a_2$ pro $a_i \in I_i$. Položme $r = r_1 a_2 + r_2 a_1$. Pak $r - r_1 = r - r_1(a_1 + a_2) = a_1(r_2 - r_1) \in I_1$, a podobně $r - r_2 \in I_2$.

Zbytek důkazu lze provést indukcí. Podle indukčního předpokladu pro $I = I_1 \cdots I_{n-1}$ je $g: R/I \to (R/I_1) \times \cdots \times (R/I_{n-1})$, $(r + I) \mapsto (r + I_1, \dots, r + I_{n-1})$, surjektivní homomorfismus. Podle předchozí části důkazu a tvrzení I.3.2 je $h: R \to R/I \times R/I_n$, $h(r) = (r + I, r + I_n)$ surjektivní homomorfismus. Protože $f = (g \times \mathrm{id}_{R/I_n}) \circ h$, je surjektivní i f. □

Z lemmatu I.3.3 jako důsledek vyplývá, že zobrazení f je isomorfismus právě když $I_1, \dots, I_n$ jsou komaximální ideály s nulovým průnikem. Opačný směr této ekvivalence je znám jako čínská věta o zbytcích. Vyslovíme ji ve tvaru, který poukazuje na nejčastější způsob aplikace.

I.3.4 Důsledek (Čínská věta o zbytcích). *Buď R okruh s ideály $I_1, \dots, I_n$. Jestliže tyto ideály jsou po dvou komaximální a mají nulový průnik, tak pro všechna $r_1, \dots, r_n \in R$ existuje právě jedno $r \in R$ takové, že $r_i \equiv r \mod I_i$, $1 \le i \le n$.* □

Z výpočetního hlediska nejsou tvrzení, jež využívají axiom výběru (a tedy potažmo Zornovo lemma) příliš cenná. Přesto taková tvrzení mají svůj význam i ve výpočetním kontextu, neboť mohou sloužit jako teoretické existenční vodítko, které motivuje k hledání algoritmů. Uvedeme několik takových základních existenčních tvrzení.

I.3.5 Lemma. *Nechť A je podmnožina okruhu R a ať I je jeho ideál. Je-li $I \cap A = \emptyset$, existuje alespoň jeden ideál $J \supseteq I$ takový, že $J \cap A = \emptyset$ a $J' \cap A \neq \emptyset$ pro každý ideál $J' \supsetneq J$.*

Důkaz. Uvažme množinu všech ideálů $J \supseteq I$, které splňují $J \cap A = \emptyset$. Je-li $(J_\alpha;\ \alpha \in \Delta)$ řetězec do sebe vřazených ideálů takové vlastnosti, má stejnou vlastnost i ideál $\bigcup(J_\alpha;\ \alpha \in \Delta)$, takže tvrzení plyne z Zornova lemmatu. (V důkazu se předpokládá, že Δ je lineárně uspořádaná množina, přičemž $J_\alpha \subseteq J_\beta$ pro $\alpha \le \beta$.) □

Vlastní ideály jsou ty, které neobsahují prvek 1. Pokud položíme $A = \{1\}$, dostaneme známý

I.3.6 Důsledek. *Buď I vlastní ideál okruhu R. Pak v R existuje maximální ideál, který I obsahuje.*

Multiplikativní množinou okruhu R se míní každá podmnožina R, která je uzavřená na násobení a neobsahuje prvek 0.

I.3.7 Tvrzení. *Buď S multiplikativní množina okruhu R a ať I je ideál tohoto okruhu, $I \cap S = \emptyset$. Pak existuje prvoideál $P \supseteq I$, který splňuje $P \cap S = \emptyset$.*

Důkaz. Použijeme lemma I.3.5 pro $A = S$ a ukážeme, že ideál J daný tímto lemmatem je prvoideál. Ať $a, a' \in R \setminus J$. Potřebujeme ukázat, že pak do J nepadne ani součin aa'. Z maximality J vyplývá neprázdnost průniků $S \cap (J + Ra)$ a $S \cap (J + Ra')$. Ať tedy $p, p' \in J$, dále $s, s' \in S$ a konečně $r, r' \in R$ jsou taková, že $s = p + ra$ a $s' = p' + r'a'$. Pak $ss' = (pp' + pr'a' + p'ra) + rr'aa'$ leží v S, a tedy ne v J. Výraz v závorce padne do J, takže musí být $rr'aa' \notin J$, a tedy i $aa' \notin J$. □

Za I můžeme zvolit nulový ideál, takže tvrzení poskytuje okamžitě

I.3.8 Důsledek. *Pro každou multiplikativní množinu S okruhu R existuje prvoideál P takový, že je $P \cap S = \emptyset$.*

Množině všech prvoideálů okruhu se někdy říká jeho *spektrum*. Množině prvoideálů, které obsahují daný ideál I se říká *varieta* I (budeme psát $\operatorname{Var} I$). *Minimálním prvkem* $\operatorname{Var} I$ se rozumí každý prvoideál $P \in \operatorname{Var} I$, který má tu vlastnost, že pro žádné $Q \in \operatorname{Var} I$ není $Q \subsetneq P$.

Následující tvrzení je příkladem použití Zornova lemmatu na klesající řetězec ideálů.

I.3.9 Tvrzení. *Buď I vlastní ideál okruhu R a ať je $P \in \operatorname{Var} I$. Pak varieta I obsahuje alespoň jeden minimální prvek Q takový, že je $Q \subseteq P$.*

Důkaz. Tvrzení bude plynout z Zornova lemmatu, pokud ukážeme že průnik řetězce do sebe vřazených prvoideálů $(P_\alpha;\ \alpha \in \Delta)$ z $\operatorname{Var} I$ je opět prvoideál. Že jde o ideál, který obsahuje I, je zřejmé. Označme průnik J a ať $ab \in J$. Pokud $a \notin J$, existuje $\beta \in \Delta$, že $a \notin P_\alpha$ pro každé $\alpha \leq \beta$. Pro taková α z $ab \in P_\alpha$ plyne $b \in P_\alpha$, odkud $b \in P_\alpha$ pro všechna $\alpha \in \Delta$, čili $b \in J$. □

Nyní se budeme věnovat základním konstrukcím, které využívají prvoideály. Přímočarou indukcí plyne dobře známé

I.3.10 Lemma. *Ať je P prvoideál okruhu R a ať $a_1, \dots, a_n$ jsou prvky R. Je-li $a_1 \cdots a_n \in P$, existuje j, $1 \leq j \leq n$, takové, že $a_j \in P$.*

Příslušnost prvoideálu do vyjádření nějakého ideálu jako součinu jiných ideálů (jež často bývají mocninami prvoideálů) lze mnohdy odvodit z následujícího jednoduchého lemmatu základního významu.

I.3.11 Lemma. *Buďte $I_1, \dots, I_n$ ideály okruhu R. Potom pro prvoideál P platí $P \supseteq I_1 \cap \dots \cap I_n$ právě když $P \supseteq I_1 \cdots I_n$. Tato situace nastane tehdy a jen tehdy pokud $P \supseteq I_j$ pro nějaké j, $1 \leq j \leq n$.*

Důkaz. Z $P \supseteq I_1 \cap \cdots \cap I_n$ máme $P \supseteq I_1 \cdots I_n$, neboť $I_1 \cap \cdots \cap I_n \supseteq I_1 \cdots I_n$. Podobně jednodušše z $P \supseteq I_j$ vyplývá $P \supseteq I_1 \cap \cdots \cap I_n$. Předpokládejme $P \supseteq I_1 \cdots I_n$. Pokud by bylo možno zvolit $a_j \in I_j \setminus P$ pro každé j, $1 \leq j \leq n$, dostali bychom spor s lemmatem I.3.10, neboť by bylo $a_1 \cdots a_n \in P$, přičemž žádný z prvků a_j by v P neležel. Proto musí být $I_j \subseteq P$ pro alespoň jedno j, $1 \leq j \leq n$. □

Pro ideál I okruhu R položme

$$\sqrt{I} = \{a \in R;\ \text{existuje } k \geq 1 \text{ takové, že } a^k \in I\}.$$

Pak je $\sqrt{I} \supseteq I$ a z binomické věty plyne, že pro $a, b \in \sqrt{I}$ máme $a + b \in \sqrt{I}$. Protože I je ideál, je ideál i $\sqrt{I}$. Tomuto ideálu se říká *radikál* I a značí se též $\mathrm{rad}_R(I)$.

Ideál $\sqrt{0}$ se nazývá *nilradikál* R. Je zjevné, že $\sqrt{I}$ je rovno vzoru nilradikálu okruhu R/I při projekci modulo I.

I.3.12 Tvrzení. *Buď I vlastní ideál okruhu R. Potom*

$$\sqrt{I} = \bigcap (P;\ P \in \mathrm{Var}\, I).$$

Důkaz. Pro prvoideál $P \supseteq I$ a pro $a \in \sqrt{I}$ máme $a^n \in P$ pro nějaké $n \geq 1$, a tedy $a \in P$, dle lemmatu I.3.10. Uvažme naopak $b \in \bigcap (P;\ P \in \mathrm{Var}\, I)$ a předpokládejme, že $b \notin \sqrt{I}$. Množina $S = \{b^k;\ k \geq 1\}$ pak neobsahuje nulu (neboť 0 v I leží), takže jde o multiplikativní množinu. Protože předpokládáme $S \cap I = \emptyset$, existuje podle tvrzení I.3.7 prvoideál $P \supseteq I$, který je s S disjunktní. To znamená $b \notin P$, takže b v uvažovaném průniku neleží. Obdrželi jsme spor. □

I.3.13 Důsledek. *Nilradikál okruhu R je roven průniku všech prvoideálů R.* □

Vedle průniku všech prvoideálů se často uvažuje i průnik všech maximálních ideálů. Tomuto průniku se říká *Jacobsonův radikál* a značí se $J(R)$. Maximální ideály jsou prvoideály, takže okamžitě můžeme vyslovit

I.3.14 Tvrzení. *V každém okruhu je nilradikál obsažen v Jacobsonově radikálu.*

Prvky Jacobsonova radikálu lze snadno charakterizovat. Tuto charakterizaci lze považovat za alternativní definici $J(R)$.

I.3.15 Tvrzení. *Prvek a okruhu R leží v $J(R)$ právě když $1 - ra$ je pro každé $r \in R$ invertibilní prvek R.*

Důkaz. Ať je $1 - ra$ pro každé r invertibilní a ať je M maximální ideál. Kdyby nebylo $a \in M$, bylo by $1 = ra + m$ pro nějaké $r \in R$ a $m \in M$. Prvky vlastních ideálů však invertibilní nejsou.

Naopak pro $a \in J(R)$ máme $ra \in J(R)$ pro každé $r \in R$ a $1 - ra$ musí být invertibilní. Kdyby totiž nebylo, leželo by $1 - ra$ v nějakém maximálním ideálu M, což vede ke sporu, neboť předpokládáme $ra \in J(R) \subseteq M$.

□

I.4 Volné moduly

Část obsahu této kapitoly lze beze změny přenést i na okruhy, jež nejsou komutativní. Je snadné si všimnout, kde je to možné.

Připomeňme, že pro libovolné moduly M_i, $i \in I$, okruhu R, je možné uvažovat jejich *direktní součet* (sumu) $\bigoplus(M_i;\ i \in I)$. Prvky této direktní sumy tvoří podmnožinu kartézského součinu množin M_i, $i \in I$, jež se sestává ze všech prvků $(m_i;\ i \in I)$, které mají $m_i \neq 0$ jen pro konečné mnoho $i \in I$. Každý modul M_j, $j \in I$, lze do $M = \bigoplus(M_i;\ i \in I)$ vnořit tak, že obrazem $m \in M_j$ je ten prvek $\nu_j(m) = (m_i;\ i \in I)$, který splňuje $m_j = m$ a má $m_i = 0$ pro $i \neq j$. Přitom obrazy $\mathrm{Im}(\nu_j)$ modulů M_j, $j \in I$, generují modul M. Pro každé $j \in I$ je podmodul N_j generovaný všemi $\mathrm{Im}(\nu_i)$, které mají $i \neq j$, možno vyjádřit jako

$$N_j = \{(m_i;\ i \in I) \in M;\ m_j = 0\}.$$

Zjevně $\mathrm{Im}(\nu_j) + N_j = M$ a $N_j \cap \mathrm{Im}(\nu_j) = 0$. Není těžké ověřit, že takovými vztahy lze direktní sumy strukturně popsat:

I.4.1 Tvrzení. *Ať M_i, $i \in I$, jsou podmoduly modulu M, které tento modul generují. Zobrazení*

$$\mu : \bigoplus M_i \to M,\ (m_i) \mapsto \sum m_i$$

je surjektivní homomorfismus modulů. Homomorfismus μ je izomorfismem modulů $\bigoplus M_i \cong M$ právě když pro každé $j \in I$ je $M_j \cap N_j = 0$, kde $N_j = \sum(M_i;$ $i \in I \setminus \{j\})$.

Důkaz. Ověřit, že μ je homomorfismus modulů, nečiní potíže. Protože moduly M_i generují M (tedy $\sum M_i = M$), jde o homomorfismus surjektivní. Prvek $(m_i;$ $i \in I)$ padne do jeho jádra právě když $\sum m_i = 0$. Uvažme takový prvek a ať $J \subseteq I$ je (konečná) množina všech $i \in I$, pro která $m_i \neq 0$. Je-li J neprázdná, má alespoň dva prvky a pro každé $j \in J$ je $-m_j = \sum_{i \in J, i \neq j} m_i$ nenulový prvek $M_j \cap N_j$. Naopak, z nenulovosti $M_j \cap N_j$ zjevně plyne existence takových nenulových $m_i \in M_i$, $i \in J \subseteq I$, že J je konečná, obsahuje j, a platí $\sum_{i \in J} m_i = 0$. Vidíme, že μ je injektivní právě když $M_j \cap N_j = 0$ pro každé $j \in I$. □

Kdykoliv v modulu M nalezneme podmoduly M_i, $i \in I$, takové, že $\sum M_i = M$ a $M_j \cap (M_i;\ i \in J \setminus \{j\}) = 0$ pro každé $j \in I$, je M podle tvrzení I.4.1 izomorfní $\bigoplus M_i$. Je zvykem i v takovém případě psát $M = \bigoplus M_i$, a nerozlišovat tak direktní sumu danou konstrukcí od direktní sumy strukturní (někteří autoři však po řadě hovoří o vnější a vnitřní direktní sumě). Chceme-li zjistit, zda modul M je roven direktní sumě generujících podmodulů M_i, bývá většinou jednodušší ověřit, že $\sum m_i$, kde $m_i \in M_i$, je rovno nule jedině tehdy, když každé m_i je nulové, než ověřovat, že moduly M_i a N_i mají pro každé $i \in I$ nulový průnik. Z tvrzení I.4.1 plyne, že oba postupy jsou možné.

Direktní sumu $\bigoplus(M_i;\ i \in I)$, ve které se všechny moduly M_i rovnají nějakému modulu N označíme $N^{(I)}$ (lze mluvit o *direktní mocnině*). Záhy objasníme zvláštní roli modulů $R^{(I)}$.

Podmnožina X modulu F se nazývá jeho *volnou bází*, jestliže X generuje F a jestliže pro každý modul M a každý výběr prvků $a_x \in M$, $x \in X$, existuje homomorfismus $\varphi : F \to M$ takový, že $\varphi(x) = a_x$ pro každé $x \in X$.

Homomorfismus φ je určen jednoznačně, neboť X generuje F (definici volné báze lze alternativně vyslovit také tak, že místo požadavku generování pomocí X se požaduje jednoznačnost φ).

Modul se nazývá *volný*, jestliže v něm lze nalézt alespoň jednu volnou bázi.

I.4.2 Lemma. *Ať X_i, $i \in \{1, 2\}$, jsou volné báze modulů F_i. Jsou-li množiny X_1 a X_2 stejně mohutné, jsou moduly F_1 a F_2 izomorfní.*

Důkaz. Uvažme nějakou bijekci $\xi : X_1 \to X_2$. Pak ξ lze rozšířit na homomorfismus $\varphi : F_1 \to F_2$ a ξ^{-1} na $\psi : F_2 \to F_1$. Protože $\psi\varphi$ a $\varphi\psi$ jsou na X_1 a X_2 po řadě identické, musí jít o identická zobrazení, takže $\varphi = \psi^{-1}$ je izomorfismus $F_1 \cong F_2$. □

I.4.3 Lemma. *Ať je X taková podmnožina modulu F, že každý prvek F lze jednoznačně vyjádřit ve tvaru $\sum_{x \in X} r_x x$, kde $r_x \in R$ je nenulové jen pro konečně mnoho $x \in X$. Potom je X volnou bází modulu F.*

Důkaz. Ať a_x, $x \in X$, jsou prvky modulu M. Definujme $\varphi : F \to M$ tak, že $\varphi(\sum r_x x) = \sum r_x a_x$. Definice je korektní, díky jednoznačnosti zápisu prvků F. Ověřit, že φ je homomorfismus, lze zcela přímočaře. □

I.4.4 Tvrzení. *Ať X je podmnožina modulu F. Je ekvivalentní:*

(i) X je volná báze F;

(ii) každý prvek F lze jednoznačně vyjádřit jako $\sum r_x x$, $x \in X$ a $r_x \in R$; a

(iii) existuje izomorfismus $F \cong R^{(X)}$, který zobrazuje každé $x \in X$ na $\nu_x(1)$ (kde $\nu_x : R \to R^{(X)}$ jsou homomorfismy, které vkládají R do x-té souřadnice).

Speciálně platí, že každý modul $R^{(X)}$ je volný, a to pro každou množinu X.

Důkaz. Je-li $\nu_x : R \to R^{(X)}$ vložením do x-té souřadnice, lze každé $(r_x;\ x \in X) \in R^{(X)}$ zapsat jako $\sum r_x \nu_x(1)$. Tento zápis je jednoznačný. Zbytek plyne z lemmat I.4.3 a I.4.2. □

Třída okruhů R, pro které platí, že dva volné moduly jsou izomorfní právě když jsou jejich volné báze stejně mohutné, je široká, avšak nezahrnuje všechny komutativní okruhy. Existují totiž takové okruhy, že lze nad nimi sestrojit modul, jenž má více volných bází různých mohutností. Ukážeme, že v případě oborů integrity je mohutnost volné báze ve volném modulu určena jednoznačně.

Z popisu volných modulů v lemmatu I.4.3 okamžitě dostáváme

I.4.5 Lemma. *Ať R je obor integrity a F volný modul nad R. Pak pro každé nenulové $r \in R$ a každá $u, v \in F$ z $ru = rv$ plyne $u = v$.*

Buď R i dále obor integrity a ať F je volný modul nad R. Podílové těleso oboru integrity R označíme T. Naším cílem je takové rozšíření F, aby v rozšířeném modulu bylo definováno skalární násobení prvky T. Naše konstrukce bude speciálním případem konstrukce torzního součinu $T \otimes F$. Provedeme ji explicitně, neboť na této úrovni se znalost obecného torzního součinu nepředpokládá.

Nosičem $T \otimes F$ je faktorizace $T \times F$ ekvivalencí $\sim$, kterou definujeme vztahem

$$(r_1/s_1, u_1) \sim (r_2/s_2, u_2) \Leftrightarrow r_1 s_2 u_1 = r_2 s_1 u_2.$$

K ověření korektnosti definice $\sim$ předpokládejme $r_1/s_1 = r_1'/s_1'$, tj. $r_1 s_1' = r_1' s_1$. Z $r_1 s_2 u_1 = r_2 s_1 u_2$ plyne $r_1 s_1' r_1' s_2 u_1 = r_1' s_1 r_2 s_1' u_2$, odkud $r_1' s_2 u_1 = r_2 s_1' u_2$ dle lemmatu I.4.5.

Relace $\sim$ je zjevně reflexivní a symetrická. Pokud $(r_1/s_1, u_1) \sim (r_2/s_2, u_2) \sim (r_3/s_3, u_3)$, tak máme $r_1 s_2 u_1 = r_2 s_1 u_2$ a $r_2 s_3 u_2 = r_3 s_2 u_3$, odkud $s_2 r_1 s_3 u_1 = s_3 r_1 s_2 u_1 = s_3 r_2 s_1 u_2 = s_1 r_2 s_3 u_2 = s_1 r_3 s_2 u_3 = s_2 s_1 r_3 u_3$, takže $r_1 s_3 u_1 = s_1 r_3 u_3$ dle lemmatu I.4.5, a tedy $(r_1/s_1, u_1) \sim (r_3/s_3, u_3)$.

Blok $\sim$ obsahující prvek $(\lambda, u) \in T \times F$ označíme $\lambda \otimes u$.

I.4.6 Lemma. *Pro každé $r \in R$ a každé $(\lambda, u) \in T \times F$ platí $(r\lambda) \otimes u = \lambda \otimes (ru)$. Každé $\lambda \otimes u$ je rovno nějakému $(1/s) \otimes v$, kde $s \in R$ je nenulové. Pro nenulová $s, s' \in R$ a $v, v' \in F$ je $(1/s) \otimes v = (1/s') \otimes v'$ právě když $s'v = sv'$. Konečně $\lambda \otimes u = 0 \otimes 0$ právě když $\lambda = 0$ nebo $u = 0$.*

Důkaz. Ať $\lambda = s/t$. Pak $(rs/t, u) \sim (s/t, ru)$, takže $(r\lambda) \otimes u = \lambda \otimes (ru)$. Zbytek se dokáže podobně snadno. □

Na $T \otimes F$ definujme operaci sčítání tak, že

$$(1/s) \otimes u \,+\, (1/s) \otimes v = (1/s) \otimes (u + v).$$

Z lemmatu I.4.6 plyne, že jde o korektně definovanou operaci. Ta je zjevně asociativní, $0 \otimes 0 = (1/s) \otimes 0$ je její neutrální prvek a $(1/s) \otimes (-u)$ je opačným prvkem prvku $(1/s) \otimes u$. Jde tedy o Abelovu grupu. Přitom pro libovolná $u, v \in F$ a $\lambda, \kappa \in T$ platí

$$\lambda \otimes u + \lambda \otimes v = \lambda \otimes (u + v) \text{ a } \lambda \otimes u + \kappa \otimes u = (\lambda + \kappa) \otimes u.$$

Prvý vztah je očividný. Pro druhý vyjádříme λ jako r/s a κ jako r'/s'. Máme $(\lambda \otimes u) + (\kappa \otimes u) = (1/(ss')) \otimes (rs'u) + (1/(ss')) \otimes (r'su) = (1/(ss')) \otimes (rs' + r's)u = (rs' + r's)/(ss') \otimes u = (\lambda + \kappa) \otimes u$.

Na $T \otimes F$ definujeme rovněž skalární násobení, a to vztahem

$$\kappa(\lambda \otimes u) = (\kappa\lambda) \otimes u.$$

Korektnost definice je opět očividná. Jistě $1(\lambda \otimes u) = \lambda \otimes u$, $(\kappa + \kappa')(\lambda \otimes u) = \kappa(\lambda \otimes u) + \kappa'(\lambda \otimes u)$, $\kappa(\kappa'(\lambda \otimes u)) = (\kappa\kappa')(\lambda \otimes u)$, takže zbývá ověřit $\kappa(\lambda \otimes u + \lambda' \otimes u') = (\kappa\lambda) \otimes u + (\kappa\lambda') \otimes u'$. To ovšem také nečiní potíže, a proto je $T \otimes F$ modulem nad T, tedy vektorovým prostorem nad T.

Tento vektorový prostor je samozřejmě rovněž R-modulem. Máme $r(1 \otimes u) = (1 \otimes ru)$ a $(1 \otimes u) + (1 \otimes v) = 1 \otimes (u + v)$, takže zobrazení $u \mapsto 1 \otimes u$ je homomorfismem R-modulů. V jeho jádru leží pouze $u = 0$, a proto můžeme prvky u a $1 \otimes u$ ztotožňovat. Volný R-modul F je tedy podmodulem vektorového prostoru $T \otimes F$.

Je-li x_i, $i \in I$, nějaká volná báze F, tak každé $\lambda \otimes u = \lambda(1 \otimes u) \in T \otimes F$ lze vyjádřit jako $\lambda(1 \otimes \sum r_i x_i) = \lambda(\sum r_i (1 \otimes x_i)) = \sum \lambda r_i (1 \otimes x_i)$, takže množina $\{1 \otimes x_i;\ i \in I\}$ vektorový prostor $T \otimes F$ generuje. Abychom dokázali, že jde o bázi, stačí ověřit, že z $\sum \lambda_i (1 \otimes x_i) = 0$ plyne nulovost všech λ_i, $i \in I$. Najděme $s \in R$, $s \neq 0$, takové, že všechna λ_i lze vyjádřit jako r_i/s, kde $r_i \in R$. Potom $\sum \lambda_i (1 \otimes x_i) = (1/s) \otimes (\sum r_i x_i) = 0$, odkud $r_i = 0$ pro všechna $i \in I$, a tedy i $\lambda_i = 0$ pro všechna $i \in I$.

Dimenze vektorového prostoru $T \otimes F$ je tedy rovna mohutnosti volné báze F. Protože dimenze vektorového prostoru je určena jednoznačně, můžeme vyslovit

I.4.7 Tvrzení. *Ať F je volný modul nad oborem integrity R. Pak všechny volné báze F mají stejnou mohutnost. Ta je rovna dimenzi vektorového prostoru $T \otimes F$, kde T značí podílové těleso oboru R.*

Této mohutnosti se říká *hodnost* (rank) volného modulu.

Později využijeme následující pozorování.

I.4.8 Lemma. *Ať M je podmodul volného R–modulu, kde R je obor integrity s podílovým tělesem T. Pak $T \otimes M = \{\lambda \otimes u;\ \lambda \in T \text{ a } u \in M\}$ je vektorový podprostor $T \otimes F$.*

Důkaz. Zjevně pro každá $x, y \in T \otimes M$ lze nalézt $s \in R$ a $u, v \in M$ tak, že $x = (1/s) \otimes u$ a $y = (1/s) \otimes v$. Z toho plyne, že $T \otimes M$ je uzavřeno na sčítání. Uzavřenost na skalární násobení je zřejmá. □

Zvláštní pozornost budeme věnovat volným modulům konečné hodnosti nad obory hlavních ideálů.

Ať R je obor hlavních ideálů a ať F je volný modul nad R konečné hodnosti $n \geq 1$. Pro volné báze $e_1, \ldots, e_n$ a $e'_1, \ldots, e'_n$, a pro prvek $a \in F$ uvažme ideály $(r_1, \ldots, r_n) = (s)$ a $(r'_1, \ldots, r'_n) = (s')$, kde $a = \sum r_i e_i = \sum r'_i e'_i$.

Podobně jako v lineární algebře sestrojme čtvercové matice M a M' řádu n nad R tak, aby $(e_1, \ldots, e_n)M = (e'_1, \ldots, e'_n)$ a $(e'_1, \ldots, e'_n)M' = (e_1, \ldots, e_n)$. Pak je též $(r_1, \ldots, r_n)M = (r'_1, \ldots, r'_n)$ a $(r'_1, \ldots, r'_n)M' = (r_1, \ldots, r_n)$. Z toho plyne, že s, jež dělí každé r_i, dělí každé r'_i, takže s dělí s'. Podobně s' dělí s, a proto máme $(s) = (s')$. Dokázali jsme, že pro daný prvek $a \in F$, $a = \sum r_i e_i$, ideál $(r_1, \ldots, r_n)$ nezávisí na volbě báze $e_1, \ldots, e_n$. Tento ideál se nazývá *obsah* (content) prvku a. Budeme ho značit $C(a)$.

I.4.9 Tvrzení. *Ať F je volný modul nad oborem hlavních ideálů R a ať $a \in F$ je nenulový, $C(a) = (s)$. Pak existuje volná báze $e_1, \ldots, e_n$ taková, že $a = se_1$. Speciálně lze každý nenulový prvek F vyjádřit jako skalární násobek prvku, který patří do nějaké volné báze.*

Důkaz. Případ $n = 1$ je jasný a dále budeme postupovat indukcí. Ať $a = \sum r_i e_i$, $1 \le i \le n$. Je-li některá z hodnot r_i nulová, lze jistě použít indukční předpoklad. Buďte všechny nenulové. Uvažme $b = a - r_1 e_1 = \sum_{i \ge 2} r_i e_i$. Podle indukčního předpokladu existuje $f \in \sum_{i \ge 2} Re_i$, jež padne do některé z těch volných bází F, jež současně obsahují e_1, a splňuje $b = tf$, kde $(t) = C(b)$. Položme $r = r_1$ a $e = e_1$. Máme $r = us$ a $t = vs$, přičemž z $(s) = (r, t)$ plyne existence $x, y \in R$ takových, že $s = xr + yt$. Odsud $xu + yv = 1$. Matice $\binom{u\ -y}{v\ \ \ x}$ má determinant rovný 1 a je vodítkem pro konstrukci volné báze s prvky $e' = ue + vf$ a $f' = -ye + xf$. Máme $se' = re + tf = a$, $e = xe' - vf'$ a $f = ye' + uf'$. □

I.4.10 Tvrzení. *Ať M je podmodul volného R-modulu F, který je konečné hodnosti n. Ať R je oborem hlavních ideálů. Mezi všemi ideály $C(a)$, $a \in M$, existuje největší.*

Důkaz. Vyberme $c \in M$ takové, že mezi uvažovanými ideály je $C(c)$ maximální. To možné je, neboť R je noetherovský okruh, takže M je noetherovský modul. Ať $e_1, \dots, e_n$ je taková volná báze M, že $c = se_1$, kde $C(c) = (s)$ (viz tvrzení I.4.9). Ukážeme, že pro každé $b = \sum r_i e_i$ z M je $C(b) = (r_1, \dots, r_n) \subseteq C(c)$. Ověření této inkluze má dva kroky – v prvém ověříme, že $r_1 \in (s)$ a v druhém, že každé r_i, $i \ge 2$, padne to (s).

Ať $(t) = (r_1, s)$ a ať $t = xr_1 + ys$. Pak $xb + yc = te_1 + (\sum_{i \ge 2} xr_i e_i) \in M$, odkud $C(c) = (s) \subseteq (t) \subseteq C(xb + yc)$. To dává $(s) = (t)$ a $r_1 \in (s)$, díky maximalitě $(s) = C(c)$. Je tedy $r_1 = sz$ pro nějaké $z \in R$, takže $se_1 + (\sum_{i \ge 2} r_i e_i) = b + (1 - z)se_1$ leží v M. Z maximality (s) a vztahu $(s) \subseteq C(b + (1 - z)se_1)$ dostáváme rovnost $(s) = C(b + (1 - z)se_1)$, takže každé r_i, $i \ge 2$, dělí s. □

V další kapitole ukážeme, jak lze tvrzení I.4.9 použít pro charakterizaci konečně generovaných modulů nad obory hlavních ideálů. Tuto kapitolu zakončíme jednou významnou obecnou vlastností volných modulů.

I.4.11 Tvrzení. *Ať R je komutativní okruh a N ať je podmodul modulu M. Pokud je M/N volný modul, lze nalézt podmodul $F \cong M/N$ modulu M takový, že $M = F \oplus N$.*

Důkaz. Uvažme $B \subseteq M$ takové, že $\{b + N;\ b \in B\}$ je volnou bází modulu M/N. Označme μ homomorfismus $M/N \to M$ takový, že $\mu(b + N) = b$ pro každé $b \in B$. Vztah $\mu(\sum r_b(b + N)) \in N$ lze též zapsat jako $\sum r_b b \in N$ nebo jako $\sum r_b(b + N) = N$. Ovšem $N = 0_{M/N}$, takže z posledního vyjádření plyne $r_b = 0$ pro každé $b \in B$, neboť modul M/N je volný. Dokázali jsme jednak $\mathrm{Im}(\mu) \cap N = 0$, jednak $\mathrm{Ker}\,\mu = 0$. Modul $\mathrm{Im}(\mu)$ je tedy volný a vzhledem k tomu, že B, jež v $\mathrm{Im}(\mu)$ leží, spolu s N generuje M, můžeme položit $F = \mathrm{Im}(\mu)$. □

I.5 Konečně generované moduly oborů hlavních ideálů

I.5.1 Lemma. *Konečně generované moduly nad noetherovskými okruhy jsou noetherovské.*

Důkaz. Konečně generované moduly jsou obrazy konečně generovaných volných modulů. Je-li R noetherovský okruh, tak volný modul R^k, $k \geq 1$, má podmodul izomorfní R^{k-1} a příslušný faktormodul je izomorfní R. Postupujeme-li indukcí, můžeme předpokládat, že R^{k-1} je noetherovský, a tím pádem je noetherovský i R^k (viz lemma I.1.6). Homomorfní obrazy noetherovských modulů jsou noetherovské. □

Ať R je komutativní okruh a M modul nad R. Modul M nazveme *cyklický* právě když existuje $a \in M$ takové, že $M = Ra$. Zobrazení $R \to M$, $r \mapsto ra$, je pak surjektivním homomorfismem modulů a jeho jádro je nějaký ideál, řekněme I. Každý cyklický modul je proto izomorfní R/I, pro nějaký ideál I, a každý modul takového tvaru je cyklický.

Homomorfismus $R \to M$, $r \mapsto ra$, lze zkonstruovat pro každé $a \in M$, bez ohledu na to, zda je M cyklický nebo ne. Jádro tohoto homomorfismu je ideál $\{r \in R;\, ra = 0\}$, který budeme značit $\mathrm{Ann}(a)$. Obecně pro $B \subseteq M$ je *anihilátor* $\mathrm{Ann}_R(B) = \mathrm{Ann}(B)$ definován jako $\{r \in R;\, rb = 0$ pro každé $b \in B\}$, a je to vždy ideál.

Pro $a, b \in M$ a $r, s \in R$ z $ra = 0$ a $sb = 0$ plyne $rs(a + b) = 0$. Je-li R obor integrity, tak z $r \neq 0$ a $s \neq 0$ plyne $rs \neq 0$. Odsud vidíme, že

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

je v případě oborů integrity podmodulem M. Tomuto podmodulu se říká *torzní část*. Modul M se nazývá *torzní* právě když je roven své torzní části. Naopak M nazveme *beztorzní* pokud $\tau(M) = 0$.

I.5.2 Lemma. *Ať je M modul nad oborem integrity R a ať $\tau(M)$ je jeho torzní část. Potom je modul $M/\tau(M)$ beztorzní.*

Důkaz. Uvažme $a \in M$ a nenulové $r \in R$ takové, že $r(a + \tau(M)) \subseteq \tau(M)$. To znamená $ra \in \tau(M)$, takže existuje nenulové $s \in R$, jež splňuje $s(ra) = 0$. Tudíž $sr \in \mathrm{Ann}(a)$, takže $a \in \tau(M)$. □

Pro ideál I komutativního okruhu R a pro R-modul M je $\{a \in M;\, ra = 0$ pro každé $r \in I\}$ jistě podmodul M. Označíme-li tento N_1 a označíme-li N_j, $j \geq 0$, analogicky definovaný podmodul vzhledem k ideálu I^j, bude $N_1 \subseteq N_2 \subseteq \dots$. Modul $N = \bigcup(N_j;\, j \geq 0)$ označíme $\tau_I(M)$. Je tedy

$$\tau_I(M) = \{a \in M;\ \text{ existuje } j \geq 1,\ \text{ že } ra = 0 \text{ pro každé } r \in I^j\}.$$

Ideály $\tau_I(M)$ jsme definovali pro obecný komutativní okruh R, zde je však budeme používat pouze v případě, kdy R je obor integrity a I jeho vlastní ideál. Pak jistě $\tau_I(M) \subseteq \tau(M)$.

I.5.3 Tvrzení. *Ať R je obor hlavních ideálů a ať $\mathcal{P}$ je množina všech jeho prvoideálů. Pak pro každý torzní R-modul M platí*

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

Důkaz. Uvažme $u \in M$ nenulové. Pak $\mathrm{Ann}(u) = (r)$ pro nějaké $r = p_1^{c_1} \dots p_k^{c_k}$, $k \geq 1$, kde p_i jsou prvočinitelé a $c_i \geq 1$, $1 \leq i \leq k$. Položme $s_i = r/p_i^{c_i}$, $1 \leq i \leq k$. Jelikož $s_1, \dots, s_k$ jsou nesoudělná, máme $1 = \sum x_i s_i$ pro nějaké $x_i \in R$, $1 \leq i \leq k$. Tudíž $u = 1 \cdot u = \sum x_i s_i u$. Ovšem $x_i s_i u \in \tau_{(p_i)}(M)$, neboť $p_i^{c_i}(x_i s_i u) = x_i r u = 0$. Dokázali jsme, že moduly $\tau_p(M)$ generují M.

Ať p je prvočinitel a ať $u \in M$ leží v průniku modulu $\tau_{(p)}(M)$ a modulu $\sum(\tau_P(M);\ P \in \mathcal{P} \setminus (p))$. Pak existuje nenulové $r \in R$, které je nesoudělné s p a splňuje $ru = 0$. Současně je $p^c u = 0$ pro nějaké $c \geq 1$. Protože existují $x, y \in R$ takové, že $xp^c + yr = 1$, máme $u = (xp^c + yr)u = 0$. Uvažovaný průnik je tudíž nulový. □

I.5.4 Tvrzení. *Ať R je obor hlavních ideálů a ať M je konečně generovaný beztorzní modul nad R. Potom je M volný modul.*

Důkaz. Uvažme nějaký surjektivní homomorfismus $\varphi : F \to M$, kde F je volný modul nad R hodnosti n. Předpokládejme, že n je nejmenší možné. Je-li $\mathrm{Ker}(\varphi) = 0$, tak $F \cong M$ a M je volný. Předpokládejme $\mathrm{Ker}(\varphi) \neq 0$. Podle tvrzení I.4.9 existuje volná báze $e_1, \dots, e_n$ modulu F a nenulové $r \in R$ takové, že $re_1 \in \mathrm{Ker}(\varphi)$. To znamená $\varphi(re_1) = r\varphi(e_1) = 0$, odkud $\varphi(e_1) = 0$, neboť R je beztorzní. Pak ovšem $\varphi(e_2), \dots, \varphi(e_n)$ generují M a n není nejmenší možné. □

Jako důsledek jdoucí mimo hlavní směr tohoto oddílu zmiňme

I.5.5 Důsledek. *Ať R je obor hlavních ideálů a ať M je podmodul volného R–modulu F konečné hodnosti n. Potom je M volný R–modul hodnosti $\leq n$.*

Důkaz. Modul F je noetherovský, podle lemmat I.1.4 a I.5.1, a proto je noetherovský i modul M, podle lemma I.1.6. To znamená, že modul M je konečně generovaný, a tedy volný, podle tvrzení I.5.4. Omezení jeho hodnosti vyplývá z lemma I.4.8 a tvrzení I.4.7 □

I.5.6 Důsledek. *Ať R je obor hlavních ideálů a ať M je konečně generovaný modul nad R. Potom existuje volný modul F takový, že $M = F \oplus \tau(M)$.*

Důkaz. Lze spojit lemma I.5.1, lemma I.5.2, tvrzení I.5.4 a tvrzení I.4.11. □

Podle důsledku I.5.6 a tvrzení I.5.3 proto pro charakterizaci konečně generovaných R-modulů, kde R je obor hlavních ideálů, potřebujeme znát strukturu konečně generovaných podmodulů $\tau_P(M)$, kde P je prvoideál. Dříve než začneme řešit tento úkol, učiníme malé obecné pozorování.

Je-li I takový ideál okruhu R, že pro daný R-modul M platí $IM = 0$ (tedy $I \subseteq \mathrm{Ann}(M)$), lze M chápat také jako R/I-modul, kde $(r + I)a = ra$ pro všechna $r \in R$, $a \in M$. Je-li R komutativní a I maximální, dostaneme tak na M strukturu vektorového prostoru. V oboru hlavních ideálů jsou prvoideály maximální, takže z $PM = 0$ vyplývá $M = \bigoplus(M_i;\ i \in I)$, kde $M_i \cong R/P$ jsou jednodimenzionální podprostory M chápaného jako vektorový prostor nad R/P, které jsou odvozeny z nějaké báze tohoto vektorového prostoru.

Mějme tedy R obor hlavních ideálů a ať P je prvoideál R. Uvažme prvočinitel p takový, že $P = (p)$. Na chvíli budeme *p-modulem* nazývat každý R-modul M takový, že $\tau_{(p)}(M) = M$. Jinými slovy, M je p-modul právě když pro každé $u \in M$ existuje $i \geq 1$ takové, že $p^i u = 0$. Nejmenší takové i se nazývá *výškou* (nebo p-výškou) prvku u. Prvky výšky $\leq i$ zjevně tvoří podmodul M. Je-li M generován prvky $g_1, \dots, g_n$ a k je nejvyšší z výšek těchto prvků, má každý prvek M výšku nejvýše k (čili platí $p^k u = 0$ pro každé $u \in M$). Prvkem výšky 0 je pouze nulový prvek M. Prvky výšky ≤ 1 tvoří podmodul, kterému se říká *dolní vrstva* (sokl). Dolní vrstvu můžeme chápat jako vektorový prostor nad tělesem $R/(p)$. Značí se $\mathrm{Soc}(M)$. (Obecně je $\mathrm{Soc}(M)$ podmodul generovaný všemi jednoduchými podmoduly. Modul je *jednoduchý*, nemá-li vlastní nenulové podmoduly.)

I.5.7 Lemma. *Pro p-modul M a $u \in M$ platí $uR = ruR$ kdykoliv $r \in R$ není dělitelné p. V takovém případě mají u i ru stejné p-výšky.*

Důkaz. Ať u má výšku k. Existují $x, y \in R$ taková, že $xp^k + yr = 1$. To znamená, že $ruR \supseteq yruR = (1 - xp^k)uR$, což se shoduje s uR, neboť $xp^k ur = 0$ pro každé $r \in R$. Jistě platí i $uR \supseteq ruR$, takže $uR = ruR$, a tudíž $u = s(ru)$ pro nějaké $s \in R$. To, že u a ru mají stejné výšky, je nyní již zřejmé. □

I.5.8 Lemma. *Každý konečně generovaný p-modul lze vyjádřit jako direktní sumu cyklických modulů $u_1R \oplus \cdots \oplus u_tR$, kde pro každé j, $1 \leq j \leq t$, existuje $m = m_j \geq 1$ takové, že $u_jR \cong R/(p^m)$.*

Důkaz. Ať M_i značí podmodul M tvořený prvky výšky $\leq i$. Buď k nejmenší takové, že $M_k = M$. Je-li $k = 0$, je M nulový modul, je-li $k = 1$, je M roven své dolní vrstvě $M_1 = \mathrm{Soc}(M)$. Případ $k > 1$ dokážeme indukcí dle k.

Modul M/M_1 je konečně generovaný a každý jeho prvek je výšky $\leq k - 1$. Podle indukčního předpokladu existují $u_1, \dots, u_{t'} \in M$ taková, že $M/M_1 = \bigoplus(u_j + M_1)R$, kde $u_j + M_1$ má v M/M_1 výšku n_j, $1 \leq n_j \leq k - 1$. Z $p^{n_j}(u_j + M_1) = M_1$ plyne $p^{n_j+1}u_j = 0$, takže vidíme, že u_j má v M výšku $n_j + 1$, $1 \leq j \leq t'$.

Uvažme podmodul N modulu M, který je generován prvky $u_1, \dots, u_{t'}$. K tomu, abychom dokázali $N = \bigoplus u_jR$, je třeba ověřit, že ze $\sum r_ju_j = 0$ plyne $r_1u_1 = \cdots = r_{t'}u_{t'} = 0$. Ať $r_j = p^{h_j}x_j$, kde p nedělí x_j, a ať $\sum r_ju_j = 0$. Potom $\sum r_j(u_j + M_1) = M_1$, takže $r_1(u_1 + M_1) = \cdots = r_{t'}(u_{t'} + M_1) = M_1$. To znamená $h_j \geq n_j \geq 1$ pro každé j, $1 \leq j \leq t'$ (činitel x_j na výšku $u_j + M_1$ v R/M_1 vliv nemá, podle lemmatu I.5.7 a $p_j^{n_j-1}u_j \notin M_j$ díky volbě n_j).

Pro každé j je $n_j \geq 1$, a proto i $h_j ge1$. Vztah $\sum r_ju_j = 0$ lze tudíž zapsat jako $p(\sum(p^{h_j-1}x_j)u_j) = 0$, takže $\sum(p^{h_j-1}x_j)u_j \in M_1$ a $\sum(p^{h_j-1}x_j)(u_j+M_1) = M_1$. Odsud $p^{h_1-1}x_j(u_1+M_1) = \cdots = (p^{h_{t'}-1}x_{t'})(u_{t'}+M_1) = M_1$, a tedy $h_j - 1 \geq n_j$ pro každé j, $1 \leq j \leq t'$. Proto $h_j \geq n_j + 1$ a $r_ju_j = p^{h_j}x_ju_j = 0$.

Ať N_0 je nějaký doplněk $N \cap M_1 = N_1$ v M_1. Takový doplněk existuje, neboť M_1 lze chápat jako vektorový prostor nad $R/(p)$. Pak $N \cap N_0 = N \cap N_0 \cap M_1 = N_1 \cap N_0 = 0$ a $N + N_0 = N + N_1 + N_0 = N + M_1 = M$. Tudíž $N = N_1 \oplus N_0$, a zbytek je již jasný. □

Nyní vyslovíme snadné obecné lemma.

I.5.9 Lemma. *Buďte $M = \bigoplus(M_i;\ i \in I)$ modul a $N = \bigoplus(N_i;\ i \in I)$ takový jeho podmodul, že $N_i \subseteq M_i$ pro každé $i \in I$. Potom $M/N \cong \bigoplus(M_i/N_i;\ i \in I)$.*

Důkaz. Vyjdeme od homomorfismu $\varphi : M \to \bigoplus(M_i/N_i)$, $\varphi(u_i;\ i \in I) = (u_i + N_i;\ i \in I)$. Jeho jádro jsou všechny prvky (u_i) takové, že $u_i \in N_i$ pro každé $i \in I$. To znamená, že $\mathrm{Ker}(\varphi) = N$, a zbytek plyne z 1. věty o izomorfismu. □

I.5.10 Lemma. *Ať $M = N_1 \oplus \cdots \oplus N_t = N_1' \oplus \cdots \oplus N_{t'}'$ jsou dvě vyjádření konečně generovaného p-modulu M jako direktní sumy cyklických modulů. Předpokládejme $N_j \cong R/(p^{m_j})$, $1 \le j \le t$, a $N_j' \cong R/(p^{m_j'})$, $1 \le j \le t'$, a dále ať $m_1 \ge m_2 \ge \cdots \ge m_t \ge 1$ a $m_1' \ge m_2' \ge \ldots m_t' \ge 1$. Potom $t = t'$ a $m_j = m_j'$, $1 \le j \le t$.*

Důkaz. Budeme postupovat obdobně jako v důkazu lemmatu I.5.8, ale z opačného konce. Dolní vrstva $\mathrm{Soc}(M)$ je zřejmě rovna direktní sumě $\mathrm{Soc}(N_1) \oplus \cdots \oplus \mathrm{Soc}(N_t)$. Odsud $t = t'$, neboť jde o dimenzi $R/(p)$-modulu $\mathrm{Soc}(M)$. Podle lemmatu I.5.9 je $M/\mathrm{Soc}(M) \cong N/\mathrm{Soc}(N_1) \oplus \cdots \oplus N/\mathrm{Soc}(N_t)$. Cyklický modul $N/\mathrm{Soc}(N)$ je generován prvky výšky $m_j - 1$, takže lemma snadno plyne indukcí dle maxima m_j, $1 \le j \le t$. □

Spojením tvrzení I.5.3, důsledku I.5.6, lemmatu I.5.8 a lemmatu I.5.10 dostáváme hlavní tvrzení této kapitoly.

I.5.11 Věta. *Ať M je konečně generovaný modul nad oborem hlavních ideálů R. Pak existují po dvou různé prvoideály P_i a moduly M_i, $1 \le i \le m$, že*

$$M = M_1 \oplus \cdots \oplus M_m \oplus F,$$

kde F je volný modul hodnosti $h_0 \ge 0$ a pro každé i, $1 \le i \le m$, je

$$M_i = N_{i1} \oplus \cdots \oplus N_{ih_i}, \quad h_i \ge 1,$$

kde N_{ij}, $1 \le j \le h_j$, je cyklický modul izomorfní $R/P_i^{t_{ij}}$, přičemž

$$t_{i1} \ge t_{i2} \ge \cdots \ge t_{ih_i} \ge 1.$$

Čísla $m, h_0, h_1, \ldots, h_m$ a t_{ij}, $1 \le i \le m$ a $1 \le j \le h_i$, jsou určena jednoznačně.

I.6 Podmoduly volných modulů v oborech hlavních ideálů

Uveďme nejprve následující jednoduché lemma

I.6.1 Lemma. *Ať M je modul nad okruhem R. Buďte N, U a V jeho podmoduly takové, že $U \subseteq V$, $U \cap N = V \cap N$ a $(U+N)/N = (V+N)/N$. Pak $U = V$.*

Důkaz. Pro každé $v \in V$ exituje $n \in N$, že $v + n = u \in U \subseteq V$. Tudíž $n = u - v \in U \cap N = V \cap N$, takže $v = u - n \in V$. □

Prvním cílem oddílu je popsat podmoduly volného modulu F konečné hodnosti n nad oborem hlavních ideálů R. Takový podmodul je beztorzní a konečné generovaný, podle lemmatu I.5.1, a proto je též volný, podle tvrzení I.5.4. Popis všech takových podmodulů, který podáme, bude ovšem jeho volnost implikovat přímo, nezávisle na výsledcích oddílu I.5. Dokážeme totiž, že v F lze nalézt volnou bázi $e_1, \ldots, e_n$ a prvky $r_1, \ldots, r_n \in R$ takové, že daný podmodul je generován $r_1e_1, \ldots, r_ne_n$. Nenulové prvky z tohoto seznamu zřejmě tvoří volnou bázi podmodulu. Přitom uvidíme, že $r_1, \ldots, r_n$ lze volit tak, aby $r_1|r_2, \ldots, r_{n-1}|r_n$. Důkaz se bude opírat o tvrzení I.4.9 a I.4.10.

I.6.2 Věta. *Ať R je obor hlavních ideálů, F volný R-modul konečné hodnosti n a $M \subseteq F$. Pak existují jednoznačně určené ideály $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n$ okruhu R takové, že po některou volnou bázi $e_1, \ldots, e_n$ modulu F platí*

$$M = I_1e_1 + \cdots + I_ne_n.$$

Důkaz. Zvolme e_1 a I_1 tak, že I_1 je největší ze všech ideálů $C(a)$, $a \in M$, a že $I_1e_1 \subseteq M$, kde $C(e_1) = R$. Taková volba je podle tvrzení I.4.10 a I.4.9 možná (připomeňme, že vztah $C(e_1) = R$ je podle tvrzení I.4.10 ekvivalentní předpokladu, že e_1 je prvek nějaké volné báze.) Je-li $n = 1$, je každé $b \in F$ tvaru re_1, přičemž z $b \in M$ plyne $r \in C(b) \subseteq I_1$, takže $I_1e_1 = M$. Pro $n = 1$ tedy hledaný rozklad existuje; dále budeme postupovat indukcí.

Uvažme modul $F' = F/Re_1$ a jeho podmodul $M' = (M + Re_1)/Re_1$. Podle indukčního předpokladu existují ideály $I_2 \supseteq \cdots \supseteq I_n$ okruhu R a prvky $e_2, \ldots, e_n \in F$ takové, že $e_2' = e_2 + Re_1, \ldots, e_n' = e_n + Re_1$ je volná báze modulu F' a $M' = I_2e_2' + \cdots + I_ne_n'$. Jsou-li $r_i \in R$, $2 \leq i \leq n$, taková, že $\sum_{i \geq 2} r_ie_i \in Re_1$, je $r_2 = \cdots = r_n = 0$, neboť $e_2', \ldots, e_n'$ je volná báze F'.

Vidíme, že $e_1, \ldots, e_n$ je volná báze F. Uvažme nyní nějaké j, $2 \leq j \leq n$, a ať $I_j = (r)$ a $I_1 = (s)$. Protože $re_j + Re_1 \in M'$, musí existovat $f \in Re_1$ že $re_j + f \in M$. Ovšem z $C(re_j + f) \subseteq I_1$ vyplývá existence $x, y \in R$ takových, že $r = xs$ a $f = yse_1$. Je tedy $I_j \subseteq I_1$ a $re_j \in M$.

Vidíme, že je $I_1 \supseteq I_2 \supseteq \ldots I_n$ a že $U = \sum I_je_j \subseteq M$. Jistě $U \cap Re_1 = M \cap Re_1 = I_1e_1$ a $(U + Re_1)/Re_1 = M' = (M + Re_1)/Re_1$. Proto $U = M$, dle lemmatu I.6.1. Existence požadovaného vyjádření M je dokázána.

Jednoznačnost vyžaduje následující úvahu. Ať $k \leq n$ je největší takové, že $I_k = I_1$. Pak $\{a \in M; C(a) = I_1\}$ zjevně leží v $I_1(Re_1 + \cdots + Re_k)$, a navíc tento podmodul generuje. Ideál I_1 je od M odvozen jednoznačným způsobem, takže je jednoznačně určen i podmodul $M_1 = I_1(Re_1 + \cdots + Re_k) = I_1e_1 + \cdots + I_1e_k$. Tento podmodul je volný (například proto, že ideál I_1 je hlavni) a k je jeho hodnost (ta je určena jednoznačně podle tvrzení I.4.7). Současně $F_1 = Re_1 + \cdots + Re_k$ je rovno $\{a \in F; I_1a \in M_1\}$.

Je-li tedy $M = I'_1e'_1 + \cdots + I'_ne'_n$ konkurenční vyjádření modulu M, bude $I_1 = I'_1 = \cdots = I'_k$, $M_1 = I_1e'_1 + \ldots I_ke'_k$ a $F_1 = Re'_1 + \cdots + Re'_k$. Modul $(M + F_1)/F_1$ je podmodulem volného modulu F/F_1, který má volné báze jak $e_{k+1} + F_1, \ldots, e_n + F_1$, tak $e'_{k+1} + F_1, \ldots, e'_n + F_1$. Přitom $(M + F_1)/F_1$ lze vyjádřit jako

$$I_{k+1}(e_{k+1} + F_1) + \cdots + I_n(e_n + F_1) = I'_{k+1}(e'_{k+1} + F_1) + \cdots + I'_n(e'_n + F_1),$$

takže z indukčního předpokladu dostáváme $I_j = I'_j$ pro každé j, $k \le j \le n$. □

Všechny ideály I_j jsou hlavní, ať například $I_j = r_jR$. Pak lze každý prvek M zapsat jako $\sum a_jr_je_j$, kde $a_j \in R$ je určeno jednoznačně kdykoliv $r_j \neq 0$. Proto z věty I.6.2 okamžitě vyplývá již dříve naznačená charakterizace volných podmodulů:

I.6.3 Důsledek. *Ať R je obor hlavních ideálů, ať F je volný modul nad R, který má konečnou hodnost n, a ať M je jeho podmodul. Pak lze nalézt volnou bázi $e_1, \ldots, e_n$ modulu F a prvky $r_1, \ldots, r_n \in R$ takové, že $r_1|r_2, \ldots, r_{n-1}|r_n$ a $M = \sum Rr_ie_i$. Ať k je nejvyšší takové, že $r_k \neq 0$, kde $0 \le k \le n$. Pak $r_1e_1, \ldots, r_ke_k$ tvoří volnou bázi modulu M.*

Připomeňme ještě jedno jednoduché lemma obecné povahy.

I.6.4 Lemma. *Ať $M = \bigoplus_{i\in I} M_i$ je modul nad okruhem R, s podmodulem $N = \bigoplus_{i\in I} N_i$, kde $N_i \subseteq M_i$ pro všechna $i \in I$. Pak $(m_i;\ i \in I) + N \mapsto (m_i + N;\ i \in I)$ určuje izomorfismus $M/N \cong \bigoplus_{i\in I} M_i/N_i$.*

Důkaz. Vyjděme z izomorfismu $(m_i; i \in I) \mapsto (m_i + N;\ i \in I)$. Jeho jádro je rovno N, takže lemma plyne z 1. věty o izomorfismu. □

I.6.5 Důsledek. *Ať M je konečně generovaný R-modul, kde R je obor hlavních ideálů. Pak existují vlastní ideály $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n \supseteq 0$ takové, že $M \cong R/I_1 \oplus \cdots \oplus R/I_n$.*

Důkaz. Modul M je obrazem volného modulu F konečné hodnosti n. Zvolme n minimální možné a pro nějaký surjektivní homorfismus $\varphi : F \to M$ najděme ideály $I_1 \supseteq I_n$ a volnou bázi $e_1, \ldots, e_n$ tak, že $\operatorname{Ker}\varphi = \sum I_je_j$. Jejich existence plyne z věty I.6.2. Je-li $I_1 = R$, je $M = \varphi(\sum_{i\ge 2} Re_j)$, což je ve sporu s volbou n. Proto je I_1 ideál vlastní a podle 1. věty o izomorfismu a podle lemmatu I.6.4 máme $M \cong F/\operatorname{Ker}\varphi \cong \bigoplus R/I_j$. □

Je nasnadě očekávat, že modul M určuje posloupnost $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n$ jednoznačně. Tak tomu skutečně je. Důkaz není obtížný, ale vyžaduje zavedení několika mála předběžných pojmů. Bylo by také možné jednoznačnost ideálů odvodit z věty I.5.11. Dáme však přednost přímému důkazu.

Je-li M modul nad komutativním okruhem R a J je ideál R, je

$$JM = \{au;\ a \in J \text{ a } u \in M\}$$

jistě podmodul M. Pokud $M = \bigoplus(M_i;\ i \in I)$, tak zřejmě $JM = \bigoplus(JM_i;\ i \in I)$.

Zapíšeme-li vztah $x = yz^{-1}$ (platný například v nějakém komutativním tělese) jako $x = y : z$, máme $x = y : z \Leftrightarrow xz = y$. Rozšířením tohoto vztahu na podmnožiny A a B modulu M nad komutativním okruhem R dostaneme tuto definici:

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

Zde nás bude zajímat situace, kdy modul M je roven R. Připomeňme, že podmoduly R se shodují s ideály R.

I.6.6 Lemma. *Ař R je komutativní okruh s ideály I a J. Pak $(I : J)$ je ideál, který obsahuje I. Přitom $(I : J) = R$ právě když $J \subseteq I$. Dále platí $(I : J) = (I : I + J)$, a je-li J hlavní ideál, tak též $J(R/I) \cong R/(I : J)$.*

Důkaz. Ověřit, že $(I : J)$ je ideál, je snadné. Pro $a \in I$ je jistě $aJ \subseteq I$, takže $(I : J) \supseteq I$. Rovnost $(I : J) = R$ nastává právě když $1 \in (I : J)$, tedy $J \subseteq I$. Pro $a \in R$ je $aJ \subseteq I$ právě když $a(I + J) \subseteq I$, a proto $(I : J) = (I : I + J)$. Předpokládejme, že $J = uR$. Homomorfismus $R \to J(R/I)$, $r \mapsto ur + I$, má jádro tvořeno všemi $r \in R$, že $ru \in I$. To jsou ovšem právě ta $r \in R$, jež splňují $rJ \subseteq I$. □

I.6.7 Lemma. *Ať I je nenulový ideál oboru hlavních ideálů R. Pro každý ideál $J \supseteq I$ platí $I = J\,(I : J)$. Pro ideály $J_1 \supseteq I$ a $J_2 \supseteq I$ máme $(I : J_1) = (I : J_2)$ právě když $J_1 = J_2$.*

Důkaz. Ať $J = bR$ a $I = aR$. Z $bR \supseteq aR$ plyne existence $c \in R$, že $a = bc$. Jistě $ar = (bR)(cR)$, přičemž $cR \subseteq (I : J)$. Je-li naopak $u \in (I : J)$, musí být $ub = ar$ pro nějaké $r \in R$, odkud $ub = bcr$ a $u = cr$, takže $cR = (I : J)$.

Je-li $J_k = b_kR$, kde $a = b_kc_k$, $k \in \{1, 2\}$, tak $J_1 = J_2 \Leftrightarrow c_1R = c_2R \Leftrightarrow (I : J_1) = (I : J_2)$. □

I.6.8 Věta. *Buď M konečně generovaný modul nad oborem hlavních ideálů R. Pak existují jednoznačně určené vlastní ideály $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n \supseteq 0$ takové, že $M \cong R/I_1 \oplus \cdots \oplus R/I_n$.*

Důkaz. Existence plyne z důsledku I.6.5. Ať ještě $M \cong R/J_1 \oplus \cdots \oplus R/J_m$, kde $J_1 \supseteq J_2 \supseteq \cdots \supseteq J_m \supseteq 0$ jsou také vlastní ideály R. Budeme postupovat indukcí dle $n + m$. Případy $n = 0$ či $m = 0$ netřeba uvažovat, neboť oba nastanou právě když M je nulový modul. Jelikož $\mathrm{Ann}(R/I) = I$, je $R/I \cong R/J$ právě když $I = J$ (to samozřejmě platí pro každý okruh). Můžeme tedy předpokládat $m \geq n$ a $m \geq 2$. Položme $I = J_1$ a $J = J_1$. Podle lemmatu I.6.6 je

$$IM = R/(I_1 : I) \oplus \cdots \oplus R/(I_n : I) \text{ a}$$
$$IM = R/(J_1 : I) \oplus \cdots \oplus R/(J_m : I).$$

Protože $(I_1 : I) = R$, máme dva rozklady modulu IM, které dohromady mají méně než $n + m$ nenulových komponent. (Přitom zřejmě $(I_1 : I) \supseteq ... \supseteq (I_n : I)$ a $(J_1 : I) \supseteq \cdots \supseteq (J_m : I)$.) Lze na ně tudíž vztáhnout indukční předpoklad, takže IM musí mít méně než m nenulových komponent. To podle lemmatu I.6.6 znamená $I \subseteq J_1 = J$. Vidíme, že J je největší ze všech ideálů I_r, $1 \leq r \leq n$, a J_s, $1 \leq s \leq m$. Zvolme $P \supseteq J$ maximální ideál. Pak

$$PM \cong P/I_1 \oplus \cdots \oplus P/I_n \cong P/J_1 \oplus \cdots \oplus P/J_m.$$

Z lemmatu I.6.4 máme

$$M/PM \cong (R/I_1)(P/I_1) \oplus \cdots \oplus (R/I_n)/(P/I_n) \cong (R/P)^n \cong (R/P)^m.$$

Odsud $n = m$, neboť toto číslo je dimenzí vektorového prostoru M/PM nad tělesem (R/P).

Víme-li, že $n = m$, tak můžeme podobnou úvahou jako výše analyzovat modul JM, a dostaneme $J \subseteq I$. Je tedy $I = J$, takže $J_s \subseteq I$ pro každé s, $1 \leq s \leq m$. Z výše uvedených vyjádření IM tedy podle indukčního předpokladu plyne, že $I_k = I$ právě když $J_k = I$, přičemž nejvyšší takové $k \leq n$ udává počet nulových komponent v těchto vyjádřeních.

Dále podle indukčního předpokladu $(I_r : I) = (J_r : I)$ pro každé r, $k < r \leq n$, a tedy $I_r = J_r$ dle lemmatu I.6.7. $\square$

II Základy Galoisovy teorie

II.1 Rekapitulace základních poznatků

Tělesem vždy budeme rozumět těleso komutativní. Homomorfismus $f: T \to R$ tělesa T do netriviálního okruhu R je vždy injektivní. Speciálně jsou proto injektivní i veškeré endomorfismy tělesa T. Mezi nimi má zvláštní postavení *Frobeniův endomorfismus* $x \mapsto x^p$, který je definován v případě kladné charakteristiky $p > 0$.

Charakteristika p udává až na isomorfismus *prvotěleso* P, tedy nejmenší podtěleso tělesa T. Prvotěleso je isomorfní p-prvkovému tělesu $\mathbb{F}_p$ v případě $p > 0$, a tělesu racionálních čísel $\mathbb{Q}$ v případě $p = 0$. Jediným endomorfismem prvotělesa P je identita 1_P (případ kladné charakteristiky je zřejmý, pro $f \in \mathrm{End}(\mathbb{Q})$ nejprve odvodíme $f(i) = i$ pro $i \in \mathbb{Z}$, odsud $f(1/j) = 1/j$ pro j nenulové, a tedy $f(i/j) = i/j$).

Všechna podtělesa daného tělesa T tvoří uzávěrový systém. Tento uzávěrový systém může obsahovat méně množin než uzávěrový systém všech podokruhů T. Je-li F podtěleso a M podmnožina T, budeme nejmenší podokruh obsahující $F \cup M$ označovat $F[M]$, zatímco nejmenší takové podtěleso označíme $F(M)$.

Pro homomorfismus okruhů $f: R \to S$ definujeme homomorfismus $f_x: R[x] \to S[x]$, který rozšiřuje f tak, aby platilo $f_x(x) = x$. Přitom $R[x]$ označuje okruh polynomů v proměnné x. Je-li $R = T$ těleso, je tento okruh eukleidovským oborem integrity. Je-li $f: R \cong S$ isomorfismus okruhů, je jím i $f_x: R[x] \cong S[x]$.

Jsou-li $R \subseteq S$ komutativní okruhy a α je prvek S, tak $j_\alpha: R[x] \to S$ označuje *dosazovací homomorfismus.* Pro $f: R \to S$ homomorfismus komutativních okruhů a $\alpha \in R$ máme $f j_\alpha = j_{f(\alpha)} f_x$. Z této rovnosti například vyplývá, že pokud α je kořenem polynomu a (tedy $j_\alpha(a) = 0$), tak je $f(\alpha)$ kořenem polynomu $f_x(a)$. Speciálně vidíme, že isomorfismy f komutativních okruhů zobrazují množinu kořenů a na množinu kořenů $f_x(a)$.

Jsou-li $T \leq U$ tělesa, nazveme $\alpha \in U$ *algebraický*, pokud je α kořen nějakého $a \in T[x]$. Všechny polynomy, jež mají za kořen α, tvoří ideál v $T[x]$ a monický generátor tohoto ideálu se nazývá *minimální polynom* prvku α nad T. Těleso U lze chápat jako vektorový prostor nad T, jeho dimenze $\dim_T(U)$ se značí $[U : T]$ a mluví se o *stupni* U nad T. Pro $\alpha \in U$ algebraický platí, že je $T(\alpha) = T[\alpha]$ a že $[T(\alpha) : T]$ se shoduje se stupněm minimálního polynomu (je-li tento roven k, tvoří $1, \alpha, \ldots, \alpha^{k-1}$ bázi U nad T). Přitom $\alpha \in U$ je algebraický nad T právě když $T(\alpha)$ je nad T konečného stupně.

V případě vřazených těles $T \leq U$ se mluví o U jako o *rozšíření* T. Máme-li $T \leq U \leq V$, je $[V : U][U : T] = [V : T]$, přičemž bázi V nad T lze sestrojit jako součiny ab, kde a probíhá bázi V nad U, b probíhá bázi U nad T. *Rozšíření* U nad T se nazývá *algebraické*, je-li každý prvek U algebraický nad T. Rozšíření konečného stupně je vždy algebraické a pro množinu M prvků z U, které jsou algebraické nad T, platí $T(M) = T[M]$. Navíc je $T(M)$ nad T algebraické rozšíření, takže má smysl mluvit o *algebraickém uzávěru* T. Prvky U, které nejsou nad T algebraické, se nazývají *transcendentní.* Těleso T je *algebraicky uzavřené*, pokud nemá vlastní algebraické rozšíření. Řekneme-li, že U je algebraický uzávěr T, míníme tím, že U je algebraicky uzavřené algebraické rozšíření T.

Ať $T \leq U$ jsou tělesa a ať $a \in T[x]$. Je-li $U = T(\alpha)$ pro nějaký kořen α polynomu a, nazveme U *kořenovým nadtělesem* T. Je-li $U = T(\alpha_1, \ldots, \alpha_k)$, kde $\alpha_1, \ldots, \alpha_k \in U$ jsou kořeny a, přičemž a se v $U[x]$ rozkládá na lineární činitele, nazývá se U *rozkladové nadtěleso* T.

Je-li $f\colon S \cong T$ isomorfismus těles, přičemž $S \leq U$ a $T \leq V$ jsou taková, že $U = S(\alpha)$, $V = T(\beta)$, kde α je kořen ireducibilního polynomu $a \in S[x]$ a β je kořen $f_x(a) \in T[x]$, tak existuje jediný isomorfismus $g\colon U \cong V$, který rozšiřuje f a zobrazí α na β.

Uvedené tvrzení o jednoznačnosti kořenových nadtěles ireducibilních polynomů se často uvádí ve tvaru, kdy U a V jsou kořenová nadtělesa téhož polynomu $a \in T[x]$, přičemž se dokazuje existence T-isomorfismu $U \cong V$. Rozdíl je pouze v tom, zda se ztotožnění S a T popisuje pomocí isomorfismu f, nebo zda se předpokládá explicitní shoda obou těles. Přecházení mezi oběma způsoby vyjádření by na této úrovni již nemělo činit potíže. Pro jistotu zopakujme, že homomorfismus těles $f\colon U \to V$ se nazývá *T-homomorfismus*, pokud U i V jsou rozšíření tělesa T, přičemž $f(t) = t$ pro každé $t \in T$.

Z jednoznačnosti kořenových nadtěles snadno vyplývá i jednoznačnost rozkladových nadtěles. To znamená, že pro každá dvě rozkladová nadtělesa U a V polynomu $a \in T[x]$ existuje T-isomorfismus $g\colon U \cong V$. Toto tvrzení se často doplňuje připomínkou, že g převádí kořeny v U na kořeny ve V, a to včetně jejich četnosti. Stojí za to si uvědomit, že tento dodatek přímo vyplývá z toho, že $g_x\colon U[x] \cong V[x]$ je isomorfismus, jenž je na $T[x]$ identitou (isomorfismy kopírují vztahy dělitelnosti).

Je-li $a \in T[x]$ ireducibilní polynom nad tělesem T, je $aT[x]$ maximální ideál okruhu $T[x]$, takže $T[x]/aT[x]$ je těleso. Přitom $t \mapsto t + aT[x]$ poskytuje ztotožnění T s podtělesem takto zkonstruovaného tělesa a $x + aT[x]$ je pak kořenem polynomu $a \in T[x]$. Tuto konstrukci lze provést opakovaně, z čehož vyplývá existence rozkladových nadtěles. Pokud souběžně provedeme konstrukci rozkladového nadtělesa pro všechna ireducibilní $a \in T[x]$, získáme těleso algebraicky uzavřené. Souběžnou konstrukci však nelze provést konstruktivně, takže ke konstrukci algebraicky uzavřených těles používáme Zornovo lemma. Jednoznačnost (T-isomorfismus) dvou algebraických uzávěrů tělesa T snadno vyjde ze spojení Zornova lemmatu a jednoznačnosti rozkladových nadtěles.

Důležité je, že každý homomorfismus $f\colon U \to V$, kde U a V jsou podtělesa algebraicky uzavřeného tělesa K (které je algebraické jak nad U, tak nad V), lze rozšířit na automorfismus tělesa K. Veškeré úvahy o T-homomorfismech algebraických rozšíření tělesa T lze proto konat uvnitř nějakého algebraického uzávěru K tělesa T.

Za známou budeme rovněž považovat strukturu konečných těles jakožto rozkladových těles polynomů $x^{p^k} - x$. Konečné těleso řádu p^k budeme značit $\mathbb{F}_{p^k}$. Multiplikativní struktura konečných těles je dána skutečností, že každá konečná podgrupa G multiplikativní grupy T^* tělesa T je cyklická.

Předpokládáme také znalost struktury podílových těles oborů integrity, znalost derivace polynomu a a souvislost derivace s přítomností vícenásobných kořenů.

II.2 Stupeň separability a separabilní rozšíření

II.2.1 Lemma. *Ať $T \leq U \leq V \leq K$ jsou algebraická rozšíření těles, přičemž K je algebraicky uzavřené. Ať Ψ je množina všech U-homomorfismů V do K a Φ je množina všech T-homomorfismů U do K. Pro každé $\varphi \in \Phi$ uvažme právě jeden T-automorfismus $\bar{\varphi}$ tělesa K, který rozšiřuje φ. Potom $\{\bar{\varphi}\psi;\ \varphi \in \Phi \quad \text{a} \quad \psi \in \Psi\}$ je rovno množině všech T-homomorfismů V do K. Jsou-li φ_1, $\varphi_2 \in \Phi$ a ψ_1, $\psi_2 \in \Psi$, tak z $\bar{\varphi_1}\psi_1 = \bar{\varphi_2}\psi_2$ plyne $\varphi_1 = \varphi_2$ a $\psi_1 = \psi_2$.*

Důkaz. Ať $\rho: V \to K$ je T-homomorfismus. Označme φ jeho zúžení na $U \to K$. Pak φ padne do Φ a $\psi = \bar{\varphi}^{-1}\rho$ je U-homomorfismus $V \to K$, tedy $\psi \in \Psi$. Z $\bar{\varphi_1}\psi_1 = \bar{\varphi_2}\psi_2$ plyne, že pro každé $u \in U$ je $\varphi_1(u) = \bar{\varphi_1}(u) = \bar{\varphi_1}\psi_1(u) = \varphi_2(u)$, takže i $\bar{\varphi_1} = \bar{\varphi_2}$ a $\psi_1 = \psi_2$. □

Ať $T \leq U$ je algebraické rozšíření těles a ať K je nějaký algebraický uzávěr U. Z univerzálních vlastností algebraického uzávěru plyne, že struktura T-homomorfismů $U \to K$ nezávisí na volbě K. Speciálně na volbě K nezávisí mohutnost (počet) takových T-homomorfismů. Tuto mohutnost nazýváme *stupeň separability* U nad T. Z lemmatu II.2.1 okamžitě plyne

II.2.2 Důsledek. *Ať $T \leq U \leq V$ jsou algebraická rozšíření těles. Stupeň separability V nad T je roven součinu stupně separability V nad U se stupněm separability U nad T.* □

Je-li $U = T(\alpha_1, \ldots, \alpha_k)$ a $U \leq K$, tak je každý T-homomorfismus $f: U \to K$ určen svými hodnotami na α_1, …, α_k. Jsou-li tyto prvky kořeny nějakého polynomu $a \in T[x]$, tak jsou $f(\alpha_1)$, …, $f(\alpha_k)$ rovněž kořeny polynomu a. Z tohoto faktu plyne řada důsledků. Je-li například $U = T(\alpha)$, α algebraický nad T, K algebraický uzávěr U, a minimální polynom α, je počet T-homomorfismů $U \to K$ omezen počtem kořenů a v K. Naše úvahy vedou k

II.2.3 Lemma. *Ať $T \leq U$ poskytuje rozšíření konečného stupně a ať s je jeho stupeň separability. Potom je $s \leq [U : T]$. Je-li navíc $\alpha \in U$ takové, že jeho minimální polynom a je stupně n a má v algebraickém uzávěru právě k kořenů, tak platí $s \leq [U : T]k/n$.*

Důkaz. Je-li $U = T(\beta)$ pro nějaké β, tak je $s \leq [U : T]$ dle úvah výše. Vztah $s \leq [U : T]$ lze tudíž dokázat indukcí dle $[U : T]$ pomocí důsledku II.2.2. Stupeň separability $T(\alpha)$ nad T je roven k, takže podle důsledku II.2.2 a prvé části tvrzení máme $s \leq k[U : T(\alpha)]$. Proto stačí uvážit, že $[U : T] = [U : T(\alpha)][T(\alpha) : T]$ a $[T(\alpha) : T] = n$. □

Buď T těleso. Polynom $a \in T[x]$ se nazývá *separabilní*, jestliže v algebraickém uzávěru T nemá vícenásobné kořeny. Je-li $T \leq U$, tak se prvek $\alpha \in U$ nazývá *separabilní*, jestliže α je kořenem nějakého separabilního polynomu $a \in T[x]$ (což nastane právě když minimální polynom α je separabilní). Rozšíření U tělesa T se nazývá *separabilní*, je-li každý prvek $\alpha \in U$ separabilní.

II.2.4 Tvrzení. *Ať $T \leq U$ je rozšíření těles konečného stupně. Pak je ekvivalentní*

(i) $U = T[\alpha_1, \ldots, \alpha_k]$ pro $\alpha_1, \ldots, \alpha_k \in U$ separabilní;

(ii) stupeň separability U nad T je roven $[U : T]$; a

(iii) U je separabilní rozšíření T.

Důkaz. Pro $U = T(\alpha)$ je stupeň separability roven počtu kořenů m_α. Proto (ii) plyne z (i) indukcí dle stupně $[U : T]$. Podobně (iii) plyne z (ii), neboť existence neseparabilního prvku stupeň separability snižuje, dle lemmatu lemma II.2.3. Implikace (iii) $\Rightarrow$ (i) je triviální. $\square$

Adjunkcí separabilního prvku tedy vždy dostaneme separabilní rozšíření. Indukcí nahlédneme, že adjunkcí konečného počtu separabilních prvků rovněž obdržíme separabilní rozšíření. Připomeňme si známý induktivní princip:

II.2.5 Lemma. *Ať jsou $T \leq U$ tělesa a ať $U = T(M)$ pro nějaké $M \subseteq U$. Pak pro každé $\alpha \in U$ existuje konečná množina $M_\alpha \subseteq M$ taková, že $\alpha \in T(M_\alpha)$.* $\square$

Nyní je již patrné, že všechny prvky $\alpha \in U$ separabilní nad T, kde $T \subseteq U$, tvoří podtěleso U. Říká se mu *separabilní uzávěr T* v U.

II.2.6 Tvrzení. *Ať $T \leq U \leq V$ jsou taková tělesa, že je U separabilní nad T a V separabilní nad U. Potom je V separabilní nad T.*

Důkaz. Uvažme $\alpha \in V$ a ať M je množina koeficientů separabilního polynomu $a \in U[x]$, jehož kořenem je α. Položme $U_1 = T(M)$ a $V_1 = U_1(\alpha)$. Pak $T \leq U_1 \leq V_1$ poskytuje rozšíření konečného stupně, přičemž separabilita V_1 nad T plyne z tvrzení II.2.4 a důsledku II.2.2. $\square$

II.2.7 Tvrzení. *Ať T je těleso a ať $a \in T[x]$ je ireducibilní polynom, který není separabilní. Potom je T kladné charakteristiky $p > 0$, některý z koeficientů a neleží v obrazu Frobeniova endomorfismu a existuje $b \in T[x]$ takové, že $a(x) = b(x^p)$.*

Důkaz. Polynom a není separabilní, a proto má společný kořen s polynomem $a' \in T[x]$. Je-li $a' \neq 0$, je $\mathrm{NSD}(a, a')$ vlastním dělitelem a, což je ve sporu s ireducibilitou a. Proto je $a' = 0$, odkud zřejmým způsobem plyne, že $a(x) = b(x^p)$, kde $p > 0$ je charakteristika T. Množina koeficientů a i b se shoduje. Pokud $b = \sum b_i x^i$, kde $b_i = c_i^p$ pro každé $i \geq 0$, tak $b(x^p) = (\sum c_i x^i)^p$, což je opět ve sporu s ireducibilitou. Důkaz je u konce. $\square$

Těleso T se nazývá *perfektní* má-li buď charakteristiku nula, nebo má-li charakteristiku $p > 0$ a Frobeniův endomorfismus je automorfismem.

Je patrné, že konečná tělesa jsou perfektní, a že perfektní jsou i tělesa algebraicky uzavřená.

Z tvrzení II.2.7 okamžitě plyne:

II.2.8 Důsledek. *Každé algebraické rozšíření perfektního tělesa je rozšíření separabilní.* □

Ať $T \leq U$ jsou tělesa. O prvku $\alpha \in U$ řekneme, že je *antiseparabilní*, pokud je algebraický a $T(\alpha)$ má nad T stupeň separability 1. Pojmy separability a antiseparability vykazují strukturní příbuznost. Například všechny antiseparabilní prvky tvoří podtěleso U (takzvaný *antiseparabilní uzávěr*). Antiseparabilními prvky se však zde zabývat nebudeme.

II.3 Jednoduchá, normální a Galoisova rozšíření

Rozšíření U tělesa T se nazývá *jednoduché*, jestliže $U = T(\alpha)$ pro nějaký prvek $\alpha \in U$, který je nad T algebraický.

Pro algebraické rozšíření U tělesa T označuje $\mathrm{Gal}(U,T)$ grupu všech T-automorfismů $U \to U$. Říká se jí *Galoisova grupa* U *nad* T. Je-li G podgrupa $\mathrm{Aut}(U)$, tak je $\mathrm{Fix}(U,G) = \{u \in U;\ g(u) = u \text{ pro každé } g \in G\}$ podtělesem U. V další kapitole ukážeme, že za určitých okolností panuje, pro dané U, jednoznačný vztah mezi grupami $\mathrm{Gal}(U,V)$, $T \subseteq V \subseteq U$, a tělesy $\mathrm{Fix}(U,G)$, $G \leq \mathrm{Gal}(U,T)$.

II.3.1 Věta. *Každé separabilní rozšíření těles konečného stupně je jednoduché.*

Důkaz. Ať U je konečným separabilním rozšířením tělesa T. Je-li T konečné těleso, je i U konečné těleso, takže věta plyne z cykličnosti U^*. Ať je tedy T nekonečné. Předpokládejme, že $\alpha \in U$ je zvoleno tak, aby $[T(\alpha) : T]$ bylo maximální možné, a že je $\beta \in U \setminus T(\alpha)$. Položíme $V = T(\alpha, \beta)$ a dokážeme, že V je jednoduché rozšíření T (tím bude dosaženo sporu s maximalitou $[T(\alpha) : T]$). Ať je K nějaký algebraický uzávěr V a ať $f_1, \ldots, f_n$ jsou všechny T-homomorfismy $V \to K$. Ze separability V plyne, že $n = [V : T] > [T(\alpha) : T]$. Je-li $1 \leq i < j \leq n$, tak je $f_i(\alpha) \neq f_j(\alpha)$ nebo $f_i(\beta) \neq f_j(\beta)$, neboť f_i i f_j jsou plně určeny obrazy α a β. Nalezneme-li $t \in T$ takové, že pro $1 \leq i < j \leq n$ je vždy $f_i(\alpha + t\beta) \neq f_j(\alpha + t\beta)$, bude důkaz u konce, neboť stupeň separability $T(\alpha + t\beta)$ bude $\geq n$, odkud $T(\alpha + t\beta) = V$. Požadované nerovnosti lze zapsat jako $\prod_{i<j}((f_j(\alpha) - f_i(\alpha)) + t(f_j(\beta) - f_i(\beta)) \neq 0$. Nahradíme-li t proměnnou x, dostaneme nenulový polynom z $U[x]$. Označme ho například b. Protože T je nekonečné, musí existovat $t \in T$ takové, že je $b(t) \neq 0$. □

II.3.2 Věta. *Ať je* U *těleso a ať je* $G \leq \mathrm{Aut}(U)$ *grupa konečného řádu* n. *Položme* $T = \mathrm{Fix}(U,G)$. *Potom je* U *separabilní rozšíření* T *stupně* n *a* $G = \mathrm{Gal}(U,T)$.

Důkaz. Uvažme $\alpha \in U$ a množinu $G(\alpha)$ všech jeho obrazů automorfismy z G (tedy orbitu α při působení G na U). Protože G obsahuje identitu, je $\alpha \in G(\alpha)$. Položme $b_\alpha = \prod_{\beta \in G(\alpha)}(x - \beta)$. Pro každé $g \in G$ je $g(G(\alpha)) = G(\alpha)$, takže $g_x(b_\alpha) = \prod(x - g(\beta)) = \prod(x - \beta) = b_\alpha$, odkud $b_\alpha \in T[x]$. Polynom b_α je separabilní, takže U je separabilní rozšíření T.

Ukážeme, že jde o rozšíření konečného stupně. Kdyby tomu tak nebylo, ležela by v U konečná rozšíření T stupně přesahujícího jakoukoliv zadanou mez. Ať $V \subseteq U$ je konečné rozšíření T, které je stupně $k > n$. Podle věty II.3.1 je V možné pro nějaké $\gamma \in V$ vyjádřit jako $T(\gamma)$. Minimální polynom γ nad T by dělil polynom b_γ, který je stupně n, a sám by byl stupně k. To není možné, a proto je stupeň U nad T konečný.

Podle věty II.3.1 existuje $\alpha \in U$, že $U = T(\alpha)$. Ať $b = b_\alpha$ a ať $a \in T[x]$ je minimální polynom prvku α. Pak $\mathrm{st}(a) = n \geq |G(\alpha)| = \mathrm{st}(b) \geq \mathrm{st}(a)$. Vidíme, že $a = b$. Počet T-homomorfismů tělesa U do algebraického uzávěru K je roven n, z čehož vyplývá, že každý se shoduje s nějakým $g \in G$. Proto musí být $G = \mathrm{Gal}(U, T)$. □

Uvažme tělesa $T \leq U \leq K$, kde K je algebraický uzávěr U. O U řekneme, že je *normální rozšíření* T, je-li to takové algebraické rozšíření, že pro každý T-homomorfismus $f : U \to K$ platí $f(U) = U$. (Jinak řečeno, každý takový homomorfismus se shoduje s T-automorfismem U.)

Normální separabilní rozšíření konečného stupně se nazývá *Galoisovo.*

II.3.3 Tvrzení. *Rozkladová nadtělesa polynomů jsou normální. Rozkladová nadtělesa separabilních polynomů jsou Galoisova.*

Důkaz. Ať $U \geq T$ je rozkladové nadtěleso polynomu $a \in T[x]$ a ať K je algebraický uzávěr U. Označme M množinu všech kořenů a. Pak každý T-homomorfismus $f : U \to K$ permutuje M, takže $f(M) = M$, a odsud $f(U) = U$. Je-li a separabilní, jsou jeho kořeny separabilní prvky a U je separabilní dle tvrzení II.2.4. □

II.3.4 Tvrzení. *Každé Galoisovo rozšíření* $U \geq T$ *je rozkladovým nadtělesem nějakého separabilního polynomu. Tento polynom lze vždy volit ireducibilní.*

Důkaz. Podle věty II.3.1 máme $U = T(\alpha)$ pro nějaký separabilní prvek α. Ať je a jeho minimální polynom. Pak $[U : T]$ je rovno stupni a, přičemž a má vesměs různé kořeny. Je-li β takový kořen, $\beta \in K$, kde K je algebraický uzávěr U, pak existuje T-homomorfismus $f : T(\alpha) \to T(\beta)$, $f(\alpha) = \beta$. Z normality U plyne $T(\beta) = U$, a tedy $\beta \in U$. □

Podobně jako se definuje rozkladové nadtěleso polynomu $a \in T[x]$, lze definovat *rozkladové nadtěleso množiny polynomů* $\mathcal{M} \subseteq T[x]$. Přitom $U \geq T$ je takovým nadtělesem právě když každý $a \in \mathcal{M}$ se v U rozkládá na kořenové činitele a současně $U = T[M]$, kde M je množina všech kořenů všech polynomů z $\mathcal{M}$.

II.3.5 Tvrzení. *Rozšíření těles* $U \geq T$ *je normální právě když existuje množina polynomů* $\mathcal{M} \subseteq T[x]$ *taková, že* U *je rozkladovým nadtělesem* $\mathcal{M}$.

Důkaz. Ať je K algebraický uzávěr U. Předpokládejme nejprve, že je U normální rozšíření T. Pro každé $\alpha \in U$ uvažme minimální polynom $a \in T[x]$. Kdyby se a nerozkládalo v U na kořenové činitele, bylo by možné sestrojit T-homomorfismus $f{:}T(\alpha)\to T(\beta)$, kde $\beta \in U \setminus T$. Protože takový homomorfismus lze rozšířit na T-homomorfiusmus $g : U \to K$, $g(\alpha) = \beta$, dostali bychom spor s normalitou. Vidíme, že za $\mathcal{M}$ lze zvolit množinu všech minimálních polynomů prvků α, kde α probíhá U.

Ať je naopak U rozkladové nadtěleso $\mathcal{M}$. Uvažme T-homomorfismus $f{:}U\to K$ a označme M množinu všech kořenů všech polynomů $a \in \mathcal{M}$. Přitom $M = \bigcup\{M_a; a \in \mathcal{M}\}$, kde M_a je množina všech kořenů polynomu a. Je třeba ukázat $f(M) = M$. To ovšem okamžitě vyplývá z $f(M_a) = M_a$, což pro každé $a \in \mathcal{M}$ zjevně platí. □

II.3.6 Tvrzení. *Ať je $T \le U$ rozšíření a ať V se skládá ze všech $\alpha \in U$, která jsou algebraická nad T a jejichž minimální polynomy se nad U rozkládají na kořenové činitele. Potom je V podtěleso U, které je největším normálním rozšířením T, jež je obsažené v U.*

Důkaz. Položme $V_1 = T(V)$ a ať $\mathcal{M} \subset T[x]$ je množina všech minimálních polynomů $a \in T[x]$ takových prvků $\alpha \in U$, že a se v $U[x]$ rozkládá na kořenové činitele. Pak V se shoduje s množinou kořenů polynomů $a \in \mathcal{M}$, takže V_1 je normální podle tvrzení II.3.5. Je-li $\beta \in V_1$ a $b \in T[x]$ je minimální polynom β, tak z normality V_1 vyplývá, že b se nad V_1 rozkládá na kořenové činitele. Proto je $\beta \in V$, takže $V_1 = V$. Dokázali jsme, že V je normální rozšíření T. Je-li $W \ge T$ jiné normální rozšíření a $W \le U$, tak jistě každý prvek $\alpha \in W$ poskytuje minimální polynom $a \in T[x]$, který se v $W[x]$ rozkládá na kořenové činitele. Proto $\alpha \in V$, odkud $W \le V$. □

Těleso V popsané v tvrzení II.3.6 se nazývá *normální uzávěr T v U*. Následující tvrzení se týká libovolného rozšíření $T \le U$.

II.3.7 Tvrzení. *Ať U je těleso.*

(i) *Pro $T \le U$ je* $\mathrm{Fix}(U, \mathrm{Gal}(U, T)) \ge T$.

(ii) *Pro $G \le \mathrm{Aut}(U)$ je* $\mathrm{Gal}(U, \mathrm{Fix}(U, G)) \ge G$.

Důkaz. Je-li $t \in T$ a $f \in \mathrm{Gal}(U, T)$, tak $f(t) = t$. Je-li $g \in G$ a $u \in \mathrm{Fix}(U, G)$, je $g(u) = u$. □

Ve větě II.3.2 jsme nahlédli, že v případě konečné grupy G dokonce máme $\mathrm{Gal}(U, \mathrm{Fix}(U, G)) = G$. Podobnou rovnost dostáváme i v části (i) předchozího tvrzení v případě, že U je Galoisovo rozšíření T.

II.3.8 Věta. *Ať je U Galoisovo rozšíření T. Potom* $\mathrm{Fix}(U, \mathrm{Gal}(U, T)) = T$.

Důkaz. Položme $S = \mathrm{Fix}(U, \mathrm{Gal}(U, T))$. Podle II.3.7(i) je $S \ge T$, takže stačí ukázat $[U : S] = [U : T]$. Podle věty II.3.2 je U separabilní rozšíření S stupně $n = |\mathrm{Gal}(U, T)|$. Protože U je normální a separabilní rozšíření T, platí $|U : T| = |\mathrm{Gal}(U, T)| = n$. □

V této kapitole jsme dokázali většinu skutečností potřebných pro formulaci hlavní věty Galoisovy teorie. Ještě připojíme jedno snadné pozorování, které rovněž použijeme.

II.3.9 Lemma. *Ať je U těleso a ať je $G \leq \mathrm{Aut}(U)$. Potom pro každé $f \in \mathrm{Aut}(U)$ máme $\mathrm{Fix}(U, fGf^{-1}) = f(\mathrm{Fix}(U, G))$.*

Důkaz. Pro $u \in \mathrm{Fix}(U, G)$ a $g \in G$ máme $(fgf^{-1})(f(u)) = fg(u) = f(u)$, takže $f(\mathrm{Fix}(U, G)) \leq \mathrm{Fix}(U, fGf^{-1})$. Tatáž nerovnost použitá pro fGf^{-1} a f^{-1} dává $f^{-1}(\mathrm{Fix}(U, fGf^{-1})) \leq \mathrm{Fix}(U, f^{-1}(fGf^{-1})f) = \mathrm{Fix}(U, G)$, tedy $\mathrm{Fix}(U, fGf^{-1}) \leq f(\mathrm{Fix}(U, G))$. □

II.4 Galoisova korespondence

Uvažme uspořádané množiny $(A, \leq)$ a $(B, \leq)$ a zobrazení $\alpha{:}A \to B$ a $\beta{:}B \to A$, jež jsou *antimonotonní* (pro $a_1, a_2 \in A$ z $a_1 \leq a_2$ plyne $\alpha(a_1) \geq \alpha(a_2)$, a pro $b_1, b_2 \in B$ z $b_1 \leq b_2$ plyne $\beta(b_1) \geq \beta(b_2)$) a jež pro všechna $a \in A$ a $b \in B$ splňují $\beta\alpha(a) \geq a$, $\alpha\beta(b) \geq b$. Dvojici (α, β) těchto vlastností nazveme *Galoisovou korespondencí* uspořádaných množin $(A, \leq)$ a $(B, \leq)$. (Přitom uspořádáním zde rozumíme částečné uspořádání.)

Uveďme základní obecné vlastnosti Galoisovy korespondence.

II.4.1 Lemma. *Zobrazení α a β poskytují vzájemně inverzní bijekce množin $\mathrm{Im}(\beta)$ a $\mathrm{Im}(\alpha)$.*

Důkaz. Pro $a \in A$ máme $\beta\alpha(a) \geq a$, odkud $\alpha\beta\alpha(a) \leq \alpha(a)$. Současně $\alpha\beta(\alpha(a)) \geq \alpha(a)$, neboť $\alpha(a) \in B$. Je tedy $\alpha\beta\alpha(a) = \alpha(a)$ pro každé $a \in A$, a podobně $\beta\alpha\beta(b) = b$ pro každé $b \in B$. □

II.4.2 Důsledek. *Jsou-li α a β surjektivní, jsou α i β bijektivní zobrazení. Pokud jsou $(A, \leq)$ a $(B, \leq)$ v takovém případě svazy, tak jsou α a β vzájemně inverzní antiisomorfismy těchto svazů.* □

Ať U je rozšíření tělesa T. Budeme-li chápat A jako množinu všech mezitěles V, $T \leq V \leq U$, a B jako množinu všech podgrup $\mathrm{Gal}(U, T)$, dostáváme podle tvrzení II.3.7 Galoisovu korespondenci, jestliže položíme $\alpha(V) = \mathrm{Gal}(U, V)$ a $\beta(H) = \mathrm{Fix}(U, H)$. Základní věta Galoisovy teorie se vztahuje k této situaci v případě, že U je Galoisovo rozšíření T.

II.4.3 Věta. *Ať U je Galoisovo rozšíření tělesa T. Potom zobrazení $V \mapsto \mathrm{Gal}(U, V)$ a $H \mapsto \mathrm{Fix}(U, H)$ jsou antiisomorfismy svazu všech mezitěles V, $T \leq V \leq U$, a svazu všech podgrup grupy $\mathrm{Gal}(U, T)$. V tomto antiisomorfismu odpovídají normální rozšíření T normálním podgrupám $\mathrm{Gal}(U, T)$.*

Důkaz. Podle úvah předcházejících dokazované tvrzení skutečně běží o Galoisovu korespondenci. Podle věty II.3.2 je každá podgrupa $\mathrm{Gal}(U, T)$ Galoisovou grupou nějakého mezitělesa, a podobně z věty II.3.8 vyplývá, že každé mezitěleso se shoduje s pevnými body nějaké podgrupy. Zbývá dokázat část o normalitě.

Je-li $V \leq U$ takové, že V je nad T normální, tak pro každé $g \in \mathrm{Gal}(U,T)$ máme $g(V) = V$. Pro $h \in \mathrm{Gal}(U,V)$ potom pro každé $v \in V$ platí $g^{-1}(v) \in V$, $hg^{-1}(v) = g^{-1}(v)$ a tedy $ghg^{-1}(v) = v$. Odsud $\mathrm{Gal}(U,V) \trianglelefteq \mathrm{Gal}(U,T)$.

Naopak, je-li $H \trianglelefteq \mathrm{Gal}(U,T)$ a $f \in \mathrm{Gal}(U,T)$, tak podle lemmatu II.3.9 máme $\mathrm{Fix}(U,H) = \mathrm{Fix}(U,fHf^{-1}) = f(\mathrm{Fix}(U,H))$. To znamená, že každé $f \in \mathrm{Gal}(U,T)$ zobrazí $\mathrm{Fix}(U,H)$ na $\mathrm{Fix}(U,H)$. Z normality U nad T tím pádem vyplývá i normalita $\mathrm{Fix}(U,H)$ nad T. $\square$

II.5 Stopa, norma, diskriminant

Uvažme nyní rozšíření U tělesa T, které je konečného stupně n. Je-li $e = (e_1,\ldots,e_n)$ nějaká báze U, kde U chápeme jako vektorový prostor nad T, přísluší každému $\alpha \in U$ matice $M_e(\alpha)$, jež vyjadřuje násobení $u \mapsto \alpha u$ chápané jako lineární zobrazení vektorového prostoru U. Máme tedy $M_e(\alpha) = (a_{ij})$, kde pro každé j, $1 \leq j \leq n$, je $\alpha e_j = \sum_i a_{ij} e_i$.

Determinant $M_e(\alpha)$ je nezávislý na volbě báze e. Nazývá se *normou* α v U nad T, a značí se $N_{U|T}(\alpha)$. Podobně i stopa $M_e(\alpha)$ (součet prvků na diagonále), je nezávislá na volbě báze. Mluvíme o *stopě* α v U nad T; značíme $\mathrm{Tr}_{U|T}(\alpha)$.

Nezávislost stopy a determinantu na volbě báze je možno objasnit také z nezávislosti charakteristického polynomu lineárního zobrazení. Na volbě báze e totiž nezávisí $\det(xI_n - M_e(\alpha))$, kde x je proměnná a I_n jednotková diagonální matice. Determinant poskytuje monický polynom stupně n, řekněme $\sum a_i x^i$. Nazývá se *charakteristický polynom* α v U nad T. Přitom stopa odpovídá koeficientu u x^{n-1}, čili $a_{n-1} = -\mathrm{Tr}_{U|T}(\alpha)$. Podobně norma odpovídá absolutnímu členu charakteristického polynomu, neboť ten je roven $\det(-M_e(\alpha)) = (-1)^n \det(M_e(\alpha))$. Je tedy $a_0 = (-1)^n \mathrm{N}_{U|T}(\alpha)$.

Hledejme nyní souvislosti charakteristického a minimálního polynomu. V případě, že $U = T(\alpha)$, můžeme uvažovat bázi 1, α, $\ldots$, α^{n-1}. Je-li $a = \sum a_i x^i$ minimální polynom, tak $\alpha\alpha^{n-1} = -a_{n-1}\alpha^{n-1} - a_{n-2}\alpha^{n-2} - \cdots - a_1\alpha - a_0$, takže pro výpočet charakteristického polynomu je třeba uvážit matici

$$\begin{pmatrix} x & 0 & \cdots & 0 & a_0 \\ -1 & x & \cdots & 0 & a_1 \\ 0 & -1 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & x & a_{n-2} \\ 0 & 0 & \cdots & -1 & x + a_{n-1} \end{pmatrix}$$

Označíme-li její determinant $\mathrm{d}(a_0,\ldots,a_{n-1})$, vidíme, že rozvojem dostáváme pro $n > 1$ vztah $\mathrm{d}(a_0,\ldots,a_{n-1}) = x\mathrm{d}(a_1,\ldots,a_{n-1}) + (-1)^{n-1}(-1)^{n-1}a_0 = a_0 + x\mathrm{d}(a_1,\ldots,a_{n-1})$. Protože případ $n = 1$ dává $\mathrm{d}(a_{n-1}) = x + a_{n-1}$, indukcí lehce ověříme $\mathrm{d}(a_0,\ldots,a_{n-1}) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Dokázali jsme, že charakteristický a minimální polynom se v případě $U = T(\alpha)$ rovnají.

V případě, kdy $[T(\alpha) : T] = k < n$, můžeme uvážit bázi s prvky tvaru $e_j\alpha^i$, kde $0 \leq i < k$, $1 \leq j \leq d$, $d = [U : T(\alpha)]$. Z $\alpha(e_j\alpha^i) = e_j\alpha^{i+1}$ vyplývá, že matice

$xI_n - M_e(\alpha)$ je složena z d matic výše uvedeného tvaru, které jsou umístěny na diagonále. Můžeme tedy vyslovit

II.5.1 Tvrzení. *Ať je $T \leq U$ rozšíření konečného stupně n a ať je $\alpha \in U$ prvek s minimálním polynomem $a = \sum a_i x^i$ a charakteristickým polynomem $c = \sum c_i x^i$. Potom $c = a^d$, kde $d = [U : T(\alpha)]$. Dále $\mathrm{N}_{U|T}(\alpha) = (-1)^n c_0 = (-1)^n a_0^d = (\mathrm{N}_{T(\alpha)|T}(\alpha))^d$ a $\mathrm{Tr}_{U|T}(\alpha) = -c_{n-1} = d\ \mathrm{Tr}_{T(\alpha)|T}(\alpha)$.* □

Jestliže U je algebraické rozšíření tělesa T a $a \in T[x]$ je minimální polynom prvku $\alpha \in U$, tak každý kořen a v algebraickém uzávěru $\bar{U}$ tělesa U je možné vyjádřit jako $g(\alpha)$, kde $g \in \mathrm{Hom}_T(T(\alpha), \bar{U})$. Předpokládejme $[U : T(\alpha)] = d$ a ať je U separabilní rozšíření T. Potom existuje, podle tvrzení II.2.2, pro každý kořen β polynomu a právě d homomorfismů $g \in \mathrm{Hom}_T(U, \bar{U})$ takových, že $g(\alpha) = \beta$. Vidíme, že $a^d = \prod(x - g(\alpha))$, kde g probíhá $\mathrm{Hom}_T(U, \bar{U})$. Spojením s tvrzením II.5.1 tudíž dostáváme:

II.5.2 Tvrzení. *Ať $U \geq T$ je separabilní rozšíření tělesa a ať $c \in T[x]$ je charakteristický polynom prvku $\alpha \in U$. Pak $c = \prod(x - g(\alpha))$, $\mathrm{N}_{U|T}(\alpha) = \prod g(\alpha)$ a $\mathrm{Tr}_{U|T}(\alpha) = \sum g(\alpha)$, kde g probíhá všechny T-homomorfismy $U \to \bar{U}$, $\bar{U}$ algebraický uzávěr U.* □

Determinant součinu dvou matic je součin jejich determinantů, stopa součtu dvou matic je součet jejich stop. Proto je $\mathrm{N}_{U|T}$ grupovým homomorfismem $U^* \to T^*$ a $\mathrm{Tr}_{U|T}$ grupovým homomorfismem $U(+) \to T(+)$. Jejich skládáním v případě vložených těles $T \leq U \leq V$ získáváme opět normy a stopy, což dokážeme nyní pro separabilní rozšíření. (Tvrzení platí i pro neseparabilní rozšíření. Důkaz není těžký, ale vyžaduje popis antiseparabilních rozšíření, který jsme pominuli.)

II.5.3 Tvrzení. *Ať $T \leq U \leq V$ je věž konečných separabilních rozšíření. Pak $\mathrm{Tr}_{V|T} = \mathrm{Tr}_{U|T}\,\mathrm{Tr}_{V|U}$ a $\mathrm{N}_{V|T} = \mathrm{N}_{U|T}\mathrm{N}_{V|U}$.*

Důkaz. Prvky $\mathrm{Hom}_T(V, \bar{V})$ vyjádříme jako v tvrzení II.2.1 složeními $\bar{f}g$, kde $f \in \mathrm{Hom}_T(U, \bar{V})$, $g \in \mathrm{Hom}_U(V, \bar{V})$ a $\bar{f}$ je nějaké pevně dané rozšíření f do $\mathrm{Aut}_T(\bar{V}, \bar{V})$. Pak $\sum \bar{f}g = \sum_f \bar{f}(\sum_g g) = \sum_f(\bar{f}\,\mathrm{Tr}_{V|U}) = \sum_f(f\,\mathrm{Tr}_{V|U}) = \mathrm{Tr}_{U|T}\,\mathrm{Tr}_{V|U}$, a podobně $\prod \bar{f}g = \prod_f \bar{f}(\prod_g g) = \prod_f(f\mathrm{N}_{V|U}) = \mathrm{N}_{U|T}\mathrm{N}_{V|U}$. □

Za zmínku rovněž stojí, že pro $t \in T$ v případě $T \leq U$, $[U : T] = n$, máme $\mathrm{N}_{U|T}(t) = t^n$ a $\mathrm{Tr}_{U|T}(t) = nt$. To vyplývá například z tvrzení II.5.1, neboť t má minimální polynom $x - t$. Pro $\alpha \in U$ je zjevně $\mathrm{Tr}_{U|T}(t\alpha) = t\,\mathrm{Tr}_{U|T}(\alpha)$, takže $\mathrm{Tr}_{U|T}: U \to T$ je možno chápat jako lineární formu nad T.

II.5.4 Lemma. *Nad libovolným tělesem je determinant matice*

$$\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}$$

roven $\prod_{i<j}(\alpha_j - \alpha_i)$.

Důkaz. Jedná se o takzvaný Vandermondův determinant. Označme jeho hodnotu $V(\alpha_1, \ldots, \alpha_n)$. Odečtením α_1-násobku každého sloupce, který není poslední, od sloupce následujícího, dostaneme vztah

$$V(\alpha_1, \ldots, \alpha_n) = (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1) \ldots (\alpha_n - \alpha_1) V(\alpha_2, \ldots, \alpha_n),$$

ze kterého již dokazovaný vztah snadno plyne. $\square$

Ať U je separabilní rozšíření T stupně n. Pro $\alpha_1, \ldots, \alpha_n \in U$ definujeme *diskriminant* $\triangle(\alpha_1, \ldots, \alpha_n)$ jako determinant symetrické matice $(\mathrm{Tr}_{U|T}(\alpha_i \alpha_j))$. Nejčastěji bude $\alpha_1, \ldots, \alpha_n$ bází U nad T. Snadno lze totiž nahlédnout, že diskriminant je roven nule, jsou-li $\alpha_1, \ldots, \alpha_n$ lineárně závislé.

II.5.5 Lemma. *Ať* $\mathrm{Hom}_T(U, \bar{U}) = \{g_1, \ldots, g_n\}$*. Označme M matici $(g_i(\alpha_j))$. Pak $M^{\mathrm{T}} M$ je rovna matici $(\mathrm{Tr}_{U|T}(\alpha_i \alpha_j))$ a $\triangle(\alpha_1, \ldots, \alpha_n) = (\det M)^2$.*

Důkaz. Na pozici (i, j) se v $M^{\mathrm{T}} M$ nachází hodnota $\sum_k g_k(\alpha_i) g_k(\alpha_j)$. Ta je rovna $\sum g_k(\alpha_i \alpha_j) = \mathrm{Tr}_{U|T}(\alpha_i \alpha_j)$, dle tvrzení II.5.2. Zbytek je zřejmý. $\square$

Pokud je U separabilní rozšíření konečného stupně n, lze zvolit bázi $1, \gamma, \ldots, \gamma^{n-1}$, neboť $U = T(\gamma)$ pro nějaké $\gamma \in U$. Matice M z lemmatu II.5.5 má v i-tém řádku $1, g_i(\gamma), (g_i(\gamma))^2, \ldots, (g_i(\gamma))^{n-1}$, takže podle lemmatu II.5.4 je její determinant roven $\prod_{j>i}(g_j(\gamma) - g_i(\gamma))$. Odsud vyplývá, že diskriminant $\triangle(1, \gamma, \ldots, \gamma^{n-1})$ je nenulový.

K přechodu mezi diskriminanty různých bází je dobré si uvědomit, že zobrazení $(\alpha, \beta) \mapsto \mathrm{Tr}_{U|T}(\alpha\beta)$ je symetrickou bilineární formou. Vskutku, fixováním jedné složky zjevně dostáváme lineární formu, a více není třeba.

Je-li h bilineární forma na vektorovém prostoru V a $H = (h(e_i, e_j))$ je její matice vůči bázi $e_1, \ldots, e_n$, tak je matice $(h(b_i, b_j))$ vzhledem k bázi $b_1, \ldots, b_n$ rovna $P^{\mathrm{T}} H P$, kde $P = (p_{ij})$, $b_j = \sum p_{ij} e_i$. Forma h je nedegenerovaná, jestliže determinant její matice je vůči některé bázi (a tím vůči všem bázím) nenulový (matici H je totiž možné chápat jako matici lineárního zobrazení $v \mapsto h(-, v)$ z V do duálního vektorového prostoru).

Můžeme tedy tyto úvahy uzavřít:

II.5.6 Tvrzení. *Ať je $T \leq U$ separabilní rozšíření stupně n. Pak je zobrazení $(\alpha, \beta) \mapsto \mathrm{Tr}_{U|T}(\alpha\beta)$ nedegenerovanou symetrickou bilineární formou $U \times U \to T$. Jsou-li $\alpha_1, \ldots, \alpha_n$ a $\beta_1, \ldots, \beta_n$ dvě báze U nad T, $\beta_j = \sum p_{ij} \alpha_i$ a $P = (p_{ij})$, je $\triangle(\beta_1, \ldots, \beta_n) = (\det P)^2 \triangle(\alpha_1, \ldots, \alpha_n) \neq 0$.* $\square$

II.5.7 Tvrzení. *Ať $U = T(\gamma)$ je separabilní rozšíření T stupně n. Pak $\triangle(1, \gamma, \ldots, \gamma^{n-1})$ lze vyjádřit jednak jako $\prod(g(\gamma) - h(\gamma))^2$, kde g, h probíhají $\mathrm{Hom}_T(U, \bar{U})$, $g \neq h$, jednak jako $(-1)^{\binom{n}{2}} \mathrm{N}_{U|T}(a'(\gamma))$, kde a je minimální polynom γ nad T.*

Důkaz. Ať $g_1, \ldots, g_n$ jsou všechny T-homomorfismy $U \to \bar{U}$. Z úvah za lemmatem II.5.5 víme, že uvažovaný diskriminant je roven $\prod_{j>i}(g_j(\gamma) - g_i(\gamma))^2$. Tuto hodnotu je též možno zapsat jako

$$(-1)^{\binom{n}{2}} \prod_{i \neq j} (g_j(\gamma) - g_i(\gamma)).$$

Z $a = \prod_i (x - g_i(\gamma))$ vyplývá $a'(g_i(\gamma)) = \prod_j (g_i(\gamma) - g_j(\gamma))$, kde $i \neq j$. Proto je $N_{U|T}(a'(\gamma)) = a'(g_1(\gamma)) \dots a'(g_n(\gamma))$ rovno $\prod_{i \neq j} (g_j(\gamma) - g_i(\gamma))$. □

Je-li U rozšíření T stupně n a α_1, …, α_n jsou prvky U, lze diskriminant $\triangle(\alpha_1, \dots, \alpha_n)$ definovat jako determinant matice $(\mathrm{Tr}_{U|T}(\alpha_i \alpha_j))$ bez ohledu na to, zda jde o bázi, či nikoliv. Ovšem v případě, že nejde o bázi, jsou α_1, …, α_n lineárně závislé nad T a dostáváme $\triangle(\alpha_1, \dots, \alpha_n) = 0$ (například z toho, že $(\alpha, \beta) \mapsto \mathrm{Tr}_{U|T}(\alpha\beta)$ je bilineární).

II.6 Algebraická nezávislost a stupeň transcendence

Nechť $T \subseteq U$ jsou do sebe vřazená komutativní tělesa.

II.6.1 Lemma. *Pro každou množinu $M \subseteq U$ platí, že těleso $T(M)$ se skládá právě ze všech prvků $p(\alpha_1, \dots, \alpha_n)/q(\beta_1, \dots, \beta_n)$, $q(\beta_1, \dots, \beta_n) \neq 0$, kde $p, q \in T[x_1, \dots, x_n]$ pro nějaké $n \leq |M|$ a kde $\alpha_i, \beta_i \in M$, $1 \leq i \leq n$.*

Důkaz. Lze postupovat přímo nebo použít toho, že $T(M)$ je obrazem podílového tělesa okruhu $T[M]$. Tento okruh je roven množině všech hodnot $p(\alpha_1, \dots, \alpha_n)$. □

Množinu $M \subseteq U$ nazveme *algebraicky nezávislou* (nad T), jestliže pro žádné po dvou různé $\alpha_1, \dots, \alpha_n \in M$ neexistuje nenulové $p \in T[x_1, \dots, x_n]$ takové, že $p(\alpha_1, \dots, \alpha_n) = 0$.

Prvek $\beta \in U$ nazveme *algebraicky závislý* (nad T) na $M \subseteq U$, jestliže β je nad $T(M)$ algebraický.

II.6.2 Lemma. *Množina $M \subseteq U$ je algebraicky nezávislá právě když pro každé $\beta \in M$ platí, že β není algebraicky závislý na $M \setminus \{\beta\}$.*

Důkaz. Uvažme $\beta \in M$ a předpokládejme, že β je algebraicky závislý na $M' = M \setminus \{\beta\}$. Pak existuje nenulový polynom s koeficienty v $T(M')$, jehož je β kořenem. Každý z těchto koeficientů má podle lemmatu II.6.1 tvar zlomku, jehož čitatel i jmenovatel jsou prvky $T[M']$. Vynásobíme-li polynom součinem jmenovatelů zmíněných zlomků, obdržíme polynom s koeficienty v $T[M']$. Odsud již plyne, že pro vhodné $n \geq 0$ a vhodná po dvou různá $\alpha_1, \dots, \alpha_n \in M'$ existuje $g \in T[x_1, \dots, x_{n+1}]$ takové, že $g(\alpha_1, \dots, \alpha_n, \beta) = 0$, $g \neq 0$.

Je-li naopak možno najít takový polynom, přičemž n je nejmenší možné, bude β algebraický nad $T(M')$. Můžeme předpokládat, že je $\beta \neq 0$ a že g není tvaru $x_{n+1} g_1$, kde $g_1 \in T[x_1, \dots, x_{n+1}]$. Uvažme g jako polynom v x_{n+1} s koeficienty v $T[x_1, \dots, x_n]$. Kdyby každý z těchto koeficientů po dosazení $\alpha_1, \dots, \alpha_n$ dal nulu, musel by každý z těchto koeficientů být roven nule, neboť n je voleno minimální. Pak by bylo $g = 0$, což je spor. Po dosazení $\alpha_1, \dots, \alpha_n$ tedy z g vznikne nenulový polynom nad $T(M')$ s kořenem β. □

Množinu $M_2 \subseteq U$ nazveme *algebraicky závislou* (nad T) na $M_1 \subseteq U$, jestliže každý prvek M_2 je algebraicky závislý na M_1.

II.6.3 Lemma. *Ať jsou M_i podmnožiny U, $1 \leq i \leq 3$. 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.*

Důkaz. Zvolme $\beta \in M_3$. Pak existují $\alpha_1, \ldots, \alpha_k \in M_2$ takové, že β je algebraické nad $T(\alpha_1, \ldots, \alpha_k)$. Stupně $[T(M_1)(\alpha_1, \ldots, \alpha_k) : T(M_1)]$ a $[T(M_1)(\beta, \alpha_1, \ldots, \alpha_k) : T(M_1)(\alpha_1, \ldots, \alpha_k)]$ jsou konečné, a proto je konečný i stupeň $[T(M_1)(\beta) : T(M_1)] \leq [T(M_1)(\beta, \alpha_1, \ldots, \alpha_k) : T(M_1)]$. $\square$

Množiny $M_1, M_2 \subseteq U$ nazveme *algebraicky ekvivalentní* (nad T), jestliže M_2 je algebraicky závislá na M_1 a M_1 je algebraicky závislá na M_2. Z lemmatu II.6.3 vidíme, že vztah být algebraicky ekvivalentní je skutečně ekvivalencí na podmnožinách U.

Všimněme si, že pro $M_1 \subseteq M_2$ vždy platí, že M_1 je algebraicky závislá na M_2.

II.6.4 Lemma. *Pro každé $M \subseteq U$ lze nalézt $M_1 \subseteq M$ algebraicky nezávislé, jež je algebraicky ekvivalentní M. Je-li $M_0 \subseteq M$ množina algebraicky nezávislá, lze M_1 zvolit tak, aby platilo $M_0 \subseteq M_1$.*

Důkaz. Sjednocením řetězce do sebe vřazených algebraicky nezávislých množin získáme opět algebraicky nezávislou množinu. Proto z Zornova lemmatu plyne existence maximální algebraicky nezávislé množiny $M_1 \subseteq M$ (která případně obsahuje M_0). Je-li $\beta \in M \setminus M_1$, tak množina $M_1 \cup \{\beta\}$ již algebraicky nezávislá není. Příslušný polynom negující algebraickou nezávislost množiny $M_1 \cup \{\beta\}$ vyjadřuje i algebraickou závislost β na M_1, neboť M_1 algebraicky nezávislé je. $\square$

Jsou-li M_1 a M_2 algebraicky ekvivalentní podmnožiny U a jsou-li $M_3 \subseteq M_1$ a $M_4 \subseteq M_2$ jejich algebraicky ekvivalentní algebraicky nezávislé podmnožiny, budou M_3 a M_4, jak ukážeme, stejné mohutnosti. Důkaz probíhá podobně jako u vektorových prostorů, přičemž algebraická nezávislost odpovídá lineární nezávislosti. Jeho základem je níže uvedené lemma o výměně.

Úvahy o systémech množin, pro které je definována nezávislost tak, aby platilo lemma o výměně, vedou k teorii matroidů. Tu zde rozvíjet nebudeme; kdybychom tak však učinili, obdrželi bychom řadu důsledků lemmatu o výměně (například stejnou mohutnost algebraicky ekvivalentních algebraicky nezávislých množin) z této teorie přímo.

Na místě je otázka, čemu při korelaci algebraické a lineární nezávislosti odpovídá vektorový prostor. Uvědomme si, že vektorový prostor je největší množina lineárně ekvivalentní své množině generátorů. Největší množina algebraicky ekvivalentní množině $M \subseteq U$ je algebraický uzávěr $T(M)$ v U (podtěleso U složené ze všech prvků algebraických nad $T(M)$). Vektorovým podprostorům tedy odpovídají podtělesa U, jež jsou v U (relativně) algebraicky uzavřená.

II.6.5 Lemma (o výměně). *Ať $M_1 \subseteq U$ je algebraicky nezávislá množina, která je algebraicky závislá na $M_2 \subseteq U$. Ať α je prvek M_1, který není prvkem M_2. Pak existuje $\beta \in M_2 \setminus M_1$ takové, že $(M_2 \setminus \{\beta\}) \cup \{\alpha\}$ je algebraicky ekvivalentní M_2.*

Důkaz. Z lemmatu II.6.4 plyne, že tvrzení stačí dokázat pro případ, kdy je M_2 algebraicky nezávislé. Předpokládejme tak a použijme lemma II.6.2 na množinu $M_2 \cup \{\alpha\}$. Prvek α je na M_2 algebraicky závislý, a proto existují po dvou různá $\beta_1, \dots, \beta_n \in M_2$ taková, že pro nějaké nenulové $g \in T[x_1, \dots, x_{n+1}]$ je $g(\beta_1, \dots, \beta_n, \alpha) = 0$. Zvolme $n \geq 0$ minimální možné a označme g_i verzi g chápanou jako polynom v x_i s koeficienty v $T[x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{n+1}]$. Označme ještě $h_i \in U[x_i]$ ten polynom, který vznikne z g_i dosazením $\beta_1, \dots, \beta_n$ a α do jeho koeficientů (ne však do x_i). Z minimality n a z nezávislosti M_2 vyplývá, že dosazením do nenulového koeficientu g_i dostaneme nenulový koeficient h_i. Ze stejného důvodu máme $\deg g_i > 0$, a proto i $\deg h_i = \deg g_i > 0$. Vidíme, že β_i je algebraicky závislé na $\beta_1, \dots, \beta_{i-1}, \beta_{i+1}, \dots, \alpha$. Současně nemohou všechna β_i padnout do M_1, neboť tato množina je algebraicky nezávislá. Vyberme tedy $\beta_i \in M_2 \setminus M_1$ a položme $\beta = \beta_i$. Důkaz je u konce. $\square$

II.6.6 Tvrzení. *Uvažme do sebe vřazená komutativní tělesa $T \subseteq U$. Ať $M_1 \subseteq U$ je nad T algebraicky nezávislá množina a ať M_1 je algebraicky závislé nad T na $M_2 \subseteq U$. Potom mohutnost M_1 nepřevyšuje mohutnost M_2.*

Důkaz. Je-li M_1 konečné nebo spočetné, můžeme podle lemmatu o výměně II.6.5 nahradit nějakou podmnožinu M_2 množinou M_1, a z toho dokazovaný vztah vyplyne. Vidíme, že zbývá vyřešit případ, kdy jsou M_1 i M_2 nekonečná. Pro tento případ uvážíme nějaké zobrazení z M_1 do množiny všech konečných podmnožin M_2 (ta je stejné mohutnosti jako M_2), které přiřazuje $\alpha \in M_1$ takové $\{\beta_1, \dots, \beta_k\} \subseteq M_2$, že α je algebraicky závislé na $\{\beta_1, \dots, \beta_k\}$. Mohutnost obrazu popsaného zobrazení bude rovna mohutnosti M_1, pokud dokážeme, že každý blok jádra zobrazení je konečný. Jsou-li ovšem $\alpha_1, \dots, \alpha_n \in M_1$ algebraicky závislá na $\{\beta_1, \dots, \beta_k\}$, je $n \leq k$ podle prvé části důkazu. $\square$

II.6.7 Důsledek. *Nechť $T \subseteq U$ jsou komutativní tělesa. Každé dvě podmnožiny U, které jsou nad T algebraicky ekvivalentní a algebraicky nezávislé, mají stejnou mohutnost.*

Z důsledku II.6.7 plyne, že shodnou mohutnost mají všechny algebraicky nezávislé množiny M, jež jsou algebraicky ekvivalentní tělesu U. Podle lemmatu II.6.4 takové množiny existují. Jsou to právě ty algebraicky nezávislé množiny, pro které je U algebraickým rozšířením $T(M)$. Takovým množinám se říká *transcendentní báze* (nad T). Společná mohutnost všech transcendentních bází se nazývá *stupeň transcendence* U nad T. Budeme ho značit $[U : T]_{tr}$.

II.6.8 Tvrzení. *Nechť $T \subseteq U \subseteq V$ jsou do sebe vřazená komutativní tělesa. Potom $[V : T]_{tr} = [V : U]_{tr} + [U : T]_{tr}$.*

Důkaz. Nechť B je transcendentní báze V nad U a A transcendentní báze U nad T. Nejprve si všimneme, že je $A \cap B = \emptyset$, neboť z algebraické nezávislosti B nad U plyne $B \cap U = \emptyset$. Ať nyní $g \in T[x_1, \dots, x_n][y_1, \dots, y_m]$ je takové, že pro nějaká po dvou různá $\alpha_1, \dots, \alpha_n \in A$ a po dvou různá $\beta_1, \dots, \beta_m \in B$ platí $g(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m) = 0$. Polynom g má koeficienty v $T[x_1, \dots, x_n]$. Z algebraické nezávislosti A vyplývá, že dosazením $\alpha_1, \dots, \alpha_n$ do nenulového koeficientu g dostaneme nenulový prvek U. Dosazením do všech koeficientů tudíž vznikne polynom $h \in U[y_1, \ldots, y_m]$, který bude nulový právě když byl nulový polynom g. Ovšem $h = 0$ plyne z algebraické nezávislosti B.

Zbývá ukázat, že V je na $A \cup B$ algebraicky závislé nad T. Protože V je algebraické nad $U(B)$, stačí ukázat, že $U(B)$ je nad T algebraicky závislé na $A \cup B$, dle lemmatu II.6.3. Množina všech prvků algebraicky závislých na $A \cup B$ nad T tvoří těleso, a proto stačí ověřit, že U je algebraicky závislé na $A \cup B$. To je ovšem zřejmé, neboť A je transcendentní báze U nad T. $\square$

II.7 Hilbertova věta o nulách

Buď R komutativní okruh. Okruh S spolu s homomorfismem $f : R \to S$ se nazývá R–algebra. Homomorfismu f se říká *strukturní* a často se explicitně nespecifikuje. To je pravda zejména tehdy, je-li f injektivní a R lze přirozeným způsobem ztotožnit s nějakým podokruhem S. Je-li R těleso, je f injektivní vždy.

Ekvivalentně lze R–algebru S definovat jako okruh, který je současně R-modulem a splňuje $r \cdot (st) = (r \cdot s)t$ pro všechna $r \in R$ a $s, t \in S$ (zde $\cdot$ značí skalární násobení, přičemž násobení v okruhu se nevyznačuje). Při takové definici se strukturní homomorfismus f získá vztahem $f(r) = r \cdot 1_S$. Je zřejmé, že $f(r_1 + r_2) = f(r_1) + f(r_2)$ pro všechna $r_1, r_2 \in R$; vztah $f(r_1 r_2) = f(r_1)f(r_2)$ plyne z $(r_1 r_2) \cdot 1_S = r_1 \cdot (r_2 \cdot 1_S) = r_1 \cdot (1_S(r_2 \cdot 1_S)) = (r_1 \cdot 1_S)(r_2 \cdot 1_S)$. Je-li naopak R-algebra zadána homomorfismem f, položíme $r \cdot s = f(r)s$. Ověřit, že S je pak R-modulem, je snadné. Přitom $r \cdot (st) = f(r)(st) = (f(r)s) \cdot t = (r \cdot s)t$.

Pojmy jako homomorfismus R–algeber nebo R–podalgebra generovaná podmnožinou $M \subseteq S$ je třeba chápat tak, že jde o současný homomorfismus okruhů a R–modulů, resp. že se jedná o nejmenší podokruh S obsahující M, který je současně R–podmodulem. Lze-li množinu M zvolit konečnou, řekneme, že okruh S je *konečně generovaný jako R–algebra.*

Okruhové generování odpovídá sčítání součinů generátorů. Při generování ve smyslu R–algebry se ještě násobí prvky R. V komutativních R–algebrách (jiné zde studovat nebudeme) jde tedy vlastně o dosazování do polynomů (více proměnných) s koeficienty v R. Proto je následující lemma zřejmé.

II.7.1 Lemma. *Ať S je komutativní R-algebra se strukturním homomorfismem $f : R \to S$. Pak S je jako R–algebra konečně generované právě když je f pro některé $n \geq 0$ možno rozšířit na surjektivní homomorfismus $g : R[x_1, \ldots, x_n] \to S$.* $\square$

Z Hilbertovy věty o bázi okamžitě plyne

II.7.2 Důsledek. *Je-li R noetherovský okruh, je každá konečně generovaná komutativní R–algebra rovněž noetherovským okruhem.* $\square$

Jsou-li $S_1 \subseteq S_2$ do sebe vřazené komutativní okruhy, lze samozřejmě S_2 chápat jako komutativní S_1–algebru.

II.7.3 Tvrzení. *Ať $S_1 \subseteq S_2$ jsou do sebe vřazené komutativní R–algebry. Jestliže A generuje S_1 jako R–algebru a B generuje S_2 jako S_1–algebru, tak $A \cup B$ generuje S_2 jako R–algebru.*

Důkaz. Každý prvek S_2 je po dosazení prvků z B hodnotou nějakého polynomu s koeficienty v S_1. Tyto koeficienty lze však získat dosazením prvků z A do polynomů s koeficienty v R. $\square$

Jsou-li A a B v předchozím tvrzení konečná, bude S_2 konečně generovanou R–algebrou. V dalších úvahách nahradíme požadavek, aby S_2 bylo konečně generováno jako S_1–algebra, silnějším požadavkem, aby S_2 bylo konečně generované jako S_1–modul. To umožní do našich úvah zahrnout aspekt dědičnosti.

II.7.4 Důsledek. *Ať $S_0 \subseteq S_1 \subseteq S_2$ jsou do sebe vřazené komutativní R–algebry, přičemž R je noetherovský komutativní okruh. Předpokládejme, že S_0 je konečně generovaná R–algebra a že S_2 je konečně generované jako S_0–modul. Potom je S_1 konečně generovanou R–algebrou.*

Důkaz. Podle důsledku II.7.2 je S_0 noetherovský okruh. Konečně generované moduly nad noetherovskými okruhy jsou noetherovské, a proto je nad S_0 i modul S_1 noetherovský (je totiž podmodulem noetherovského S_0–modulu S_2), a tím pádem konečně generovaný, takže lze použít tvrzení II.7.3. $\square$

II.7.5 Tvrzení. *Ať $S_1 \subseteq S_2$ jsou do sebe vřazené komutativní R–algebry, přičemž S_2 je jako S_1–modul konečně generované. Je-li R noetherovský komutativní okruh a je-li S_2 jako R–algebra konečně generované, je konečně generovanou R–algebrou i S_1.*

Důkaz. Budeme hledat S_0, jež by vyhovovalo předpokladům důsledku II.7.4. Budiž M konečná množina, jež generuje S_2 jako S_1–modul a obsahuje 1. Ať je dále C konečná množina, která generuje S_2 jakožto R–algebru. Pro každé $c \in C$ a $m \in M$ uvažme vyjádření $cm = \sum_{m' \in M} s_{cmm'} m'$, kde $s_{cmm'} \in S_1$. Za S_0 zvolíme R–podalgebru S_1 generovanou množinou všech hodnot $s_{cmm'}$. Označme S_3 ten S_0–podmodul S_2, který je generován M. Podle důsledku II.7.4 stačí ověřit, že platí $S_3 = S_2$. Každý prvek S_2 odpovídá nějaké hodnotě polynomu nad R po dosazení prvků z C. Protože S_3 je (mimo jiné) R-modul, stačí ověřit, že do S_3 padne každé $c_1 \dots c_k$, $k \geq 1$, kde c_i jsou (ne nutně různé) prvky C. Položme $c = c_1$ a $a = c_2 \dots c_k$ a postupujme indukcí dle k. Pro $k > 1$ máme $a \in S_3$ z indukčního předpokladu a pro $k = 1$ máme $a = 1 \in S_3$ z volby M. Proto $S_3 = S_2$ bude platit, jestliže z $a \in S_3$ a $c \in C$ vždy obdržíme $ac \in S_3$. Je-li $a = \sum s_m m$, kde $s_m \in S_0$, $m \in M$, je $ac = \sum s_m cm$. Ovšem $cm = \sum s_{cmm'} m'$ do S_3 zjevně padne. $\square$

II.7.6 Lemma. *Buď K komutativní těleso a ať $n \geq 1$. Pak $K(x_1, \dots, x_n)$ není jako K–algebra konečně generované.*

Důkaz. Postupujme sporem a předpokládejme, že $g_1, \dots, g_k$ jsou generátory. Těleso $K(x_1, \dots, x_n)$ chápeme jako podílové těleso okruhu $K[x_1, \dots, x_n]$, takže $g_i = p_i/q_i$ pro nějaká $p_i, q_i \in K[x_1, \dots, x_n]$. Okruh $K[x_1, \dots, x_n]$ je Gaussův a je to vlastní podokruh $K(x_1, \dots, x_n)$. Existuje tedy alespoň jedno q_i stupně ≥ 1. Vyjádřeme $(q_1 \cdots q_k + 1)^{-1}$ jako polynomiální hodnotu s koeficienty v K po dosazení hodnot p_i/q_i. Vhodným vynásobením obou stran tohoto vyjádření dostaneme rovnost

$$(q_1 \cdots q_k + 1)a = q_1^{r_1} \cdots q_k^{r_k},$$

pro nějaké $a \in K[x_1, \dots, x_n]$. Polynom $q_1 \cdots q_k + 1$ je stupně alespoň 1 a žádný z polynomů q_i s ním nemá společný dělitel stupně ≥ 1. To je ovšem spor se skutečností, že $K[x_1, \dots, x_n]$ je Gaussův. □

Buď K i nadále komutativní těleso. Konečně generované komutativní K–algebry se (někdy) nazývají *afinní K–algebry.* U afinních algeber budeme implicitně předpokládat, že obsahují těleso K.

II.7.7 Tvrzení. *Afinní K–algebra je tělesem právě když je rozšířením K konečného stupně.*

Důkaz. Uvažme afinnní K–algebru S a předpokládejme, že běží o těleso. Je tedy $S = K[M]$ pro nějakou konečnou $M \subseteq S$. Transcendentní stupeň S nad K je tudíž konečný. Označme B nějakou transcendentní bázi S nad K. Těleso $S = K[M] = K(B)[M]$ je nad $K(B)$ algebraické konečného stupně a S je jako $K(B)$–modul (tedy jako vektorový prostor nad tělesem $K(B)$) konečně generované. Podle tvrzení II.7.5 je afinní K–algebrou i těleso $K(B)$. To podle lemmatu II.7.6 znamená, že B je množina prázdná. □

Připomeňme, že kulatými závorkami označujeme v Gaussových okruzích ideál generovaný prvky (či ideály) uvedenými v závorkách.

II.7.8 Lemma. *Uvažme prvky $\alpha_1, \dots, \alpha_n \in K$. Ideál $(x_1 - \alpha_1, \dots, x_n - \alpha_n)$ je v $K[x_1, \dots, x_n]$ maximální. Přitom $a \in K[x_1, \dots, x_n]$ v tomto ideálu leží právě když $a(\alpha_1, \dots, \alpha_n) = 0$.*

Důkaz. Polynomy $x_i - \alpha_i$ jsou monické a okruhy $K[x_1, \dots, x_{i-1}]$ jsou obory integrity, $1 \leq i \leq n$. Chápeme-li $a \in K[x_1, \dots, x_n]$ jako polynom v x_n nad $K[x_1, \dots, x_{n-1}]$, můžeme a vyjádřit standardním dělením se zbytkem ve tvaru $a_n(x_n - \alpha_n) + b_{n-1}$, kde $a_n \in K[x_1, \dots, x_n]$ a $b_{n-1} \in K[x_1, \dots, x_{n-1}]$. Indukčním postupem tedy zjevně obdržíme existenci takových $a_i \in K[x_1, \dots, x_i]$, $1 \leq i \leq n$, že $a = \beta + \sum a_i(x_i - \alpha_i)$, kde $\beta \in K$. □

II.7.9 Věta (Hilbertova o nulách). *Nechť K je algebraicky uzavřené komutativní těleso a ať $S = K[x_1, \dots, x_n]$ pro nějaké $n \geq 1$. Potom:*

(i) Ideál M okruhu S je maximální právě když existují $\alpha_1, \dots, \alpha_n \in K$ taková, že

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

(ii) Pro každý vlastní ideál J okruhu S je množina společných nul

$$\mathbb{V}(J) = \{(\alpha_1, \dots, \alpha_n) \in K^n;\ g(\alpha_1, \dots, \alpha_n) = 0 \text{ pro všechna } g \in J\}$$

neprázdná a $\sqrt{J}$ je rovno

$$\{g \in K[x_1, \dots, x_n];\ g(\alpha_1, \dots, \alpha_n) = 0 \text{ pro všechna } (\alpha_1, \dots, \alpha_n) \in \mathbb{V}(J)\}.$$

Důkaz. Ať M je maximální ideál S. Pak S/M je těleso, které je afinní K–algebrou . Přitom K jako podokruh S/M je dáno vnořením $K \to S/M$, $\alpha \mapsto \alpha + M$. Toto vnoření je ovšem isomorfismem, neboť K je algebraicky uzavřené a S/M je podle tvrzení II.7.7 algebraickým rozšířením K. Speciálně je popsané vnoření surjektivním homomorfismem, takže pro každé x_i, $1 \leq i \leq n$, existuje $\alpha_i \in K$ takové, že $x_i - \alpha_i \in M$. Vidíme, že M obsahuje ideál $(x_1 - \alpha_1, \dots, x_n - \alpha_n)$. Z lemmatu II.7.8 plyne, že M je tomuto ideálu rovno.

Buď J nějaký vlastní ideál S. Je-li $(\alpha_1, \dots, \alpha_n) \in \mathbb{V}(J)$, tak J podle lemmatu II.7.8 leží v $(x - \alpha_1, \dots, x - \alpha_n)$, a naopak. Jinými slovy, společné nuly J jsou určeny maximálními ideály S, které obsahují J. Je-li $a^k \in J$ pro nějaké $a \in S$ a $k \geq 1$, shodují se nuly polynomu a^k s nulami polynomu a, neboť S je oborem integrity. K důkazu (ii) je proto třeba ověřit, že každé $a \in S$, které se nuluje na $\mathbb{V}(J)$, padne do $\sqrt{J}$.

Polynom $1 - a$ nemá s J žádnou společnou nulu, takže z části (i) plyne, že je $(J, 1 - a) = J + (1 - a)S$ rovno S. Toto pozorování však použijeme pouze jako motivační, budeme potřebovat totiž podobný vztah „s jedním stupněm volnosti navíc“. Uvážíme okruh $S[x_{n+1}]$ (který ztotožňujeme s $K[x_1, \dots, x_{n+1}]$) a v něm ideály $JS[x_{n+1}]$ a $(1 - ax_{n+1})S[x_{n+1}]$. Předpokládejme, že nejsou komaximální. Pak jsou obsaženy v nějakém ideálu maximálním, a proto existuje $(\alpha_1, \dots, \alpha_n, \beta) \in K^{n+1}$ takové, že $(\alpha_1, \dots, \alpha_n) \in \mathbb{V}(J)$ a $1 - a(\alpha_1, \dots, \alpha_n)\beta = 0$. Z prvé podmínky ovšem máme $a(\alpha_1, \dots, \alpha_n) = 0$, a protože $0 \neq 1$, musí zmíněné ideály být komaximální.

Okruh S je noetherovský, takže J je generováno konečně mnoha polynomy, řekněme $g_1, \dots, g_k$. Z dokázané komaximality plyne existence takových prvků $q_1, \dots, q_k$ a q z $S[x_{n+1}]$, že

$$1 = (\sum q_i g_i) + (1 - ax_{n+1})q.$$

Uvažme homomorfismus $\phi: S[x_{n+1}] \to K(x_1, \dots, x_n)$, který je na S identický a zobrazuje x_{n+1} na $1/a$ (o a můžeme zjevně předpokládat, že je nenulové). Z předchozí rovnosti máme

$$1 = \phi(1) = (\sum \phi(q_i) g_i) + 0 = \sum \phi(q_i) g_i.$$

Přitom každé $\phi(q_i)$ je možné vyjádřit ve tvaru b_i/a^{e_i}, kde $b_i \in S$, $e_i \geq 0$. Vhodným vynásobením vztahu pak dostaneme rovnost

$$a^f = \sum b_i g_i,$$

pro nějaké $f \geq 1$ a nějaké $b_i \in S$. Dokázali jsme $a \in \sqrt{J}$. □

II.7.10 Důsledek. *Buď K algebraicky uzavřené komutativní těleso. Každý prvoideál okruhu $S = K[x_1, \dots, x_n]$ je roven průniku maximálních ideálů S.*

III Celistvost, mříže a Dedekindovy okruhy

III.1 Determinanty

Pro determinanty matic nad komutativními okruhy platí většina vztahů známých z lineární algebry. Protože však tyto vztahy byly vysloveny s ohledem na aplikace ve vektorových prostorech formou odpovídající úvodnímu vysokoškolskému kurzu, jeví se vhodné je zde nabídnout k zopakování v obecnější formě a se zkrácenými důkazy.

Ať R je komutativní okruh. Množinu všech $n \times m$ matic budeme značit $\mathrm{M}_{n,m}(R)$. Tuto množinu lze pokládat za R-modul. V případě $n = m$ je možno matice násobit a dostáváme *maticový okruh* $\mathrm{M}_{n,n}(R)$. Je-li $A \in \mathrm{M}_{n,n}(R)$, tak do $\mathrm{M}_{n,n}(R)$ padne i matice *transponovaná*, kterou značíme A^{T}.

Determinant matice $A = (a_{ij})$ se definuje vztahem

$$\det A = \sum_{\sigma \in \mathrm{S}_n} (\operatorname{sgn} \sigma)\, a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}.$$

Pro každé $\sigma \in \mathrm{S}_n$ je $\operatorname{sgn} \sigma = \operatorname{sgn} \sigma^{-1}$, takže z rovnosti

$$a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} = a_{\sigma^{-1}(1),1} \cdots a_{\sigma^{-1}(n),n}$$

bezprostředně dostáváme $\det A = \det A^{\mathrm{T}}$.

Liší-li se matice A, B, C pouze v jednom řádku, přičemž tento řádek v C je součtem odpovídajících řádků v A a B, pak zjevně $\det C = \det A + \det B$. Podobně pro sloupce.

Za samozřejmý budeme rovněž považovat vztah $\det B = r \det A$ v případě, kdy B vznikne z A tak, že prvky jistého řádku jsou nahrazeny svými r-násobky.

III.1.1 Lemma. *Ať $A \in \mathrm{M}_{n,n}(R)$ má s-tý a r-tý sloupec (řádek) shodný. Pak* $\det A = 0$.

Důkaz. Je-li $\tau \in \mathrm{S}_n$ libovolná transpozice, tak platí

$$\det A = \sum_{\sigma \in A_n} \operatorname{sgn} \sigma((a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}) - (a_{1,\tau\sigma(1)} \cdots a_{n,\tau\sigma(n)})),$$

kde A_n je alternující grupa sudých permutací. Zvolíme-li $\tau = (r\ s)$, bude $a_{i,\sigma(i)}$ rovno $a_{i,\tau\sigma(i)}$ pro každé i, $1 \le i \le n$. □

Z předchozího již plyne, že přičtením násobku daného sloupce k sloupci odlišnému se hodnota determinantu nezmění — totéž platí pro řádky.

Odsud vyplývá, že výměnou dvou různých řádků (sloupců) se hodnota determinantu změní na hodnotu opačnou.

Pro každé s a t, kde $1 \leq s, t \leq n$, definujeme k matici $A = (a_{i,j}) \in \mathrm{M}_{n,n}(R)$ matici $\bar{A}_{st}$ jako $(n-1) \times (n-1)$ matici, jež vznikne vypuštěním s-tého řádku a t-tého sloupce.

Matice $\operatorname{Adj} A = (d_{ij}) \in \mathrm{M}_{n,n}(R)$, kde $d_{ij} = (-1)^{i+j} \det \bar{A}_{ji}$ se nazývá *adjunkt* matice A. Uvedená definice se používá pro $n > 1$. Pro $n = 1$ se klade $\operatorname{Adj} A = \mathrm{I}_1$. (Obecně I_n zde značí $n \times n$ matici s jedničkami na diagonále a nulami mimo diagonálu.)

III.1.2 Lemma. *Ať je v matici $A \in \mathrm{M}_{n,n}(R)$, $n > 1$, nahrazen s-tý řádek řádkem $(0, \dots, 0, 1, 0, \dots, 0)$, kde 1 se nachází na t-té pozici. Determinant takto pozměněné matice je roven $(-1)^{s+t} \det \bar{A}_{st}$.*

Důkaz. Je třeba $n - s$ transpozic k přesunu s–tého řádku na n–tý a $n - t$ transpozic k přesunu t–tého sloupce na n–tý. Vzniklá matice má determinant shodný s maticí $\bar{A}_{st}$. □

III.1.3 Tvrzení. *Ať $n > 1$ a $A = (a_{ij}) \in \mathrm{M}_{n,n}(R)$. Pak pro každé s, $1 \leq s \leq n$, platí*

$$\det A = \sum_j a_{sj} (-1)^{s+j} \det \bar{A}_{sj} \qquad a \qquad \det A = \sum_i a_{is} (-1)^{s+i} \det \bar{A}_{is}.$$

Důkaz. Stačí dokázat pouze prvý vztah. Nahradíme-li A soustavou n matic, z nichž j–tá má na místě (s, j) hodnotu a_{sj} a má nuly na ostatních místech j–tého řádku (zatímco v jiných řádcích se s A shoduje), bude $\det A$ roven součtu determinantů těchto matic. Zbytek plyne z lemmatu III.1.2. □

Symbol δ_{st} se níže používá ve standardním významu ($\delta_{st} = 1$ pokud $s = t$, jinak $\delta_{st} = 0$).

III.1.4 Důsledek. *Ať $n > 1$ a ať $A = (a_{ij}) \in \mathrm{M}_{n,n}(R)$. Pro $1 \leq s, t \leq n$ máme*

$$\sum_j a_{sj} (-1)^{t+j} \det \bar{A}_{tj} = \delta_{st} \det A \qquad a \qquad \sum_i a_{is} (-1)^{t+i} \det \bar{A}_{it} = \delta_{st} \det A.$$

Důkaz. Pro $s = t$ je zde reprodukováno předchozí tvrzení. To lze použít i pro $s \neq t$, neboť v takovém případě je součet shodný s rozvojem podle t–tého řádku matice, která vznikne z A náhradou t–tého řádku s–tým řádkem. Determinant takové matice je však podle lemma III.1.1 roven nule. □

III.1.5 Tvrzení. *Ať je $A \in \mathrm{M}_{n,n}(R)$ a ať B je adjunkt matice A. Potom $AB = BA = (\det A)\mathrm{I}_n$.*

Důkaz. Případ $n = 1$ je jasný, neboť pak $B = I_1$. V matici AB máme na místě (s, t) hodnotu $\sum a_{sj} (-1)^{j+t} \det A_{tj} = \delta_{st} \det A$. V matici BA máme na místě (s, t) hodnotu $\sum (-1)^{i+s} \det A_{is} a_{it} = \delta_{st} \det A$. Vztah tedy plyne z důsledku III.1.4. □

III.2 Celistvá rozšíření

Nejprve připomeneme, co se rozumí značením $(A : B)$, které bylo zavedeno již dříve, včetně motivace tohoto značení. V tělese je $x = yz^{-1}$ právě když $xz = y$. Píšeme-li yz^{-1} jako $y : z$, tak $xz = y$ právě když $y : z = x$. Zaměníme-li rovnost za inkluzi a uvažujeme-li na místo prvků y a z množiny A a B, dostaneme definici

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

Přitom R je komutativní okruh a A i B jsou podmnožiny nějakého R–modulu M. Častým je přitom případ, kdy $M = R$.

III.2.1 Lemma. *Je-li A podmodul R–modulu M, je $(A : B)$ ideál R, pro libovolné $B \subseteq M$.*

Důkaz. Pro $u, v \in (A : B)$ a $r \in R$ máme pro $b \in B$ jak $(u+v)b = ub+vb \in A$, tak $(ru)b = r(ub) \in A$. □

Je-li $U \subseteq R$, tak se místo $U \cap (A : B)$ píše též $(A :_U B)$. O ideálu $(0 : B)$ se mluví jako o *anihilátoru* B a označuje se též $\mathrm{Ann}(B)$.

III.2.2 Tvrzení. *Ať $R \subseteq S$ jsou komutativní okruhy a ať M je S–modul, který je jako R–modul konečně generovaný n prvky, kde $n \geq 1$. Ať I je ideál R a ať $s \in S$ je takové, že $sM \subseteq IM$. Potom existují $a_i \in I^i$, $1 \leq i \leq n$, takové, že $s^n + a_1 s^{n-1} + \cdots + a_{n-1}s + a_n \in (0 :_S M) = \mathrm{Ann}(M)$.*

Důkaz. Ať $g_1, \ldots, g_n$ jsou generátory M jakožto R-modulu. Pro $j \in \{1, \ldots, n\}$ uvažme matici indukovanou translací s, tedy uvažme $b_{ij} \in I$ taková, že

$$sg_i = \sum_j b_{ij} g_j.$$

Pro $B = (b_{ij})$ máme $(s\mathrm{I}_n - B)(g_1, \ldots, g_n)^{\mathrm{T}} = 0$. Položme $C = s\mathrm{I}_n - B$ a ať D je adjunkt C. Podle tvrzení III.1.5 je $DC = (\det C)\mathrm{I}_n$, takže z $DC(g_1, \ldots, g_n)^{\mathrm{T}} = 0$ plyne $(\det C)g_i = 0$ pro každé i, $1 \leq i \leq n$. Dokázali jsme, že $\det C \in (0 :_S M)$.

Existence $a_i \in I^i$ takových že $\det C = s^n + a_1 s^{n-1} + \cdots + a_n$ plyne přímo z definice C. □

Ať R je podokruh komutativního okruhu S, a ať $s \in S$. Řekneme, že s je *celistvé* nad R právě když existuje $h \geq 1$ a $r_0, r_1, \ldots, r_{h-1} \in R$ taková, že

$$s^h + r_{h-1}s^{h-1} + \cdots + r_1 s + r_0 = 0.$$

Celistvé prvky jsou tedy kořeny monických polynomů z $R[x]$.

Řekneme, že S je *celistvé* nad R, pokud je každý prvek S celistvý nad R. Homomorfismus komutativních okruhů $f : R_1 \to R_2$ nazveme *celistvý*, je-li R_2 celistvé nad $\mathrm{Im}(f)$.

III.2.3 Tvrzení. *Ať R je Gaussův obor integrity a ať T je jeho podílové těleso. Je-li $u \in T$ prvek celistvý nad R, je $u \in R$.*

Důkaz. Ať $u^h + r_{h-1}u^{h-1} + \cdots + r_1u + r_0 = 0$. Vyjádříme u jako s/t tak, aby $s, t \in R$ byla nesoudělná. Potom $s^h + r_{h-1}s^{h-1}t + \cdots + r_1st^{h-1} + r_0t^h = 0$, takže každý ireducibilní dělitel t musí být dělitelem s. Z jejich nesoudělnosti plyne invertibilita t. □

Jsou-li $R \subseteq S \subseteq T$ komutativní okruhy, přičemž $a_1, \ldots, a_n \in S$ generují S jako R–modul a $b_1, \ldots, b_m \in T$ generují T jako S–modul, tak $\{a_ib_j;\ 1 \le i \le n$ a $1 \le j \le m\}$ zjevně generuje T jako R–modul.

III.2.4 Tvrzení. *Ať R je podokruh komutativního okruhu S a ať je $u \in S$. Je ekvivalentní:*

(i) *u je celistvé nad R;*

(ii) *$R[u]$ je podokruh S, který je konečně generovaný jako R–modul;*

(iii) *existuje podokruh S, který je konečně generovaný jako R–modul a obsahuje $R[u]$;*

(iv) *existuje věrný $R[u]$–modul, který je jako R–modul konečně generovaný.*

Důkaz. Implikace (ii)⇒(iii) a (iii)⇒(iv) jsou triviální. Jestliže pro vhodná $r_0, r_1, \ldots, r_{h-1} \in R$ platí $u^h + r_{h-1}u^{h-1} + \cdots + r_1u + r_0 = 0$, tak je $R[u] = \{\sum_{0 \le i < h} t_iu^i;\ t_i \in R\}$, takže $R[u]$ je jako R–modul konečně generován množinou $\{1, u, \ldots, u^{h-1}\}$. Odsud (i)⇒(ii) a zbývá dokázat (iv)⇒(i).

Ať tedy je M věrný $R[u]$–modul, který je generovaný n prvky. Použijeme tvrzení III.2.2 tak, že $S = R[u]$ a $I = R$. Máme $uM \subseteq M = RM$, takže $u^n + a_1u^{n-1} + \cdots + a_{n-1}u + a_n$ padne pro vhodná $a_i \in R$ do anihilátoru M. Věrnost M znamená, že tento anihilátor obsahuje pouze prvek 0. □

III.2.5 Tvrzení. *Ať je R podokruh komutativního okruhu S a ať $u_1, \ldots, u_n \in S$ jsou celistvá nad R. Potom $R[u_1, \ldots, u_n]$ je podokruh S, který je nad R celistvý a který je jakožto R–modul konečně generovaný.*

Důkaz. Přímočarým postupem indukcí ověříme, že $R[u_1, \ldots, u_n]$ je jakožto R–modul konečně generované. Stačí si uvědomit, že pro i, $1 \le i \le n$, je u_i celistvé nad $R[u_1, \ldots, u_{i-1}]$, takže $R[u_1, \ldots, u_i]$ je jakožto $R[u_1, \ldots, u_{i-1}]$–modul konečně generované. Z indukčního kroku lze získat konečnou generovanost $R[u_1, \ldots, u_{i-1}]$ jakožto R–modulu. Spojením obou vztahů dostaneme konečnou generovanost $R[u_1, \ldots, u_i]$ nad R.

Je-li $u \in R[u_1, \ldots, u_n]$, tak je $R[u_1, \ldots, u_n]$ možné chápat jako $R[u]$–modul. Ten je samozřejmě věrný a celistvost u nad R plyne z tvrzení III.2.4. □

III.2.6 Důsledek. *Ať $R \subseteq S$ jsou komutativní okruhy. Pak množina všech $u \in S$, jež jsou celistvé nad R, tvoří podokruh S obsahující R.*

Důkaz. Ať $u, v \in S$ jsou prvky celistvé nad R. Podle tvrzení III.2.5 je $R[u, v]$ podokruh S, který se skládá pouze z celistvých prvků. Protože $u + v$, uv i $-v$ leží v $R[u, v]$, musí být také celistvé. □

Podokruhu všech celistvých prvků z důsledku III.2.6 se říká *celistvý uzávěr* R v S.

III.2.7 Tvrzení. *Ať jsou $R \subseteq S \subseteq T$ komutativní okruhy, přičemž S je celistvé nad R. Je-li $t \in T$ celistvé nad S, je t celistvé nad R.*

Důkaz. Uvažme $t \in T$ takové, že $t^h + s_{h-1}t^{h-1} + \cdots + s_1 t + s_0 = 0$ pro vhodná $s_0, s_1, \ldots, s_{h-1} \in S$. Pak je t celistvé nad $C = R[s_0, s_1, \ldots, s_{h-1}]$ a $C[t]$ je konečně generované nad R, a tudíž je $C[t]$ konečně generovaný R–modul, který je věrným $R[t]$–modulem. Z tvrzení III.2.4 proto plyne, že prvek t je nad R celistvý. $\square$

III.2.8 Důsledek. *Ať jsou $R \subseteq S \subseteq T$ komutativní okruhy, přičemž S je celistvé nad R. Celistvý uzávěr R v T je pak shodný s celistvým uzávěrem S v T. Speciálně platí, že T je celistvé nad S právě když je celistvé nad R.* $\square$

III.2.9 Tvrzení. *Ať je $R \subseteq T$, kde T je těleso a R je okruh. Ať je U rozšíření T a ať je $\alpha \in U$ celistvé nad R. Pak jsou nad R celistvé jak všechny koeficienty minimálního polynomu $a \in T[x]$ prvku α, tak všechny kořeny tohoto polynomu, které leží v U.*

Důkaz. Tvrzení zjevně stačí dokázat pro případ, kdy U je rozkladovým nadtělesem minimálního polynomu prvku α nad T. Můžeme tedy předpokládat, že U je algebraickým rozšířením T a že $\bar{U}$ je algebraický uzávěr U. Víme, že α je kořenem nějakého monického polynomu $c \in R[x] \subseteq T[x]$. Proto a dělí c. Je-li $\beta \in \bar{U}$ nějaký jiný kořen a, existuje $g \in \mathrm{Hom}_T(U, \bar{U})$ takové, že $g(\alpha) = \beta$. Pak je ovšem β kořen $g_x(c) = c$, takže β je celistvé nad R. Protože koeficienty a leží v podokruhu $\bar{U}$, který je generován kořeny a, musí být podle důsledku III.2.6 tyto koeficienty celistvé. $\square$

III.2.10 Důsledek. *Ať je $R \subseteq T$, kde T je těleso a R je okruh. Ať je U rozšíření T konečného stupně a ať je $\alpha \in U$ celistvé nad R. Pak $N_{U|T}(\alpha)$ i $\mathrm{Tr}_{U|T}(\alpha)$ jsou nad R celistvé.*

Důkaz. Podle tvrzení II.5.1 lze normu i stopu prvku odvodit z koeficientů minimálního polynomu. $\square$

III.2.11 Tvrzení. *Ať $R \subseteq S$ jsou obory integrity, přičemž S je celistvé nad R. Okruh S je tělesem právě když R je tělesem.*

Důkaz. V oborech integrity lze pro celistvé prvky $s \neq 0$ zjevně nalézt $r_0, \ldots, r_{n-1} \in R$ tak, že $s^n + r_{n-1}s^{n-1} + \cdots + r_1 s + r_0 = 0$ a $r_0 \neq 0$. Ze zápisu $s(s^{n-1} + r_{n-1}s^{n-2} + \cdots + r_1) = r_0$ plyne invertibilita s, je-li r_0 invertibilní. Naopak, je-li S těleso a $r \in R$ nenulové, je r^{-1} celistvé a z $r^{-n} + r_{n-1}r^{-(n-1)} + \cdots + r_1 r^{-1} + r_0 = 0$ plyne $r^{-1} = -(r_{n-1} + \cdots + r_1 r^{n-2} + r_0 r^{n-1}) \in R$. $\square$

Tvrzení III.2.11 je celkem prosté, avšak má důležitý důsledek.

III.2.12 Tvrzení. *Ať $R \subseteq S$ jsou komutativní okruhy, přičemž S je celistvé nad R. Ideál I okruhu S je maximální právě když $I \cap R$ je maximální v R.*

Důkaz. Okruh $R/R \cap I \cong (R+I)/I$ lze uvedeným ztotožněním považovat za podokruh S/I. Přitom S/I je nad $(R+I)/I$ celistvý. Tyto okruhy jsou tělesa právě když ideály I a $R \cap I$ jsou v S a R po řadě maximální. $\square$

III.3 Celistvě uzavřené obory integrity

Jsou-li $R \subseteq S$ komutativní okruhy takové, že R je rovno svému celistvému uzávěru v S, nazýváme R v S *celistvě uzavřené*. Obor integrity se nazývá *celistvě uzavřený*, je-li celistvě uzavřený ve svém podílovém tělese. Z tvrzení III.2.3 vyplývá, že Gaussovy obory integrity jsou vždy celistvě uzavřené.

Z tvrzení III.2.9 a důsledku III.2.10 můžeme okamžitě odvodit:

III.3.1 Tvrzení. *Ať je T podílové těleso celistvě uzavřeného oboru integrity R a ať $U \geq T$ je algebraické rozšíření těles. Pak minimální polynom $m_{\alpha,T}$ každého celistvého prvku $\alpha \in U$ padne do $R[x]$. Je-li U nad T konečného stupně, tak také platí, že v R leží jak $N_{U|T}(\alpha)$, tak $\mathrm{Tr}_{U|T}(\alpha)$.* □

Uvažme nyní situaci, kdy R je celistvě uzavřený obor integrity, T jeho podílové těleso, U separabilní rozšíření T konečného stupně n a S celistvý uzávěr R v U.

Připomeňme, že R^* a S^* označují příslušnou multiplikativní grupu invertibilních prvků (grupu jednotek).

III.3.2 Tvrzení. *Pro každé $\alpha \in S$ je $N_{U|T}(\alpha) \in R$ a $\mathrm{Tr}_{U|T}(\alpha) \in R$. Navíc $\alpha \in S^*$ právě když $N_{U|T}(\alpha) \in R^*$.*

Důkaz. Norma i stopa padne do T dle důsledku 2.10. Je-li $\alpha\beta = 1$, kde α i β jsou z S, tak $N_{U|T}(\alpha)N_{U|T}(\beta) = 1$. Ať je naopak $N_{U|T}(\alpha) \in R^*$. Invertibilita α v S pak vyplývá z toho, že $N_{U|T}(\alpha) = \alpha \prod_g g(\alpha)$, kde g probíhá neidentické T–homomorfismy $U \to \bar{U}$ (zjevně stačí ukázat, že $\prod_g g(\alpha)$ leží v S. To ovšem plyne z toho, že $g(\alpha) \in S$ pro každé g). □

III.3.3 Lemma. *Pro libovolná $\alpha_1, \dots, \alpha_k \in U$ existuje $r \in R$ takové, že $r\alpha_1, \dots, r\alpha_k \in S$.*

Důkaz. Je snadné si uvědomit, že stačí lemma dokázat pouze pro $k = 1$. Položme $\alpha = \alpha_1$ a zapišme jeho minimální polynom $a \in T[x]$ ve tvaru

$$x^n + (r_1/s_1)x^{n-1} + \cdots + (r_{n-1}/s_{n-1})x + (r_n/s_n),$$

kde $r_i, s_i \in R$, $1 \leq i \leq n$. Toto vyjádření můžeme upravit tak, aby platilo $s_1 = \cdots = s_n = s \in R^*$. Pak

$$(sx)^n + (r_1 s^0)(sx)^{n-1} + \cdots + (r_{n-1}s^{n-2})x + (r_n s^{n-1}) = 0,$$

z čehož vyplývá, že $s\alpha$ je celistvé, a tedy $s\alpha \in S$. □

Vidíme, že je-li $\alpha_1, \dots, \alpha_n$ nějaká báze U nad T, tak $r\alpha_1, \dots, r\alpha_n$ je pro vhodné $r \in R$ bází U nad T, jež se skládá pouze z prvků S. Báze $\alpha_1, \dots, \alpha_n$ tělesa U nad T se nazývá *celistvá*, jestliže $\alpha_1, \dots, \alpha_n$ leží v S a každý prvek S lze vyjádřit jako $\sum r_i\alpha_i$, kde $r_i \in R$. Je zřejmé, že takové vyjádření je jednoznačné. Obecně nemusí celistvé báze existovat. Záhy však nahlédneme, že existují, je-li R obor integrity hlavních ideálů.

III.3.4 Tvrzení. *Ať $\alpha_1, \dots, \alpha_n \in S$ tvoří bázi U nad T, a ať $d = \triangle(\alpha_1, \dots, \alpha_n)$. Potom je $dS \subseteq R\alpha_1 + \dots + R\alpha_n$.*

Důkaz. Ať Tr značí $\mathrm{Tr}_{U|T}$. Vyjádříme $\alpha \in U$ jako $\sum t_i\alpha_i$, kde $t_i \in T$. Pak pro každé $\beta \in U$ je $\mathrm{Tr}(\alpha\beta) = \sum_i t_i \mathrm{Tr}(\alpha_i\beta)$. Necháme-li β probíhat α_j, $1 \le j \le n$, nahlédneme, že $t_1, \dots, t_n$ jsou řešením lineární soustavy rovnic $\mathrm{Tr}(\alpha\alpha_j) = \sum_i \mathrm{Tr}(\alpha_i\alpha_j)x_i$. Je-li $\alpha \in S$, padnou stopy $\mathrm{Tr}(\alpha\alpha_j)$ do R. Determinant soustavy je roven $d \neq 0$ a podle Cramerova pravidla jsou řešení t_i tvaru r_i/d, kde $r_i \in R$ je determinant matice, v níž je i–tý sloupec nahrazen sloupcem $(\mathrm{Tr}(\alpha\alpha_1), \dots, \mathrm{Tr}(\alpha\alpha_n))^{\mathrm{T}}$. Vidíme tedy, že $d\alpha = \sum r_i\alpha_i \in S$. □

III.3.5 Lemma. *Množina $M \subseteq U$ je S–modul. Pro každé $\mu \in U^*$ je $\mu M \subseteq U$ rovněž S–modul a $\alpha \mapsto \mu\alpha$ je izomorfismus S–modulů $M \cong \mu M$.*

Důkaz. Množina μM je zjevně uzavřená na součiny a násobky prvky S. Násobení prvkem μ je slučitelné jak se sčítáním, tak se skalárním násobením, takže jde o homomorfismus. Jeho jádro je ovšem triviální. □

Je dobré si uvědomit, že každý S–modul je současně R–modulem, a každý izomorfismus S–modulů je současně izomorfismem R–modulů. Podmoduly S–modulu jsou také R–podmoduly, takže S–modul, který je jako R–modul noetherovský, je noetherovský i jako S–modul. Proto z tvrzení III.3.4 a lemmatu III.3.5 snadno dokážeme

III.3.6 Důsledek. *Je-li obor R noetherovský, je noetherovský i obor S.*

Důkaz. Podle lemmatu III.3.5 stačí dokázat, že je noetherovský R–modul dS, kde d je jako v tvrzení III.3.4. Podle tohoto tvrzení tomu tak vskutku je, neboť dS je podmodulem noetherovského R–modulu (viz lemmata I.1.6 a I.5.1). □

Předchozí důsledek využijeme až později. Nyní budeme, jak jsme již výše naznačili, studovat situaci, kdy R je obor hlavních ideálů.

III.3.7 Tvrzení. *Ať je R obor hlavních ideálů. Pak má U celistvou bázi.*

Důkaz. Nechť $\alpha_1, \dots, \alpha_n \in S$ tvoří bázi U nad T. Podle tvrzení III.3.4 je $dS \subseteq R\alpha_1 + \dots + R\alpha_n$, kde $d = \triangle(\alpha_1, \dots, \alpha_n)$. Ovšem $R\alpha_1 + \dots + R\alpha_n = \sum R\alpha_i$ je R–modul, ve kterém $\alpha_1, \dots, \alpha_n$ je volnou bází. Proto je dS rovněž volný R–modul hodnosti $\le n$ (jak plyne z důsledku I.5.5 nebo z důsledku I.6.3). Podle lemmatu III.3.5 platí $dS \cong S$. Protože S obsahuje volný R–modul $\sum R\alpha_i$ hodnosti n, je $S \cong dS$ hodnosti $\ge n$, takže hodnost R–modulu S je přesně n. □

III.3.8 Věta. *Ať je R obor integrity hlavních ideálů. Každý nenulový konečně generovaný S–podmodul tělesa U je volným R–modulem hodnosti $[U : T]$. Speciálně má U celistvou bázi.*

Důkaz. Ať M je nenulový konečně generovaný S–modul, který leží v U, a ať $\mu_1, \dots, \mu_t$ je nějaké množina jeho generátorů. Uvažme nenulové $r \in R$ takové, že $r\mu_1, \dots, r\mu_k$ padne do S. Jeho existence plyne z lemmatu III.3.3. Pak $M \cong rM \subseteq S$, takže M je volný modul hodnosti nanejvýš $n = [U : T]$. Zvolíme-li nenulové $\sigma \in M$, obdržíme $S \cong S\sigma \subseteq M$, takže M obsahuje volný R–modul hodnosti $\geq n$. Hodnost M je tedy rovna n. $\square$

V teorii čísel se často pracuje se situací, kdy $R = \mathbb{Z}$ a $T = \mathbb{Q}$. Pak U je možné chápat jako podtěleso algebraického uzávěru $\bar{\mathbb{Q}}$, a ten je možno pokládat za podtěleso $\mathbb{C}$. Jinými slovy $\bar{\mathbb{Q}}$ je těleso všech algebraických čísel. Místo U se v této situaci píše většinou K. Máme $\mathbb{Q} \leq K < \bar{\mathbb{Q}}$, neboť K je nad $\mathbb{Q}$ konečného stupně. Přitom o K hovoříme jako o *číselném tělese* (number field). Celistvý uzávěr $\mathbb{Z}$ v K se značí $\mathbb{Z}_K$ a máme $\mathbb{Z}_K = \mathbb{Z}_{\bar{\mathbb{Q}}} \cap K$. Prvkům $\mathbb{Z}_{\bar{\mathbb{Q}}}$ se říká *algebraická celá čísla* (algebraic integers).

Uvažme nyní nějaký konečně generovaný $\mathbb{Z}_K$–modul $M \subseteq K$. Podle III.3.8 má strukturu volné abelovské grupy hodnosti $n = [K : Q]$ a můžeme ho vyjádřit jako $\mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$, kde $\alpha_1, \ldots, \alpha_n$ je nějaká jeho volná báze. Je-li $\beta_1, \ldots, \beta_n$ nějaká jiná jeho volná báze a P přechodová matice vyjadřující β_j jako celočíselné kombinace α_i, musí být P i P^{-1} matice celočíselné, z čehož vyplývá, že jejich determinant je roven ± 1. Podle tvrzení II.5.6 je $\triangle(\beta_1, \ldots, \beta_n) = (\det P)^2 \triangle(\alpha_1, \ldots, \alpha_n)$, takže vidíme, že hodnota diskriminantu $\triangle(\alpha_1, \ldots, \alpha_n)$ je nezávislá na volbě báze. Místo $\triangle(\alpha_1, \ldots, \alpha_n)$ proto můžeme psát pouze $\triangle(M)$.

Je-li $M' \supseteq M$ další konečně generovaný $\mathbb{Z}_K$–modul obsažený v K, můžeme najít bázi $\alpha_1, \ldots, \alpha_n$ modulu M' a kladná čísla $r_1, \ldots, r_n$ tak, že $r_1\alpha_1, \ldots, r_n\alpha_n$ je báze modulu M (to plyne například z lemmatu I.6.3). Pak $r = r_1 \cdots r_n$ je rovno $|M'/M| = |M' : M|$ a přechodová matice P (viz tvrzení II.5.6) má determinant rovný r. Můžeme vyslovit:

III.3.9 Tvrzení. *Ať K je číselné těleso a ať $M \subseteq M' \subseteq K$ jsou konečně generované nenulové $\mathbb{Z}_K$–moduly. Potom je index $|M' : M|$ konečný a $\triangle(M) = |M' : M|^2 \triangle(M')$.* $\square$

III.3.10 Důsledek. *Ať $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}_K$, kde K je číselné těleso stupně n. Pak $\alpha_1, \ldots, \alpha_n$ tvoří celistvou bázi právě když $|\triangle(\alpha_1, \ldots, \alpha_n)|$ je kladné a nejmenší možné.* $\square$

III.4 Dedekindovy obory integrity

Okruh S nazveme *Dedekindovým oborem*, jde-li o celistvě uzavřený noetherovský obor integrity, ve kterém je každý prvoideál maximálním ideálem.

III.4.1 Věta. *Ať R je Dedekindův obor, T jeho podílové těleso a U separabilní rozšíření T konečného stupně. Potom celistvý uzávěr S oboru R v U je rovněž Dedekindův obor. Speciálně platí, že $\mathbb{Z}_K$ je Dedekindův obor pro libovolné číselné těleso K.*

Důkaz. Z důsledku III.3.6 plyne, že S je noetherovské. Je-li P prvoideál S, je $P \cap R$ prvoideál R. Tento provideál je maximální, protože R je Dedekindův obor. Podle tvrzení III.2.12 je proto maximální i P v S. Z lemma III.3.3 plyne, že U je podílové těleso S. Použijeme-li důsledek III.2.8 tak, že na místě T uvažujeme U, vidíme, že S musí být v U celistvě uzavřené. $\square$

III.4.2 Lemma. *Pro každý nenulový ideál I noetherovského komutativního okruhu R existují prvoideály $P_1, \ldots, P_r$ takové, že $I \supseteq P_1 \cdots P_r$.*

Důkaz. Je-li množina ideálů, pro které lemma neplatí, neprázdná, existuje mezi nimi nějaký maximální vzhledem k inkluzi, neboť R je noetherovský. Označme ho I. Ten jistě není prvoideálem, a proto existují ideály $A \supsetneq I$ a $B \supsetneq I$ takové, že $AB \subseteq I$. Každý z ideálů A a B obsahuje součin prvoideálů, a proto takový součin obsahuje i I. Dosáhli jsme sporu. $\square$

Uvažme nyní nějaký Dedekindův obor R a ať T označuje jeho podílové těleso.

III.4.3 Lemma. *Ať P je prvoideál Dedekindova oboru R. Položme $P^{-1} = (R :_T P)$. Potom je každý nenulový ideál A okruhu R vlastní podmnožinou množiny*

$$AP^{-1} = \{\sum a_i p_i;\ \ a_i \in A \ \text{ a } \ p_i \in P^{-1}\}.$$

Důkaz. Máme $P^{-1} = \{t \in T;\ tP \subseteq R\}$, takže $R \subseteq P^{-1}$ a A je jistě podmnožinou popsané množiny. Je třeba dokázat, že je to vlastní podmnožina. Nejprve ukážeme, že R je vlastní podmnožina R–modulu P^{-1}.

Ať a je nenulový prvek P a ať $P_1 \cdots P_r \subseteq aR \subseteq P$, kde $P_1, \ldots, P_r$ jsou prvoideály R a r je nejmenší možné. Protože P je prvoideál, tak je některý z $P_1, \ldots, P_r$ obsažen v P. Můžeme proto předpokládat $P_1 \subseteq P$. Protože P_1 je maximální, musí být $P_1 = P$. Z minimality r vyplývá, že $P_2 \cdots P_r$ není obsaženo v aR. Uvažme $b \in (P_2 \cdots P_r) \setminus aR$. Pak $a^{-1}b \notin R$. Na druhé straně $bP = bP_1 \subseteq P_1 \cdots P_r \subseteq aR$, takže $(a^{-1}b)P \subseteq R$, z čehož plyne $a^{-1}b \in P^{-1} \setminus R$.

Ať $\alpha_1, \ldots, \alpha_n$ je systém generátorů A jako R–modulu (připomeňme, že A je konečně generované, protože R je noetherovské). Budeme předpokládat $AP^{-1} = A$ a ukážeme, že tento předpoklad vede ke sporu. Pro každé $u \in P^{-1}$ uvážíme matici $U \in \mathrm{M}_{n,n}(R)$, která vyjadřuje translaci $u\colon A \to A$, $\alpha \mapsto u\alpha$, vůči generátorům $\alpha_1, \ldots, \alpha_n$. Je tedy $(u\alpha_1, \ldots, u\alpha_n)^{\mathrm{T}} = U(\alpha_1, \ldots, \alpha_n)^{\mathrm{T}}$, takže pro $V = u\mathrm{I}_n - U$ máme $V(\alpha_1, \ldots, \alpha_n)^{\mathrm{T}} = 0$. Uvážíme-li adjunkt matice V, tak z tvrzení III.1.5 vyplývá, že $(\det V)\alpha_i = 0$ pro každé i, $1 \le i \le n$. Vše probíhá v tělese T, takže $\det V = 0$ a u je kořenem monického polynomu $\det(x\mathrm{I}_n - U)$. Z toho plyne $u \in R$, takže $P^{-1} = R$, a to je spor s prvou částí důkazu. $\square$

Označení P^{-1} pro $(R :_T P) = \{t \in T;\ tP \subseteq R\}$ budeme používat i nadále. Také množinu $\{\sum a_i p_i;\ \ a_i \in A \ \text{ a } \ p_i \in P^{-1}\}$ budeme i dále značit AP^{-1}. Je-li $A \subseteq P$, je AP^{-1} zjevně ideál R.

III.4.4 Věta. *Každý vlastní ideál I Dedekindova oboru R lze jednoznačně, až na pořadí, vyjádřit jako součin prvoideálů $P_1 \cdots P_r$.*

Důkaz. Nejprve dokážeme, že PP^{-1} je rovno R. Pro každé $t \in P^{-1}$ je $tP \subseteq R$, takže $PP^{-1} \subseteq R$. Protože PP^{-1} je R–modul, musí to být ideál R. Jelikož $1 \in P^{-1}$ a P je maximální, máme dvě možnosti: buď $PP^{-1} = P$, nebo $PP^{-1} = R$. Prvá možnost je však vyloučena lemmatem III.4.3, volíme-li $A = P$.

Buď nyní I nějaký vlastní nenulový ideál, který nelze vyjádřit jako součin prvoideálů. Okruh R je noetherovský, a proto lze I zvolit tak, aby bylo vzhledem k uvedené vlastnosti maximální. Pak $I \subseteq P$ pro nějaký prvoideál P. Z $I = IR = I(P^{-1}P) = (IP^{-1})P$, $P \neq I$ a $IP^{-1} \subseteq PP^{-1}$ plyne, že IP^{-1} je vlastní ideál R. Současně I je vlastní ideál R, podle lemmatu III.4.3. Protože I bylo voleno jako maximální co do nemožnosti vyjádření součinem prvoideálů, musí být $IP^{-1} = P_1 \dots P_r$ pro vhodné prvoideály $P_1, \dots, P_r$. To ale vede ke sporu, neboť pak $I = IR = (IP^{-1})P = P_1 \cdots P_r P$.

Zbývá dokázat jednoznačnost dekompozice. Ať $I = P_1 \cdots P_r = Q_1 \cdots Q_s$. Budeme postupovat indukcí dle $r + s \geq 2$. Protože $Q_1 \cdots Q_s \subseteq P_1$, musí být $Q_j \subseteq P_1$ pro nějaké j, $1 \leq j \leq s$, neboť P_1 je prvoideál. Odsud $Q_j = P_1$ a lze předpokládat $j = 1$. Položme $P = Q_1 = P_1$, a dále ať $P' = P_2 \dots P_r$ pro $r \geq 2$ an $P' = R$ pro $r = 1$. Podobně budiž $Q' = Q_2 \dots Q_s$, je-li $s \geq 2$, a $Q' = R$ je-li $s = 1$. Pak $P' = RP' = P^{-1}(PP') = P^{-1}(PQ') = Q'$, takže lze použít indukční předpoklad. □

Ať je i nadále R Dedekindův obor integrity a ať je T jeho podílové těleso. *Lomeným ideálem* T se rozumí každý nenulový konečně generovaný R–podmodul T.

III.4.5 Lemma. *Nenulový R–podmodul A tělesa T je lomeným ideálem právě když existuje $c \in R$, $c \neq 0$, takové, že cA je ideál R.*

Důkaz. Jsou-li p_1/q_1, ..., p_k/q_k generátory R–modulu $A \subseteq T$, je $q_1 \cdots q_k A$ rovněž R–modul. Všechny prvky tohoto R–modulu padnou do R, takže jde o ideál R.

Je-li naopak cA ideál R, tak je cA konečně generovaný R–modul (to plyne z toho, že R je noetherovský). Zobrazení $a \mapsto ca$ je isomorfismus R–modulů A a cA, a proto je i A konečně generovaný. □

Nenulovým ideálům R se říká, jsou-li pojednávány souběžně s lomenými ideály, také ideály *celistvé*. Jsou-li A a B celistvé ideály, je $AB = \{\sum r_i a_i b_i;\ r_i \in R,\ a_i \in A \text{ a } b_i \in B\}$ rovněž celistvý ideál. Všechny celistvé ideály tvoří komutativní monoid, který má za podmonoid množinu všech hlavních celistvých ideálů.

Při stejné definici součinu je AB lomený ideál, pokud A i B jsou lomené ideály. Lomené ideály proto tvoří komutativní monoid, přičemž celistvé ideály jsou jeho podmonoid. Jednotkou je opět R.

Pokud A je nenulový R–podmodul T, tak je i $A^{-1} = (R :_T A) = \{b \in T;\ bA \subseteq R\}$ podmodulem T. Pro každé $a \in A$ je $aA^{-1} \subseteq R$, takže A^{-1} je podle III.4.5 lomeným ideálem. Současně máme $AA^{-1} \subseteq R$, takže k důkazu následujícího tvrzení stačí ověřit opačnou inkluzi.

III.4.6 Tvrzení. *Ať T je podílové těleso Dedekindova oboru integrity R. Potom je monoid $\mathcal{I}_T$ všech lomených ideálů T grupa.*

Důkaz. Požadované vlastnosti A^{-1} dokážeme postupně pro $A = P$ celistvý prvoideál, pro $A = P_1 \cdots P_k$ celistvý ideál, který je součinem prvoideálů P_1, ..., P_k, a konečně pro A obecný lomený ideál, kde cA je celistvý pro nějaké $c \in R$, $c \neq 0$.

Je-li $A = P$, je $P^{-1}P = R$, neboť $P^{-1}P$ je ideál R, který obsahuje maximální ideál P jako vlastní podmnožinu (viz lemma III.4.3). Je-li $A = P_1 \cdots P_k$, tak je $B = P_1^{-1} \cdots P_k^{-1}$ inverzní prvek A. To znamená, že je $BA = R$, a proto je $B \subseteq A^{-1}$, takže stačí ukázat $A^{-1} \subseteq B$. Pro $b \in A^{-1}$ máme $bA \subseteq R$, odkud $bAB \subseteq RB = B$. Jelikož $AB = R$, dostaneme $b \in B$, jak třeba.

Ať je nyní A obecný lomený ideál, $cA \subseteq R$. Pak $(cA)^{-1} = \{b \in T;\ bcA \subseteq R\} = c^{-1}\{b \in T;\ bA \subseteq R\} = c^{-1}A^{-1}$, takže $(cA)^{-1}cA = R$ dává $(c^{-1}A^{-1})(cA)$ $= A^{-1}A = R$. □

Pro $a \in R$ nenulové, je $(aR)^{-1} = a^{-1}R$. To znamená, že pro $b/c \in T$, kde $b, c \in R$, máme $(b/c)R = (bR)/(cR)$. *Hlavní lomené ideály* aR, $a \in T^*$, *jsou tedy* v $\mathcal{I}_R$ rovny podílům hlavních celistvých ideálů.

Je-li A obecný lomený ideál, tak pro nějaké $c \in R$ je cA celistvý ideál, takže z $cA = (cR)A$ plyne, že každý lomený ideál je roven podílu dvou celistvých, přičemž za jmenovatel lze vždy zvolit ideál hlavní.

III.4.7 Tvrzení. *Každý lomený ideál lze až na pořadí jednoznačně vyjádřit jako součin* $P_1^{r_1} \cdots P_k^{r_k}$, *kde* P_i *je prvoideál a* $r_i \neq 0$, $1 \leq i \leq k$, *přičemž pro* $1 \leq i < j \leq k$ *platí* $P_i \neq P_j$.

Důkaz. Pokud bude $P_1^{r_1} \cdots P_k^{r_k} = P_1^{s_1} \cdots P_k^{s_k}$, tak převedením záporných exponentů na druhou stranu rovnice dostaneme dvě různá vyjádření celistvého ideálu. Jednoznačnost jeho vyjádření plyne z věty III.4.4, takže musí být $r_1 = s_1$, $\ldots$, $r_k = s_k$. □

III.4.8 Důsledek. *Grupa* $\mathcal{I}_T$ *je isomorfní volné abelovské grupě s bází tvořenou všemi prvoideály.* □

Množinu všech hlavních lomených ideálů označíme $\mathcal{P}_T$ (principal fractional ideals). Je to podgrupa $\mathcal{I}_T$, která je zjevně izomorfní grupě T^*/R^*. Kvocient $\mathcal{C}l_T = \mathcal{I}_T/\mathcal{P}_T$ se nazývá *třídová grupa* (class group).

Pro hlavní lomené ideály máme $aR = R$ právě když a je invertibilní prvek R, tedy $a \in R^*$. Přirozeným způsobem tudíž dostáváme exaktní posloupnost

$$1 \to R^* \to T^* \to \mathcal{I}_T \to \mathcal{C}l_T \to 1.$$

Popsat strukturu $\mathcal{C}l_T$ nějakým obecným způsobem se nezdá být možné. Rovnost $\mathcal{C}l_T = 1$ nastává právě když každý lomený ideál T je hlavní, tedy právě když každý ideál R je hlavní. Jinými slovy, $\mathcal{C}l_T = 1$ právě když je R obor integrity.

Je-li T číselné těleso a R obor integrity všech algebraických celých čísel obsažených v T, je T generováno R (existuje celistvá báze), takže ho lze ztotožnit s podílovým tělesem R. V takovém případě je třídová grupa vždy konečná. Důkaz tohoto faktu se opírá o tzv. Minkowského teorii, které se též říká „geometrie čísel“.

III.5 Mříže

Ať V značí reálný vektorový prostor konečné dimenze n. Podgrupu L Abelovy grupy $V(+,-,0)$ nazveme *mříží*, pokud existují $e_1,\dots,e_m \in V$ lineárně nezávislé a takové, že

$$L = \left\{ \sum k_i e_i;\ k_i \in \mathbb{Z},\ \text{kde } 1 \leq i \leq m \right\}.$$

Mříž se nazývá *úplná*, je-li $n = m$. Množina $\{e_1,\dots,e_m\}$ není určena jednoznačně, ale číslo m je grupou L jednoznačně dáno. Je rovno jednak dimenzi podprostoru, který generuje L, jednak velikosti volné báze volné Abelovy grupy, kterou L je.

Základní buňkou mříže (vůči bázi $e_1,\dots,e_m$) nazveme množinu

$$\left\{ \sum \lambda_i e_i;\ 0 \leq \lambda_i < 1,\ \text{kde } 1 \leq i \leq m \right\}.$$

(V angličtině se tato množina nazývá „fundamental mesh“. Zvolený překlad prozrazuje bezradnost, jak naložit se slovem „mesh“. Toto slovo se zdá v našem kontextu odkazovat na význam „prázdný prostor uvnitř drátěné konstrukce“, čili na něco jako je naše pytlácké oko.)

Topologie V přenesená z euklidovského prostoru $\mathbb{R}^n$ není závislá na volbě báze V. Vektorový prostor V můžeme proto v dalším považovat za topologický prostor. Podgrupa D Abelovy grupy $V(+,-,0)$ se nazývá *diskrétní*, je-li její každý bod izolovaný (má okolí, ve kterém není žádný další prvek D).

III.5.1 Lemma. *Diskrétní podgrupa D vektorového prostoru V tvoří uzavřenou podmnožinu V.*

Důkaz. Předpokládejme, že existuje $x \in V \setminus D$, jež leží v uzávěru D. Dokážeme, že každé okolí U bodu 0 (který samozřejmě v D leží) obsahuje nějaký nenulový prvek D.

Pro U zvolme $U' \subset U$ tak, aby z $a, b \in U'$ vždy plynulo $a - b \in U$. Dále vybereme $x_1, x_2 \in (x + U') \cap D$, $x_1 \neq x_2$. Pak $x_1 - x_2 \in D$ a současně

$$x_1 - x_2 = (x_1 - x) - (x_2 - x) \in U.$$

□

III.5.2 Tvrzení. *Nechť V je konečně rozměrný reálný vektorový prostor. Podgrupa $V(+,-,0)$ je diskrétní právě když je ve V mříží.*

Důkaz. Je zřejmé, že každá mříž je diskrétní podgrupou V. Uvažme naopak nějakou diskrétní podgrupu D Abelovy grupy $V(+,-,0)$ a vybereme $e_1,\dots,e_m \in D$ takové, že jde o vektory lineárně nezávislé, přičemž m je maximální možné. Podgrupa $L \subseteq D$ generovaná těmito vektory je mříží. Ať B označuje její základní buňku vůči $e_1,\dots,e_m$. Pro každé $d \in D$ zvolme $a_d \in L$ a $b_d \in B$, že $d = a_d + b_d$. Taková a_d a b_d musí existovat, neboť D leží ve vektorovém prostoru, který generují $e_1,\dots,e_m$. Máme $b_d = d - a_d \in B \cap D$ pro každé

$d \in D$ a množina $S = \{b_d;\ d \in D\}$ je podle lemmatu III.5.1 bez hromadného bodu. Protože S leží uvnitř kompaktní množiny, musí S být množina konečná. Máme $D = L + S$, takže index $|D : L| = q$ je konečný. Grupa D je proto konečné generovaná a má nějakou volnou bázi $f_1, \ldots, f_r$. Podgrupa grupy D generovaná $qf_1, \ldots, qf_r$ je rovněž volná hodnosti r, takže z $qD \subseteq L$ dostáváme $r \leq m$. Rovnost $r = m$ pak plyne z toho, že r musí být rovno alespoň dimenzi vektorového podprostoru, který D generuje. Dokázali jsme, že r je rovno dimenzi tohoto podprostoru, a proto jsou $f_1, \ldots, f_r$ nutně vektory lineárně nezávislé. Grupa D je vskutku mříží. □

III.5.3 Lemma. *Ať L je mříží ve V. Mříž L je úplná právě když lze nalézt omezenou množinu $B \subseteq V$ takovou, že $V = \bigcup(a + B;\ a \in L)$.*

Důkaz. Ať L je mříž, generovaná lineárně nezávislou množinou $e_1, \ldots, e_m \in V$. Je-li $n = m = \dim V$, lze za B zvolit základní buňku L. Předpokládejme tedy naopak, že existuje B omezené takové, že množiny $a + B$ pokrývají celé V.

Zvolme nějaké $x \in V$. Cílem bude ukázat, že x leží ve vektorovém podprostoru generovaném $e_1, \ldots, e_m$. Tento podprostor označíme U. Je to uzavřená podmnožina V, a ke každému ix, $i \geq 1$ celé, lze nalézt $a_i \in U$ a $b_i \in B$ taková, že $ix = a_i + b_i$. Tudíž $x = i^{-1}a_i + i^{-1}b_i$ a limita posloupnosti $i^{-1}b_i$ je rovna nule, neboť $b_i \in B$ a B je omezená množina. Tím pádem je x roven limitě posloupnosti $i^{-1}a_i$. Každý prvek posloupnosti leží v U, takže z uzavřenosti U vyplývá $x \in U$. □

Každá báze $e = \{e_1, \ldots, e_n\}$ vektorového prostoru V poskytuje positivně definitní bilineární formu $\langle u, v\rangle = \sum \alpha_i\beta_i$, kde $u = \sum \alpha_i e_i$ a $v = \sum \beta_i e_i$. Ztotožnění $u = \sum \alpha_i e_i$ s $(\alpha_1, \ldots, \alpha_n) \in \mathbb{R}^n$ dovoluje tuto bilineární formu chápat jako standardní skalární součin. Podobně můžeme skrze toto ztotožnění přenést na V Lebesgueovu míru. Budeme ji značit vol_e nebo jen vol.

Je známo, že pro rovnoběžnostěn A s vrcholy $a_{i_1} + a_{i_2} + \cdots + a_{i_k}$, kde pro daná $a_1, \ldots, a_n \in V$ probíhá $i_1, \ldots, i_k$ všechny celočíselné posloupnosti, jež splňují $1 \leq i_1 < \cdots < i_k \leq n$, platí

$$vol(A) = |\det(\langle a_i, a_j\rangle)|^{1/2} = |\det(a_{ij})|,$$

kde $a_j = \sum a_{ij}e_i$ (označíme-li totiž matici (a_{ij}) jako P a matici $(\langle a_i, a_j\rangle)$ jako S, tak platí $S = P^T P$).

Je-li $a = \{a_1, a_2, \ldots, a_n\}$ báze, tak pro každou $M \subseteq V$ měřitelnou platí $vol_a(M) = vol(A)^{-1} vol(M)$. Budeme-li porovnávat $vol(M_1)$ a $vol(M_2)$, kde M_1 i M_2 jsou měřitelné množiny, není nutné specifikovat volbu báze e, neboť při jiné volbě se $vol(M_1)$ i $vol(M_2)$ mění o týž lineární faktor. (V tomto smyslu je třeba chápat znění obou níže uvedených tvrzení.)

III.5.4 Lemma. *Ať L je úplná mříž ve V a ať $a = \{a_1, \ldots, a_n\}$ a $b = \{b_1, \ldots, b_n\}$ jsou dvě takové báze, že $L = \{\sum k_i a_i;\ k_i \in \mathbb{Z}\} = \{\sum k_i b_i;\ k_i \in Z\}$. Označme po řadě A a B základní buňky L vůči bázím a a b. Potom $vol(A) = vol(B)$.*

Důkaz. Buď T přechodová matice od a k b, a ať S je přechodová matice od b k a. Protože a i b poskytují mříž L, musí být obě matice celočíselné. Současně je $ST = TS = I_n$, takže $|\det S| = |\det T| = 1$, a tedy $vol_a(M) = vol_b(M)$ pro každé měřitelné M. Speciálně $1 = vol_a(A) = vol_b(B) = vol_a(B)$. Zbytek je zřejmý. $\square$

Společná hodnota $vol(A)$ a $vol(B)$ se obvykle označuje $vol(L)$.

V dalším použijeme též fakt, že konvexní množiny jsou měřitelné. O $M \subseteq V$ řekneme, že je to množina *středově souměrná*, pokud pro každé $x \in M$ platí $-x \in M$.

III.5.5 Věta (Minkowského o mřížovém bodě). *Ať L je úplná mříž v reálném vektorovém prostoru dimenze n. Potom každá středově souměrná konvexní množina $M \subseteq V$, která splňuje*

$$vol(M) > 2^n vol(L),$$

obsahuje alespoň jeden nenulový mřížový bod.

Důkaz. Budeme dokazovat, že z $vol(M) > 2^n vol(L)$ plyne existence $x_1, x_2 \in L$ takových, že $(x_1 + 1/2M) \cap (x_2 + 1/2M) \neq 0$ a $x_1 \neq x_2$.

Předpokládejme opak a ať A je základní buňka L. Množiny $A \cap (x + (1/2)M)$, $x \in L$, jsou tedy po dvou disjunktní, takže $vol(L) \geq \sum_{x \in L} vol(A \cap (x + 1/2M))$. Posunutím o $-x$ přejde $A \cap (x + (1/2)M)$ na $(A - x) \cap (1/2)M$; tyto množiny mají stejnou velikost. Platí totiž $V = \bigcup(x + A;\ x \in L) = \bigcup(A - x;\ x \in L)$. S ohledem na $\bigcup((A - x) \cap (1/2)M;\ x \in L) = (1/2)M$ tedy máme $vol(L) \geq \sum vol((A - x) \cap (1/2)M) \geq vol((1/2)M) = 1/2^n vol(M)$, což je spor.

Ať tedy $x_1 + (1/2)y_1 = x_2 + 1/2(y_2)$, kde $x_1 \neq x_2$, a $y_1, y_2 \in M$. Pak $y = x_1 - x_2 = (1/2)y_2 - (1/2)y_1$ leží ve středu úsečky spojující y_2 a $-y_1$, takže je $y \in M$. Současně $y = x_1 - x_2 \in L$. $\square$

III.6 Rozšíření Dedekindových oborů

III.6.1 Lemma. *Ať R je Dedekindův obor a ať P je prvoideál R. Potom je R/P těleso a pro každé $i \geq 0$ je P^i/P^{i+1} vektorovým prostorem nad R/P, jehož dimenze je rovna jedné.*

Důkaz. Vyjdeme z toho, že P^i/P^{i+1} je R–modul. Protože $P \cdot P^{i+1} = P^{i+1}$, tak je tento modul možno chápat jako (R/P)–modul. Přitom R/P je komutativní těleso, neboť P je maximální ideál.

Podle III.4.4 máme $P^i \neq P^{i+1}$. Zvolme $\alpha \in P^i \setminus P^{i+1}$ a položme $A = \alpha R + P^{i+1}$. Naším cílem je ukázat $A = P^i$. Předpokládejme $P^{i+1} \subsetneq A \subsetneq P^i$ a vynásobme všechny ideály tohoto řetězce lomeným ideálem P^{-i}. Podle tvrzení III.4.6 je $P \subsetneq A \cdot P^{-i} \subsetneq R$. Lomený ideál, který leží v R, je (celistvým) ideálem R. Obdrželi jsme spor s maximalitou P. □

V kapitole III.4 jsme dokázali, že $\mathbb{Z}_K$ je Dedekindův obor pro každé číselné těleso K. Úvahy v důkazu použité lze zobecnit na případ, kdy R je Dedekindův obor (potom je R, mimo jiné, celistvě uzavřené ve svém podílovém tělese T), U je separabilní rozšíření T konečného stupně a S je celistvý uzávěr R v U. Uvidíme, že pak je i S Dedekindův obor. Tak tomu je dokonce i v případě, kdy se nepředpokládá separabilita U nad T; to však zde dokazovat nebudeme.

Označení R, S, T a U budeme v uvedeném významu používat i nadále. Hlavním cílem této kapitoly ovšem není důkaz toho, že S je Dedekindův obor, nýbrž vztahy prvoideálů $\mathsf{p} \subseteq R$ a prvoideálů $\mathsf{P} \subseteq S$, které p obsahují. Dosažené výsledky se samozřejmě aplikují zejména na případy $R = \mathbb{Z}$ a $S = \mathbb{Z}_K$. Pro správné uchopení vztahů logické závislosti se však zdá být vhodné je dokázat v odpovídajícím stupni obecnosti.

III.6.2 Lemma. *Okruh S je noetherovský R–modul. Pro každé $\alpha \in U$ lze nalézt nenulové $r \in R$ takové, že $r\alpha \in S$.*

Důkaz. Existence $r \in R$ je dokázána v úvahách před tvrzením III.3.4, přičemž z tvrzení III.3.4 vyplývá, že $S \subseteq (R\alpha_1 + \cdots R\alpha_n)d^{-1} = R(d^{-1}\alpha_1) + \cdots + R(d^{-1}\alpha_n)$, kde $\alpha_1, \ldots, \alpha_n \in S$ tvoří nějakou bázi U nad T a $d = \triangle(\alpha_1, \ldots, \alpha_n)$ je diskriminant. Vidíme, že S je podmodul konečně generovaného (a tedy noetherovského) R–modulu, a proto běží rovněž o noetherovský R–modul. □

III.6.3 Lemma. *Celistvý uzávěr S Dedekindova oboru R v tělese U, které je separabilním rozšířením konečného stupně podílového tělesa T oboru R, je rovněž Dedekindův obor.*

Důkaz. Z lemmatu III.6.2 vidíme, že U je možné považovat za podílové těleso S a že S je noetherovský okruh. Z důsledku III.2.8 plyne, že S je rovné svému celistvému uzávěru v U. Proto je S v U celistvé uzavřené. Zbývá dokázat, že nenulové prvoideály jsou maximální.

Ať je tedy P nenulový prvoideál S, a ať $\mathsf{p} = \mathsf{P} \cap R$. Z Zornova lemmatu plyne existence $\mathsf{J} \supseteq \mathsf{P}$, J maximální ideál S. Naším cílem je dokázat $\mathsf{J} = \mathsf{P}$, tedy dovést ke sporu existenci $\alpha \in \mathsf{J} \setminus \mathsf{P}$.

Víme, že $\mathsf{J} \cap R$ je provideál R, takže $\mathsf{J} \cap R = \mathsf{p}$. Indukcí dle m dokážeme, že pro každý polynom $\sum r_i x^{m-i} \in R[x]$ stupně m z $\gamma = \sum r_i \alpha^{m-i} \in \mathsf{P}$ plyne $r_i \in \mathsf{p}$, $0 \leq i \leq m$. Případ $m = 0$ je zřejmý, budiž $m \geq 1$ a uvažme $\gamma - r_m = \alpha(\sum r_i \alpha^{m-1-i}) \in \mathsf{J}$. Máme $r_m = \gamma - (\gamma - rm) \in \mathsf{J} \cap R = \mathsf{p}$, takže $\gamma - r_m \in \mathsf{P}$ a z $\alpha \notin \mathsf{P}$ plyne $\sum r_i \alpha^{m-1-i} \in \mathsf{P}$, $0 \leq i \leq m-1$. Podle indukčního předpokladu padnou všechna r_i do p. Tím je indukce dokončena a kýžený spor obdržíme, zvolíme-li za $\sum r_i x^{m-i}$ minimální polynom s kořenem α. Ten je totiž monický a 1 nepatří do p. $\square$

Poznamenejme, že separabilita U nad T byla potřebná v důkaze lemmatu III.6.2, a to díky použití tvrzení III.3.4.

III.6.4 Lemma. *Ať* p *je nenulový prvoideál* R*. Potom je* $\mathsf{p}S$ *vlastní ideál* S *a pro prvoideál* P *okruhu* S *platí* $\mathsf{p} = \mathsf{P} \cap R$ *právě když se* P *vyskytuje v rozkladu* $\mathsf{p}S$ *na součin kladných mocnin prvoideálů.*

Důkaz. Zvolme $x \in \mathsf{p} \setminus \mathsf{p}^2$. Pak $xR = \mathsf{pa}$ pro nějaký (ne nutně vlastní) ideál a okruhu R, který nepadne do p. Proto $R = \mathsf{p} + \mathsf{a}$, takže $1 = b + a$ pro nějaká $b \in \mathsf{p}$ a $a \in \mathsf{a}$. Máme $a \notin \mathsf{p}$ a $a\mathsf{p} \subseteq \mathsf{ap} = xR$.

Předpokládejme nyní $\mathsf{p}S = S$. Potom je $aS = a\mathsf{p}S \subseteq xS$, takže $a = xy$ pro nějaké $y \in S$. Z $a, x \in R \subseteq T$ plyne $y = ax^{-1} \in T \cap S = R$. Z $x \in \mathsf{p}$ a $y \in R$ máme $a \in \mathsf{p}$, což je spor. Vidíme, že $\mathsf{p}S$ je vlastní ideál S.

V rozkladu $\mathsf{p}S$ na kladné mocniny prvoideálů se P vyskytuje právě když $\mathsf{p}S \subseteq \mathsf{P}$, což dává $\mathsf{p} \subseteq R \cap \mathsf{P}$. Ovšem $\mathsf{p} \subseteq R \cap \mathsf{P}$ právě když $\mathsf{p} = R \cap \mathsf{P}$, neboť $R \cap \mathsf{P}$ je prvoideál R. Z $\mathsf{p} = R \cap \mathsf{P}$ naopak samozřejmě plyne $\mathsf{p}S \subseteq \mathsf{P}$. $\square$

Prvoideál p okruhu R se často ztotožňuje s ideálem $\mathsf{p}S$ okruhu S. Je-li $\mathsf{p}S = \mathsf{P}_1^{e_1} \dots \mathsf{P}_r^{e_r}$ a $\mathsf{P} = \mathsf{P}_i$, $1 \leq i \leq r$, nazývá se e_i *ramifikačním indexem* (ukazatelem větvení) prvoideálu P.

Stupeň inertnosti (nehybnosti) P nad p se definuje jako stupeň rozšíření tělesa R/p tělesem S/P. (Přitom R/p chápeme jako podtěleso S/P ztotožněním $R/\mathsf{p} = R/R \cap \mathsf{P}$ s $R\mathsf{P}/\mathsf{P}$.)

Je-li $\mathsf{p} = \mathsf{P}_1^{e_1} \dots \mathsf{P}_r^{e_r}$, tak se pro označení stupně inertnosti P_i nad p používá f_i.

III.6.5 Tvrzení. *Pro každý nenulový prvoideál* p *okruhu* R *platí (takzvaná) fundamentální rovnost*

$$\sum e_i f_i = n = [U : T].$$

Důkaz. Z čínské věty o zbytcích máme $S/\mathsf{p}S \cong \oplus S/\mathsf{P}_i^{e_i}$, přičemž z $\mathsf{p} \subseteq \mathsf{p}S$ plyne, že tento isomorfismus lze chápat i jako isomorfismus vektorových prostorů nad tělesem $F = R/\mathsf{p}$.

Chápeme-li $S/\mathsf{P}_i^{e_i}$ jako vektorový prostor nad S/P_i, je jeho dimenze dle lemmatu III.6.1 rovna e_i. Dimenze $S/\mathsf{P}_i^{e_i}$ nad F je proto rovna $e_i f_i$ a vidíme, že fundamentální rovnost obdržíme srovnáním dimenzí na obou stranách isomorfismu, pokud ověříme, že $S/\mathsf{p}S$ má jako vektorový prostor nad F dimenzi n. Vybereme $\omega_1, \dots, \omega_m \in S$ taková, že $\omega_1 + \mathsf{p}S, \dots, \omega_m + \mathsf{p}S$ je báze $S/\mathsf{p}S$, a budeme dokazovat, že $\omega_1, \dots, \omega_m$ je nutně bází U nad T.

Předpokládejme nejprve, že $\omega_1, \ldots, \omega_m$ jsou nad T lineárně závislé. Pak podle lemmatu III.6.2 existují $r_1, \ldots, r_m \in R$ taková, že $\sum r_i \omega_i = 0$ a ideál I okruhu R generovaný $r_1, \ldots . r_m$ je nenulový. Zvolme $\rho \in I^{-1} \setminus I^{-1}p$. Pak $\rho r_1, \ldots, \rho r_m$ leží v R a generují ideál ρI, který neleží v p (z $\rho I \subseteq \mathsf{p}$ bychom měli $\rho \in \mathsf{p}I^{-1}$). To znamená, že alespoň jedno ρr_i nepadne do p, takže poskytuje nenulový koeficient vůči $F = R/\mathsf{p}$, a to je spor s volbou $\omega_1, \ldots, \omega_m$.

Uvažme nyní R–modul $M = R\omega_1 + \cdots + R\omega_m$. Podle lemmatu III.6.2 stačí ukázat $M \supseteq dS$ pro nějaké nenulové $d \in R$, neboť každé $\alpha \in U$ lze pak získat jako podíl prvku z dS a prvku z R. Inkluzi $M \supseteq dS$ budeme dokazovat ve formě $d(S/M) = 0$. Podle lemmatu III.6.2 je S, a tím pádem i S/M, noetherovský R–modul. Prvky $\omega_1, \ldots, \omega_m$ generují S modulo $\mathsf{p}S$, takže $S = M + \mathsf{p}S$ a $\mathsf{p}(S/M) = S/M$.

Ať je $\beta_1, \ldots, \beta_q$ nějaký systém generátorů S/M. Pak existuje $q \times q$ matice (p_{ij}) prvků z p taková, že $\beta_i = \sum_j p_{ij}\beta_j$. Označme B matici $(p_{ij}) - I_q$ a položme $d = \det B$. Počítáno modulo p je d rovno $(-1)^q$, a proto je $d \neq 0$. Označme A adjunkt matice B. Podle tvrzení III.1.5 je $AB = dI_q$. Současně ale $B(\beta_1, \ldots, \beta_q)^{\mathrm{T}} = 0$, takže $d\beta_1 = \cdots = d\beta_q = 0$, a tím pádem $d(S/M) = 0$. $\square$

Poznamenejme, že použitá závěrečná úvaha používá argumentaci, kterou lze použít i při důkazu Nakayamova lemmatu.

Je-li X podokruh komutativního okruhu Y, je $\{y \in Y;\ yY \subseteq X\} = (X : Y)$ ideál Y, který je obsažen v X. Každý ideál Y obsažený v X zjevně v $(X : Y)$ leží, takže $(X : Y)$ je největším ideálem Y, který je v X obsažen. V číselněteoretickém kontextu se mu říká *průvodič* (conductor) X. Uvidíme, že v mnoha důležitých situacích je průvodič ideál nenulový.

Uvědomme si, že pokud je Y generován jako X–modul prvky $y_1, \ldots, y_n$, tak je $(X : Y)$ rovno $\bigcap (X : y_i)$, $1 \leq i \leq n$, kde $(X : y_i) = \{y \in Y;\ yy_i \in X\}$.

III.6.6 Lemma. *Ať X je podokruh S, který obsahuje R, a ať $\alpha_1, \ldots, \alpha_n \in X$ tvoří bázi U nad T. Potom je průvodič $(X : S)$ nenulový.*

Důkaz. Dokážeme nenulovost $R \cap (X : S) = (X :_R S)$, což je ideál R rovný $\bigcap (X :_R \omega_j)$, $1 \leq j \leq m$, kde $\{\omega_1, \ldots, \omega_m\}$ je nějaká množina generátorů S chápaného jako R–modul (viz lemma III.6.2). Protože pro každé $\omega \in S$ je $(X :_R \omega) = \{r \in R;\ r\omega \in X\}$ ideálem R, stačí dokázat, že tento ideál je pro každé $\omega \in S$ nenulový. To ovšem snadno odvodíme úvahou o lineární závislosti množiny $\{\alpha_1, \ldots, \alpha_n, \omega\}$, z níž vyplývá existence $r_i \in R$, $1 \leq i \leq n$, a $r \in R$, $r \neq 0$, takových, že $r\omega = \sum r_i \alpha_i \in X$. $\square$

III.6.7 Lemma. *Ať $I = \mathsf{P}_1^{e_1} \ldots \mathsf{P}_k^{e_k}$ je ideál S, kde P_i jsou prvoideály a $e_i \geq 1$, $1 \leq i \leq k$, a ať p je prvoideál R. Pak $I \cap R \subseteq \mathsf{p}$ právě když $\mathsf{p} = \mathsf{P}_i \cap R$ pro některé i, $1 \leq i \leq k$.*

Důkaz. Z $I = \mathsf{P}_1^{e_1} \ldots \mathsf{P}_k^{e_k}$ plyne $I \cap R = \bigcap (\mathsf{P}_i^{e_i} \cap R;\ 1 \leq i \leq k)$, takže jistě $I \cap R \subseteq \mathsf{P}_i \cap R$. Protože $\mathsf{P}_i \cap R \supseteq \mathsf{P}_i^{e_i} \cap R \supseteq (\mathsf{P}_i \cap R)^{e_i}$, musí existovat e_i', $1 \leq e_i' \leq e_i$, taková, že $\mathsf{P}_i^{e_i} \cap R = (\mathsf{P}_i \cap R)^{e_i'}$. Vidíme, že $I \cap R$ je součinem mocnin prvoideálů $\mathsf{P}_i \cap R$, $1 \leq i \leq k$. $\square$

III.6.8 Důsledek. *Ať I je ideál S a ať p je nenulový prvoideál R. Jsou-li ideály I a $\mathsf{p}S$ nesoudělné (tj. $I + \mathsf{p}S = S$), jsou nesoudělné i ideály $I \cap R$ a p (tj. $I \cap R + \mathsf{p} = R$).*

Důkaz. Ať $\mathsf{P}_1, \ldots, \mathsf{P}_k$ jsou jako v lemmatu III.6.7. Podle něj nesoudělnost $I \cap R$ a p znamená, že je $\mathsf{p} \neq \mathsf{P}_i \cap R$, $1 \leq i \leq k$. Ovšem kdyby některá z těchto rovností nastala, bylo by jak $I \subseteq \mathsf{P}_i$, tak $\mathsf{p}S \subseteq \mathsf{P}_i$, dle lemmatu III.6.4. $\square$

IV Minkowského teorie

IV.1 Číselná tělesa

V této kapitole připomeneme některé poznatky z předchozích částí, které se týkají číselných těles.

Připomeňme, že komutativní těleso K se nazývá *číselným tělesem*, je-li charakteristiky nula a je-li konečného stupně nad svým prvotělesem. Tato definice je alternativou vůči definici v kapitole III.3, neboť prvotěleso K je isomorfní $\mathbb{Q}$, takže K lze považovat za mezitěleso $\mathbb{Q} \leq K < \mathbb{C}$, $[K : \mathbb{Q}] < \infty$.

Všechny prvky K jsou algebraická komplexní čísla, přičemž ta z nich, která jsou algebraická celá (jsou kořenem monického celočíselného polynomu), tvoří celistvý uzávěr $\mathbb{Z}$ v K; značíme ho $\mathbb{Z}_K$.

Připomeňme, že obecně se diskriminant v konečném separabilním rozšíření $U|T$ s bází $\alpha_1, \ldots, \alpha_n$ definuje jako determinant matice $(\mathrm{Tr}_{U|T}(\alpha_i\alpha_j))$ a že ho alternativně lze obdržet jako čtverec determinantu matice $(g_i(\alpha_j))$, kde $g_1, \ldots, g_n$ jsou všechny T–homomorfismy $U \to \bar{U}$ (viz II.5.5). Přitom z tvrzení II.5.6 víme, že hodnota diskriminantu je vždy nenulová.

V číselných tělesech je význam diskriminantu umocněn tím, že v jistém smyslu nezávisí na výběru báze. To vyplývá z věty III.3.8 a z úvah, které za ní následují. Připomeneme je.

Okruh $\mathbb{Z}_K$ je jako Abelova grupa konečně generovaný, proto je konečně generovanou Abelovou grupou i každý jeho ideál (takže $\mathbb{Z}_K$ je noetherovský okruh). Volná báze $\mathbb{Z}_K$ jakožto $\mathbb{Z}$–modulu (tedy jako Abelovy grupy) se nazývá *celistvá báze*. Každý prvek K má celočíselný násobek, který padne do $\mathbb{Z}_K$. Proto je velikost číselné báze nutně rovna $n = [K : \mathbb{Q}]$. Z úvah o determinantu přechodových matic (tvrzení II.5.6) pak vyplývá, že hodnota diskriminantu $\triangle(\mathbb{Z}_K)$ na volbě celistvé báze nezávisí.

Je-li I nenulový ideál, tak je velikost jeho celistvé báze rovněž $n = [K : \mathbb{Q}]$. Důvod je přímočarý: zobrazení $x \mapsto cx$ je pro každé $c \in \mathbb{Z}_K$, $c \neq 0$, isomorfismus $\mathbb{Z}_K$ a hlavního ideálu $c\mathbb{Z}_K$. Hodnost nenulového ideálu I (jakožto Abelovy grupy) je tedy uzavřena mezi shodnými hodnostmi $c\mathbb{Z}_K$ a $\mathbb{Z}_K$, kde $c\mathbb{Z}_K \subseteq I$.

Pro ideál I platí stejné úvahy o determinantu přechodové matice, a proto je velikost jeho diskriminantu nezávislá na volbě celistvé báze. Píšeme $\triangle(I)$ a máme

$$\triangle(I) = |\mathbb{Z}_K : I|^2 \triangle(\mathbb{Z}_K),$$

kde význam $|\mathbb{Z}_K : I|$ lze snadno přiblížit, neboť z teorie konečně generovaných Abelových grup plyne, že I má celistvou bázi, jejíž prvky jsou celočíselnými nenulovýni násobky nějaké celistvé báze $\mathbb{Z}_K$.

Protože $\mathbb{Z}_K$ je Dedekindův a protože lomené ideály $\mathbb{Z}_K$ mají podle lemmatu

III.4.5 strukturu volného $\mathbb{Z}$–modulu hodnosti $n = [K : \mathbb{Q}]$, vidíme, že diskriminant $\triangle(I)$ je definován i pro ideály lomené, a že pro $I' \subseteq I$ dva lomené ideály platí

$$\triangle(I') = |I : I'|\triangle(I).$$

Index $|\mathbb{Z}_K : I|$, kde I je ideál okruhu $\mathbb{Z}_K$, se často označuje $\mathcal{N}(I)$ a nazývá *absolutní normou* ideálu I. Důvod této terminologie vyplývá z následujícího tvrzení.

IV.1.1 Lemma. *Ať je I hlavní ideál okruhu $\mathbb{Z}_K$ generovaný prvkem α. Potom*

$$|\mathbb{Z}_K : I| = |N_{K|\mathbb{Q}}(\alpha)|.$$

Důkaz. Uvažme nějakou bázi $e_1, \dots, e_n$ tělesa K nad $\mathbb{Q}$. Podle definice normy je $N_{K|\mathbb{Q}}(\alpha)$ rovno determinantu matice $A = (a_{ij})$, kde $\alpha e_j = \sum_i a_{ij} e_i$. Zvolme $e_1, \dots, e_n$ tak, aby šlo o celistvou bázi $\mathbb{Z}_K$. Sloupcové vektory matice A pak tvoří celistvou bázi ideálu I.

Matici A můžeme chápat jako přechodovou matici od báze $e_1, \dots, e_n$ k bázi $\alpha e_1, \dots, \alpha e_n$. Z věty o podgrupách konečně generované beztorzní abelovské grupy plyne, že výběr celistvé báze $e_1, \dots, e_n$ lze provést také tak, aby $d_1 e_1, \dots, d_n e_n$ byla celistvá báze ideálu I, kde $d_i \geq 1$ jsou celá čísla, $1 \leq i \leq n$.

Matice přechodu mezi dvěma celistvými bázemi ideálu I má determinant rovný ± 1, takže determinant matice A a determinant diagonální matice, která má na digonále hodnoty $d_1, \dots, d_n$, se musí až na znaménko shodovat. Ovšem $d_1 \cdots d_n = |\mathbb{Z}_K : I|$. □

IV.1.2 Tvrzení. *Ať $I = P_1^{r_1} \cdots P_k^{r_k}$ je faktorizace ideálu I okruhu $\mathbb{Z}_K$ na prvoideály. Potom*

$$\mathcal{N}(I) = \mathcal{N}(P_1)^{r_1} \cdots \mathcal{N}(P_k)^{r_k}.$$

Důkaz. Podle čínské věty o zbytcích je $\mathbb{Z}_K/I \cong \mathbb{Z}_K/P_1^{r_1} \oplus \cdots \oplus \mathbb{Z}_K/P_k^{r_k}$, takže $\mathcal{N}(I) = \mathcal{N}(P_1^{r_1}) \cdots \mathcal{N}(P_k^{r_k})$. Stačí tedy ukázat $\mathcal{N}(P^j) = (\mathcal{N}(P))^j$, pro každý prvoideál P a každé $j \geq 1$. Ovšem $\mathcal{N}(P^j) = |\mathbb{Z}_K : P^j| = |\mathbb{Z}_K : P| \cdot |P : P^2| \cdots |P^{j-1} : P^j|$. Podle Lemmatu III.6.1 je $|\mathbb{Z}_K/P| = |P^{i-1}/P^i|$ pro každé $i \geq 1$. □

IV.1.3 Tvrzení. *Pro každou konstantu $C > 0$ platí, že existuje pouze konečně mnoho ideálů I daného okruhu $\mathbb{Z}_K$, jež splňují $\mathcal{N}(I) < C$.*

Důkaz. Z tvrzení IV.1.2 plyne, že stačí dokázat existenci omezeného počtu prvoideálů P, jež splňují $\mathcal{N}(P) < C$. Průnik $P \cap \mathbb{Z}$ je prvoideál $\mathbb{Z}$, a tedy roven $p\mathbb{Z}$ pro nějaké prvočíslo p. Protože $\mathbb{Z}_K/P$ je těleso, musí být $\mathcal{N}(P) = |\mathbb{Z}_K : P|$ rovno nějakému p^f, $f \geq 1$. Stačí tedy pro každé prvočíslo $p < C$ dokázat omezený počet prvoideálů P, jež splňují $P \cap \mathbb{Z} = p\mathbb{Z}$. Tato podmínka je ekvivalentní podmínce $p \in P$, tedy $p\mathbb{Z}_K \subseteq P$. Tu splňují právě ty prvoideály P, jež se vyskytují v prvoideálovém rozkladu $p\mathbb{Z}_K$. Takových prvoideálů je samozřejmě jen konečně mnoho. □

IV.2 Prostor Minkowského

Minkowského přístup, ve kterém se prvky číselného tělesa K stupně n považují za body n–rozměrného prostoru, se často nazývá „geometrie čísel“.

IV.2.1 Lemma. *Ať $D = \{(u,v) \in \mathbb{C} \times \mathbb{C};\ v = \overline{u}\}$ a ať $G\colon D \to \mathbb{R}^2$, $G(u,v) = (a,b)$ pro každé $u = a + ib \in \mathbb{C}$. Pak je G isomorfismus reálných vektorových prostorů a pro $(u_1,v_1),(u_2,v_2) \in D$ je souřadnicový skalární součin $G(u_1,v_1)$ a $G(u_2,v_2)$ roven $(u_1\overline{u}_2 + v_1\overline{v}_2)/2$.*

Důkaz. Prvá část důkazu je zřejmá, druhá je patrná, zapíšeme-li u_1 jako $a_1 + ib_1 = \overline{v}_1$ a u_2 jako $a_2 + ib_2 = \overline{v}_2$. Pak $u_1\overline{u}_2 = (a_1a_2 + b_1b_2) - i(a_1b_2 - a_2b_1)$, zatímco $v_1\overline{v}_2 = (a_1a_2 + b_1b_2) + i(a_1b_2 - a_2b_1)$. □

Definujme nyní $K_{\mathbb{C}}$ jako komplexní vektorový prostor tvořený všemi n–ticemi $(u_g;\ g \in \mathrm{Hom}(K,\mathbb{C}))$. Jeho dimenze je rovna n; pořadí zápisu n–tic však neupravujeme. Množina $\mathrm{Hom}(K,\mathbb{C})$ zde tedy vystupuje jako množina indexů. Využijeme toho, že na této množině je definována involuce $g \mapsto \overline{g}$, kde $\overline{g}(\alpha) = \overline{g(\alpha)}$ pro každé $\alpha \in K$.

Pevné body této involuce jsou *reálné homomorfismy*, neboť zobrazují K do $\mathbb{R}$. Ostatním homomorfismům se říká *komplexní*.

Na $K_{\mathbb{C}}$ uvážíme jednak hermitovský součin $\langle u,v\rangle = \sum u_g\overline{v}_g$, jednak involuci $F : (u_g;\ g \in \mathrm{Hom}(K,\mathbb{C})) \mapsto (\overline{u_{\overline{g}}};\ g \in \mathrm{Hom}(K,\mathbb{C}))$. Zobrazení F tedy mění hodnotu u_g na číslo komplexně sdružené, a získaná hodnota je přiřazena indexu $\overline{g}$.

IV.2.2 Lemma. *Ať $u,v \in K_{\mathbb{C}}$. Pak $\langle F(u),F(v)\rangle = \overline{\langle u,v\rangle}$.*

Důkaz. Uvažme (u_g) a (v_g), kde $g \in \mathrm{Hom}(K,\mathbb{C})$. Pak $\overline{\langle u,v\rangle} = \sum \overline{u}_g v_g = \sum \overline{u_{\overline{g}}} v_{\overline{g}} = \langle F(u),F(v)\rangle$. □

IV.2.3 Důsledek. *Ať $u,v \in K_{\mathbb{C}}$. Z $F(u) = u$ a $F(v) = v$ plyne $\langle v,u\rangle = \langle u,v\rangle \in \mathbb{R}$.*

Komplexní vektorový prostor $K_{\mathbb{C}}$ lze samozřejmě považovat také za reálný vektorový prostor. Zobrazení F je automorfismus tohoto reálného vektorového prostoru, neboť zjevně $F(u+v) = F(u) + F(v)$ a $F(\lambda u) = \lambda F(u)$ pro $u,v \in K_{\mathbb{C}}$ a $\lambda \in \mathbb{R}$. Množina pevných bodů F je tudíž reálný vektorový podprostor $K_{\mathbb{C}}$ a hermitovský součin $\langle\ ,\ \rangle$ indukuje na tomto podprostoru součin skalární, dle důsledku IV.2.3. Označíme ho $K_{\mathbb{R}}$.

Reálný vektorový prostor $K_{\mathbb{R}}$ vybavený popsaným skalárním součinem se nazývá *Minkowského prostor*. Metriku odvozenou od jeho skalárního součinu budeme nazývat metrikou *kanonickou*, a budeme ji značit *vol*.

Prvky $K_{\mathbb{R}}$ jsou tedy ty n–tice $(u_g;\ g \in \mathrm{Hom}(K,\mathbb{C}))$, že $u_{\overline{g}} = \overline{u_g}$. Pro reálný homomorfismus g tento vztah znamená $u_g \in R$.

Počet reálných homomorfismů se obvykle značí r a počet dvojic komplexně sdružených komplexních homomorfismů se obvykle označuje s. Je tedy $n = r + 2s$.

IV.2.4 Tvrzení. *Ať $\Sigma \subseteq \mathrm{Hom}(K, \mathbb{R})$ obsahuje všech r reálných homomorfismů a ať z každé z s dvojic komplexně sdružených homomorfismů obsahuje právě jeden homomorfismus. Definujme $G: K_{\mathbb{R}} \to \mathbb{R}^{r+2s}$, $(u_g) \mapsto (a_g)$ tak, že $a_g = u_g$ pro $g \in \Sigma$ reálné a $(a_g, a_{\overline{g}}) = (\mathrm{Re}(u_g), \mathrm{Im}(u_g))$ pro $g \in \Sigma$ komplexní.*

Položme $\tau_g = 1$ pro reálné $g \in \mathrm{Hom}(K, \mathbb{C})$ a $\tau_g = 2$ pro g komplexní. Definujeme-li na $\mathbb{R}^{r+2s}$ skalární součin $\langle -, - \rangle$ tak, že pro $(a_g), (b_g) \in \mathbb{R}^{r+2s}$ je $\langle a, b \rangle = \sum \tau_g a_g b_g$, je G isomorfismus i vzhledem ke skalárnímu součinu.

Důkaz. Prvá část lemmatu plyne z definice $K_{\mathbb{R}}$. Druhou lze odvodit z lemmatu IV.2.1. $\square$

Jednotková krychle ve skalárním součinu $\langle a, b \rangle = \sum \tau_g a_g b_g$ má takové vrcholy (e_g), $g \in \mathrm{Hom}(K, \mathbb{C})$, že $e_g \in \{0, 1\}$ pro g reálný a $e_g \in \{0, 1/\sqrt{2}\}$ pro g komplexní. Její objem ve standardním skalárním součinu je tedy 2^{-s}, takže můžeme vyslovit

IV.2.5 Důsledek. *Ať je vol_0 standardní míra v $\mathbb{R}^{r+2s}$. Pak pro každou měřitelnou množinu $M \subseteq K_{\mathbb{R}}$ platí $vol(M) = 2^s vol_0(G(M))$.*

Na $K_{\mathbb{C}}$ lze přirozeně definovat stopu $\mathrm{Tr}: K_{\mathbb{C}} \to \mathbb{C}$, $(u_g) \mapsto \sum u_g$. Jde o lineární formu, která splňuje $\mathrm{Tr}(F(u)) = \overline{\mathrm{Tr}(u)}$, takže při zúžení na $K_{\mathbb{R}}$ dostáváme lineární formu $\mathrm{Tr}: K_{\mathbb{R}} \to \mathbb{R}$.

Definujme $f : K \to K_{\mathbb{C}}$ tak, že $f(\alpha) = (g(\alpha);\ g \in \mathrm{Hom}(K, \mathbb{C}))$. Hodnota odpovídající indexu $\overline{g}$ je rovna $\overline{g}(\alpha) = \overline{g(\alpha)}$, takže $F(f(\alpha)) = f(\alpha)$ pro každé $\alpha \in K$, a tedy $\mathrm{Im}(f) \subseteq K_{\mathbb{R}}$.

Z tvrzení II.5.2 okamžitě máme

IV.2.6 Lemma. *Ať $\alpha \in K$. Potom $\mathrm{Tr}(f(\alpha)) = \mathrm{Tr}_{K|Q}(\alpha)$.*

IV.2.7 Tvrzení. *Je-li I nenulový ideál $\mathbb{Z}_k$, pak je $f(I)$ úplnou mříží v $K_{\mathbb{R}}$ a $vol f(I) = \sqrt{|\triangle(I)|}$.*

Důkaz. Uvažme celistvou bázi $\alpha_1, \ldots, \alpha_n$ ideálu I. Vidíme, že $f(I)$ je rovno celočíselným kombinacím prvků $f(\alpha_1), \ldots, f(\alpha_n)$. Podle lemmatu II.5.5 je $\triangle(I)$ rovno $(\det(M))^2$, kde $M = (g_i(\alpha_j))$, $\mathrm{Hom}(K, \mathbb{C}) = \{g_1, \ldots, g_n\}$. Protože $\triangle(I)$ je celé a nenulové, a protože sloupcové vektory matice M jsou po řadě rovny $f(\alpha_1), \ldots, f(\alpha_n)$, musí být tyto vektory lineárně nezávislé. Vidíme, že $f(I)$ je v $K_{\mathbb{R}}$ vskutku mříží.

Matice $(\langle f(\alpha_i), f(\alpha_j) \rangle)$ má na pozici (i, j) hodnotu $\sum_k g_k(\alpha_i)\overline{g_k}(\alpha_j)$, takže je rovna $M^T \overline{M}$ (pro srovnání připomeňme, že $M^T M$ dává matici $(\mathrm{Tr}(\alpha_i \alpha_j))$). Tudíž $vol(f(I)) = \sqrt{|\det(M^T \overline{M})|} = \sqrt{|\det(M)|^2} = \sqrt{|(\det(M))^2|} = \sqrt{|\triangle(I)|}$. $\square$

IV.2.8 Tvrzení. *Ať je I nenulový ideál $\mathbb{Z}_k$ a ať c_g, $g \in \mathrm{Hom}(K, \mathbb{C})$, jsou kladná reálná čísla, $c_g = c_{\overline{g}}$. Je-li $(2/\pi)^s \sqrt{|\triangle(I)|} < \prod c_g$, existuje $\alpha \in I$, $\alpha \neq 0$, jež pro všechna $g \in \mathrm{Hom}(K, \mathbb{C})$ splňuje $|g(\alpha)| < c_g$.*

Důkaz. Položme $M = \{(u_g) \in K_{\mathbb{R}};\ |u_g| < c_g \text{ pro všechna } g \in \mathrm{Hom}(K, \mathbb{C})\}$. Ať $G: K_{\mathbb{R}} \to \mathbb{R}^{r+2s}$ je stejné jako v tvrzení IV.2.4. Potom

$$G(M) = \{(a_g),\ |a_g| < c_\rho \text{ a } a_\rho^2 + a_{\overline{\rho}}^2 < c_\rho^2\},$$

kde ρ odkazuje na reálné homomorfismy g a σ vybírá z každé dvojice $\{g, \overline{g}\}$ komplexních homomorfismů právě jeden.

Objem $G(M)$ ve standardní metrice vol_0 je $\prod_\rho(2c_\rho)\prod_\sigma(\pi c_\sigma^2)$, což podle důsledku IV.2.5 dává $vol(M) = 2^{r+s}\pi^s \prod c_g$. Máme tedy

$$vol(M) > 2^n\sqrt{|\triangle(I)|} = 2^n vol(f(I)).$$

Podle Minkowského věty o mřížovém bodě v M leží některý z bodů $(g(\alpha); g \in \mathrm{Hom}(K, \mathbb{C}))$, kde $\alpha \in I$, $\alpha \neq 0$. Příslušnost tohoto bodu k M znamená $|g(\alpha)| < c_g$, pro všechna $g \in \mathrm{Hom}(K, \mathbb{C})$. □

IV.2.9 Tvrzení. *Ať I je nenulový ideál číselného tělesa K. Pak existuje $\alpha \in I$, $\alpha \neq 0$, takové, že*

$$|N_{K|Q}(\alpha)| \leq (2/\pi)^s\sqrt{|\triangle(I)|}.$$

Důkaz. Norma $N_{K|Q}(\alpha)$ je pro každé $\alpha \in I$ celé číslo (viz např. tvrzení III.3.2). Proto stačí dokázat $|N_{K|Q}(\alpha)| < E$, kde $E = \epsilon + (2/\pi)^s\sqrt{|\triangle(I)|}$ a $\epsilon > 0$ je vhodně zvolené. Zvolme $c_g > 0$ reálná tak, že $c_g = c_{\overline{g}}$, $g \in \mathrm{Hom}(K, \mathbb{C})$, a $\prod c_g = E$. Podle tvrzení IV.2.8 můžeme nalézt $\alpha \in I$, $\alpha \neq 0$, takové, že $|g(\alpha)| < c_g$, $g \in \mathrm{Hom}(K, \mathbb{C})$. To ovšem znamená, že $|N_{K|Q}(\alpha)| = \prod |g(\alpha)| < E$. □

Ze vztahu $\triangle(I) = |\mathbb{Z}_K : I|^2\triangle(\mathbb{Z}_K)$ vyplývá, že $\sqrt{|\triangle(I)|} = \sqrt{|\triangle(\mathbb{Z}_K)|}|\mathbb{Z}_K : I|$, kde $|\mathbb{Z}_K : I|$ píšeme též jako $\mathcal{N}(I)$ (viz kapitola IV.1).

Položíme-li $C = (2/\pi)^s\sqrt{|\triangle(\mathbb{Z}_K)|}$, tak z lemmatu IV.1.1 a tvrzení IV.2.9 vyplývá, že existuje $\alpha \in I$, $\alpha \neq 0$, jež splňuje $|N_{K|Q}(\alpha)| = |\mathcal{N}(\alpha\mathbb{Z}_K)| < C\mathcal{N}(I)$.

Podle tvrzení IV.1.3 existuje jen konečně mnoho ideálů I s $\mathcal{N}(I) \leq C$. Tato fakta nám dopomohou k důkazu

IV.2.10 Věta. *Třídová grupa $\mathcal{C}l_K$ číselného tělesa K je vždy konečná.*

Důkaz. Ať J je nenulový lomený ideál. Podle předchozího bude stačit, když dokážeme, že J je možné vyjádřit jako $(\beta\mathbb{Z}_K)I = \beta I$, kde $\beta \in K$ a kde I je (celistvý) ideál, jenž splňuje $\mathcal{N} < C$

Uvažme $\gamma \in \mathbb{Z}_K$, $\gamma \neq 0$, takové, že γJ^{-1} je celistvý ideál (viz lemma III.4.5) a ať $\alpha \in \gamma J^{-1}$ splňuje $|\mathcal{N}((\alpha\mathbb{Z}_K)(\gamma J^{-1}))| \leq C$. Přitom $I = (\alpha\mathbb{Z}_K)(\gamma J^{-1})^{-1} = \alpha\gamma^{-1}J$ je ideál celistvý a $J = (\gamma\alpha^{-1})I$. (Celistvost I vyplývá z toho, že $\alpha_0 J_0^{-1}$ je celistvý kdykoliv J_0 je celistvý a $\alpha_0 \in J_0$, neboť z $\alpha_0\mathbb{Z}_K \subseteq J_0$ plyne $\alpha J_0^{-1} \subseteq J_0 J_0^{-1} = \mathbb{Z}_K$.) □

Řádu třídové grupy $\mathcal{C}l_K$ se říká *třídové číslo* (class number) a značívá se h_K. Jeho hodnota (i struktura $\mathcal{C}l_K$) se jeví být velice těžko odhadnutelná.

Je známo, že okruh algebraických celých kvadratického tělesa $\mathbb{Q}(\sqrt{d})$ je pro $d < 0$, d nedělitelné čtvercem, obor hlavních ideálů (tj. má $h_K = 1$) právě pro $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$.

Pro $\mathbb{Q}(\sqrt{d})$, $2 \leq d < 100$ nedělitelné čtvercem, dostáváme obory hlavních ideálů pro $d = 2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, 38, 41, 43, 46, 47, 53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97$. Je však otevřenou otázkou, zda $\mathbb{Q}(\sqrt{d})$, d bez čtvercových dělitelů, je oborem hlavních ideálů pro nekonečně mnoho $d > 1$.

Historicky vzato je zkoumání Velké Fermatovy věty spjato se zkoumáním struktury cyklotomického okruhu $\mathbb{Z}[\xi_p]$, kde $\xi = \xi_p$ je p–tá odmocnina z jedné. Rovnost $y^p = z^p - x^p$ lze totiž zapsat jako

$$y \cdots y = (z - x)(z - \xi x) \cdots (z - \xi^{p-1} x)$$

a z toho lze odvodit spor v případě, že $\mathbb{Z}[\xi_p]$ je oborem hlavních ideálů. Argumentaci lze prodloužit i na situaci, kdy p nedělí třídové číslo h_p, avšak pro $p \mid h_p$ se naznačený postup použít nepodařilo. Prvočísla s $p \nmid h_p$ se nazývají *regulární*, ostatní jsou *iregulární*. Pro $p < 100$ jsou iregulární prvočísla 37, 59 a 67.

IV.3 Dirichletova věta o jednotce

Začneme multiplikativní verzí teorie Minkowského. Ta vychází z multiplikativní grupy $K_{\mathbb{C}}^* = \prod_g(\mathbb{C}^*;\ g \in \mathrm{Hom}(K,\mathbb{C}))$, kterou budeme zobrazovat na $\prod_g(\mathbb{R}; g \in \mathrm{Hom}(K,\mathbb{C}))$ pomocí $\ell{:}\mathbb{C}^* \to \mathbb{R}$, $z \mapsto \log|z|$.

Vidíme, že $\ell : \prod_g \mathbb{C}^* \to \prod_g \mathbb{R}$ je homomorfismus komutativních grup, který převádí multiplikativní notaci na aditivní. Jeho jádrem jsou n–tice $(z_g;\ g \in \mathrm{Hom}(K,\mathbb{C})$, kde $|z_g| = 1$ pro každé g (i nadále předpokládáme $n = [K : Q]$). Definujeme-li $N : K_{\mathbb{C}}^* \to \mathbb{C}^*$, $(z_g;\ g \in \mathrm{Hom}(K,\mathbb{C})) \mapsto \prod z_g$ a $\mathrm{Tr} : \prod_g \mathbb{R} \to \mathbb{R}$, $(x_g;\ g \in \mathrm{Hom}(K,\mathbb{C})) \mapsto \sum x_g$, vidíme, že je $\ell N = \mathrm{Tr}\,\ell$.

Definujme $f : K^* \to K_{\mathbb{C}}^*$ stejně jako v předchozí kapitole, $f(\alpha) = (g(\alpha); g \in \mathrm{Hom}(K,\mathbb{C}))$. Pak $N_{K|\mathbb{Q}}(\alpha) = \prod g(\alpha) = N(f(\alpha))$, takže diagram

$$\begin{tikzcd}
K^* \arrow[r, "f"] \arrow[d, "N_{K|\mathbb{Q}}"'] & K_{\mathbb{C}}^* \arrow[r, "\ell"] \arrow[d, "N"'] & \prod_g \mathbb{R} \arrow[d, "\mathrm{Tr}"'] \\
\mathbb{Q}^* \arrow[r] & \mathbb{C}^* \arrow[r, "\ell"] & \mathbb{R}
\end{tikzcd}$$

komutuje. Na $K_{\mathbb{C}}^*$ přeneseme definici F s předchozí kapitoly, tedy $F(z_g;\ g \in \mathrm{Hom}(K,\mathbb{C})) = (z_g;\ g \in \mathrm{Hom}(K,\mathbb{C}))$. Z kapitoly IV.2 víme, že $F(f(\alpha)) = f(\alpha)$ pro každé $\alpha \in K$. Chápeme-li F na K^* jako identitu a na $\mathbb{C}^*$ jako $z \mapsto \overline{z}$, vidíme, že je $f \circ F = F \circ f$, $N \circ F = F \circ N$ a $N_{K|\mathbb{Q}} \circ F = F \circ N_{K|\mathbb{Q}}$. K tomu, aby platily vztahy komutování i v ostatních případech, je třeba na $\prod_g \mathbb{R}$ definovat F tak, že $F(x_g;\ g \in \mathrm{Hom}(K,\overline{\mathbb{C}})) = (x_{\overline{g}};\ g \in \mathrm{Hom}(K,\overline{\mathbb{C}}))$. Pak je jak $F \circ \ell = \ell \circ F$, tak $\mathrm{Tr} \circ F = F \circ \mathrm{Tr}$.

Je-li φ některý z homomorfismů v uvedeném diagramu, tak z $F(x) = x$ plyne $F(\varphi(x)) = \varphi(F(x)) = \varphi(x)$, takže dostáváme komutativní diagram

$$\begin{tikzcd}
K^* \arrow[r, "f"] \arrow[d, "N_{K|\mathbb{Q}}"'] & K_{\mathbb{R}}^* \arrow[r, "\ell"] \arrow[d, "N"'] & {[\prod_g \mathbb{R}]^+} \arrow[d, "\mathrm{Tr}"'] \\
\mathbb{Q}^* \arrow[r] & \mathbb{R}^* \arrow[r, "\ell"] & \mathbb{R}
\end{tikzcd}$$

kde $[\prod_g \mathbb{R}]^+ = \{x_g \in \prod_g \mathbb{R}; x_{\overline{g}} = x_g \text{ pro každé } g \in \mathrm{Hom}(K,\mathbb{C})\}$.

Podobně jako v základní aditivní verzi, i zde prostor $[\prod_g \mathbb{R}]^+$ zobrazíme na „standardní“ reálný prostor, a to na prostor $\mathbb{R}^{r+s}$. Zobrazení je definováno tak, že zachovává hodnoty x_g, g reálný homomorfismus, a dvojici (x_g, x_g) odpovídající dvojici komplexně sdružených komplexních homomorfismů zobrazí na $2x_g$. Označíme-li popsané zobrazení G, dostaneme prodloužení námi uvažovaného komutativního diagramu, neboť zjevně platí $\mathrm{Tr} \circ G(x) = \mathrm{Tr}(x)$, pro každé $x = (x_g) \in [\prod_g \mathbb{R}]^+$.

Pro $(z_g) \in K_{\mathbb{R}}^*$ máme

$$G \circ \ell(z_g) = (\log|z_{\rho_1}|, \ldots, \log|z_{\rho_r}|, \log|z_{\sigma_1}|^2, \ldots, \log|z_{\sigma_s}|^2).$$

V dalších úvahách budou hrát značnou roli následující množiny:

$$\begin{array}{rcl} \mu(K) & = & \{\alpha \in K;\ \alpha^k = 1 \text{ pro nějaké } k \geq 1\}, \\ \mathbb{Z}_K^* & = & \{\alpha \in \mathbb{Z}_K;\ N_{K|\mathbb{Q}}(\alpha) = \pm 1\}, \\ S & = & \{y \in K_{\mathbb{R}}^*;\ N(y) = \pm 1\} \ \text{ a} \\ H & = & \{x \in [\Pi_g \mathbb{R}]^+;\ \operatorname{Tr}(x) = 0\}. \end{array}$$

Z tvrzení III.3.2 vyplývá, že výše uvedené vyjádření $\mathbb{Z}_K^*$ je vskutku pouze jiný způsob popisu invertibilních prvků $\mathbb{Z}_K$.

IV.3.1 Lemma. *Pro každé $\alpha \in K$ je $N_{K|\mathbb{Q}}(\overline{\alpha}) = N_{K|\mathbb{Q}}(\alpha)$ a $N_{K|\mathbb{Q}}(|\alpha|^2) = (N_{K|\mathbb{Q}}(\alpha))^2$.*

Důkaz. Prvá rovnost vyplývá z toho, že zúžení $z \mapsto \overline{z}$ na K je jedním z automorfismů K. Druhá rovnost pak vyplývá z multiplikativity normy, neboť $|\alpha|^2 = \alpha\overline{\alpha}$. □

IV.3.2 Důsledek. *Pro $\alpha \in \mathbb{Z}_K$ platí $\alpha \in \mathbb{Z}_K^* \Leftrightarrow |\alpha| = 1$.*

Důkaz. Podle lemmatu IV.3.1 je $\alpha \in \mathbb{Z}_K^*$ právě když $N_{K|\mathbb{Q}}(|\alpha|^2) = 1$. Pro $t \in \mathbb{Q}$, $t > 0$, ovšem máme $N_{K|\mathbb{Q}}(t) = 1 \Leftrightarrow t = 1$. □

IV.3.3 Lemma. *Pro každé celé $k \in \mathbb{Z}$ existuje, až na násobení invertibilními prvky, pouze konečně mnoho $\alpha \in \mathbb{Z}_K$ takových, že $N_{K|\mathbb{Q}}(\alpha) = k$.*

Důkaz. Hlavní ideál $k\mathbb{Z}_K$, $k \neq 0$, je v Z_K konečného indexu $\mathcal{N}(k\mathbb{Z}_K) = |\mathbb{Z}_K : k\mathbb{Z}_K|$. Stačí proto dokázat, že z $\alpha = \beta \pmod{k\mathbb{Z}_K}$, $|N_{K|\mathbb{Q}}(\alpha)| = |N_{K|\mathbb{Q}}(\beta)| = k$, vyplývá invertibilita $\alpha\beta^{-1}$. Ať tedy $\beta = \alpha + k\gamma$, $\gamma \in \mathbb{Z}_K$. Pišme N místo $N_{K|\mathbb{Q}}$. Máme $N(\beta)\beta^{-1} \in \mathbb{Z}_K$, a proto $\alpha\beta^{-1} = 1 - (k\beta^{-1})\gamma = 1 \pm (N(\beta)\beta_{-1})\gamma \in \mathbb{Z}_K$. Stejně tak ovšem $\beta\alpha^{-1} \in \mathbb{Z}_K$, takže $\alpha\beta^{-1}$ je invertibilní prvek $\mathbb{Z}_K$. □

Vraťme se k výše uvažovanému komutativnímu diagramu a k jeho vztahu k množinám $\mathbb{Z}_K^* \subseteq K^*$, $S \subseteq K_{\mathbb{R}}^*$ a $H \subseteq [\prod_g \mathbb{R}]^+$. Pro $y \in S$ je $0 = \ell(1) = \ell N(y) = \operatorname{Tr} \ell(y)$, takže $\ell(y) \in H$, a tedy $\ell(S) \subseteq H$. Snadno nahlédneme, že dokonce platí $\ell(S) = H$. Nás však bude zajímat $\Gamma = \ell \circ f(\mathbb{Z}_K^*)$. Protože $f(\mathbb{Z}_K^*) \subseteq S$, je $\Gamma \subseteq H$. Zúžení $\ell \circ f$ na $\mathbb{Z}_K^*$ označíme λ.

IV.3.4 Tvrzení. *Posloupnost*

$$1 \longrightarrow \mu(K) \longrightarrow \mathbb{Z}_K^* \xrightarrow{\lambda} \Gamma \longrightarrow 0$$

je exaktní.

Důkaz. Jde o ověčení, že $\mu(K) = \operatorname{Ker}(\lambda)$. Pokud $\alpha^k = 1$, tak $g(\alpha)^k = 1$ pro každé $g \in \operatorname{Hom}(K, \mathbb{C})$. To znamená $\ell \circ f(\alpha) = 0$, takže $\alpha \in \operatorname{Ker}(\lambda)$. Zbývá ověřit $\operatorname{Ker}(\lambda) \subseteq \mu(K)$, tedy ověřit, že $\{\alpha \in \mathbb{Z}_K^*;\ |g(\alpha)| = 1 \text{ pro každé } g \in \operatorname{Hom}(K, \mathbb{C})\}$ leží v $\mu(K)$. Ovšem k tomu stačí nahlédnout, že uvedená množina je konečná, neboť všechny konečné podgrupy K^* leží v $\mu(K)$. Množina $\{y \in K_{\mathbb{R}};\ |y_g| \leq 1$ pro všechna $g \in \mathrm{Hom}(K, \mathbb{C})\}$ je omezená, a proto v ní leží jen konečně mnoho prvků mříže $f(\mathbb{Z}_K)$. □

IV.3.5 Věta. *Grupa* $\Gamma = \mathrm{Im}(\lambda)$ *je úplnou mříží v* $(r+s-1)$*–rozměrném vektorovém prostoru* H.

Důkaz. Nejprve vyložíme, že Γ je mříží. To podle tvrzení III.5.2 znamená dokázat, že Γ je diskrétní podgrupa H. K tomu stačí dokázat, že pro každé $c > 0$ obsahuje množina $U_c = \{(x_g) \in [\prod_g \mathbb{R}]^+;\ |x_g| \leq c$ pro všechna $g \in \mathrm{Hom}(K, \mathbb{C})$. pouze konečně mnoho bodů Γ. Vzorem U_c v zobrazení $\ell : K_{\mathbb{C}}^* \to [\prod_g \mathbb{R}]^+$ je množina $\{(z_g) \in K_{\mathbb{R}}^*;\ e^{-c} \leq |z_g| \leq e^c\}$. To je ovšem množina, která obsahuje jen konečně mnoho prvků mříže $f(\mathbb{Z}_K)$, neboť je to množina omezená. Proto obsahuje $f^{-1}\ell^{-1}(U_c)$ jen konečně mnoho bodů $\mathbb{Z}_K$, a tím spíše $\mathbb{Z}_K^*$. Přitom $\Gamma \cap U_c = U_c \cap \lambda(\mathbb{Z}_K^*) = \lambda_{-1}(U_c) \cap \mathbb{Z}_K^* \subseteq f^{-1}\ell^{-1}(U_c) \cap \mathbb{Z}_K^*$.

Nyní je třeba ověřit, že mříž Γ je v H úplná. Podle lemmatu III.5.3 stačí nalézt omezenou množinu $B \subseteq H$ takovou, že $H = \bigcup_{\gamma \in \Gamma}(B + \gamma)$. Přitom B sestrojíme jako $\ell(T)$, kde T bude vhodná omezená podmnožina $S = \{y \in K_{\mathbb{R}}^*;\ \mathrm{N}(y) = \pm 1\}$. Přitom omezenost T je vyjádřena existencí $c_g > 0$, že $|x_g| < c_g$ pro každé $(x_g) \in T$. Pak je $\ell(T) = \{(\log|x_g|);\ (x_g) \in T\}$ rovněž omezná, neboť z $(x_g) \in S$ vyplývá $\prod |x_g| \leq 1$, takže $|x_g| > \prod_{g' \neq g} |c_{g'}|^{-1} > 0$ implikuje omezení $\log|x_g|$ zdola.

Je-li $B = \ell(T)$ a $\gamma = \ell f(\alpha) \in \Gamma$, $\alpha \in \mathbb{Z}_K^*$, je $B + \gamma = \ell(Tf(\alpha))$, neboť $\ell(Tf(\alpha)) = \{(\log|x_g g(\alpha)|);\ (x_g) \in T\} = \{(\log|x_g|) + (\log|g(\alpha)|);\ (x_g) \in T)\} = \ell(T) + \ell f(\alpha)$. Naším cílem tedy vlastně je nalézt $T \subseteq S$ omezenou tak, aby platilo $S = \bigcup(Tf(\alpha));\ \alpha \in \mathbb{Z}_K^*)$.

Přitom T budeme hledat ve tvaru $\bigcup(S \cap Xf(\alpha_i^{-1});\ 1 \leq i \leq N)$, kde X je omezená podmnožina $K_{\mathbb{R}}$ a $\alpha_1, \ldots, \alpha_N$ jsou vhodné prvky $\mathbb{Z}_K$.

Položíme $X = \{(z_g) \in K_{\mathbb{R}}; |z_g| < c_g\}$, kde $c_g > 0$, $g \in \mathrm{Hom}(K, \mathbb{C})$, jsou takové, že c_g je vždy rovno $c_{\overline{g}}$, a že $\prod c_g > (2/\pi)^s \sqrt{|\triangle(\mathbb{Z}_K)|}$, a prvky $\alpha_1, \ldots, \alpha_N$ zvolíme tak, aby každé $\beta \in \mathbb{Z}_K$, jež splňuje $0 < |N_{K|\mathbb{Q}}(\beta)| \leq \prod c_g$, bylo možné vyjádřit ve tvaru $\alpha_i \alpha$, kde $1 \leq i \leq N$ a $\alpha \in \mathbb{Z}_K^*$. Taková volba α_i je podle lemmatu IV.3.3 možná.

Uvažme nyní libovolné $y = (y_g) \in S$. Pak $Xy = \{(z_g y_g);\ |z_g| < c_g\} = \{(z'_g);\ |z'_g| < c_g|y_g|\}$. Přitom $\prod |y_g| = 1$, takže pro Xy existují $c'_g > 0$ taková, že $Xy = \{(z_g);\ |z_g| < c'_g\}$, $\prod c'_g = \prod c_g$ a $c'_{\overline{g}} = c'_g$ (je totiž $y_{\overline{g}} = \overline{y_g}$). Podle tvrzení IV.2.8 můžeme pro každé $y \in S$ tedy nalézt $\alpha_y \in \mathbb{Z}_K$, $\alpha_y \neq 0$, že $f(\alpha_y) \in Xy$. Přitom je $\mathrm{N}_{K,\mathbb{Q}}(\alpha_y) < \prod c'_g = \prod c_g$, takže $\alpha_y = \alpha_i \alpha^{-1}$ pro nějaké $\alpha \in \mathbb{Z}_K^*$ a i, $1 \leq i \leq N$. Vidíme, že existuje $x \in X$, jež splňuje $f(\alpha_i \alpha^{-1}) = xy$, takže $y^{-1} = (xf(\alpha_i)^{-1})f(\alpha) \in Tf(\alpha)$. Přitom je vhodné připomenout, že S tvoří podgrupu $K_{\mathbb{R}}^*$. Z $f(\alpha) \in S$ a $y \in S$ tedy vskutku plyne $xf(\alpha_i)^{-1} \in S \cap Xf(\alpha_i^{-1})$. Dokázali jsme, že $S = S^{-1} \subseteq \bigcup(Tf(\alpha);\ \alpha \in \mathbb{Z}_K^*)$. □

Úplná mříž v H je volná abelovská grupa řádu $\dim H = r + s - 1$. Můžeme proto vyslovit

IV.3.6 Věta (Dirichletova o jednotkách). *Ať* K *je číselné těleso. Potom je*

$\mathbb{Z}_K^*$ *součinem konečné cyklické grupy* $\mu(K)$ *a volné abelovské grupy řádu* $r+s-1$.

Důkaz. Použij tvrzení IV.3.4 a větu IV.3.5. $\square$

Každému systému $\varepsilon_1, \dots, \varepsilon_t \in \mathbb{Z}_t^*$, $t = r+s-1$, takovému, že každé $\varepsilon \in \mathbb{Z}_K^*$ lze jednoznačně zapsat jako $\varepsilon = \zeta\varepsilon_1^{\nu_1} \cdots \varepsilon_t^{\nu_t}$, kde $\zeta \in \mu(K)$ a $\nu_1, \dots, \nu_t$ jsou celá čísla, se říká systém *fundamentálních jednotek*.

Mějme tedy fundamentální jednotky $\varepsilon_1, \dots, \varepsilon_t$. Pak $\lambda(\varepsilon_1), \dots, \lambda(\varepsilon_t)$ tvoří bázi mříže $\lambda(\mathbb{Z}_K^*)$ v H. Její objem $vol(\lambda(\mathbb{Z}_K^*))$ záleží pouze na volbě míry vol, nikoliv na volbě fundamentálních jednotek (viz lemma III.5.4). Přitom míru vol můžeme uvažovat buď kanonickou (indukovanou souřadnicovým skalárním součinem v $[\prod_g \mathbb{R}]$, jehož je $[\prod_g \mathbb{R}]^+$ podprostorem), nebo danou ztotožněním $G\colon[\prod_g \mathbb{R}]^+ \cong \mathbb{R}^{r+s}$. ve kterém $(x_g, x_{\overline{g}})$ přechází na $2x_g$ pro každou dvojici $(g, \overline{g})$, g komplexní homomorfismus. Zvykem je pracovat s posledně zmíněnou metrikou, takže $vol(\lambda(\mathbb{Z}_K^*))$ je definováno jako $vol_0(G(vol(\lambda(\mathbb{Z}_K^*))))$, kde vol_0 označuje míru indukovanou na $\{x \in \mathbb{R}^{r+s}; \operatorname{Tr} x = 0\}$ standardním souřadnicovým skalárním součinem v $\mathbb{R}^{r+s}$.

Pro $\varepsilon \in \mathbb{Z}_K^*$ budem $\lambda_i(\varepsilon)$, $1 \le i \le r+s$, používat ve významu souřadnic vektoru $G(\lambda(\varepsilon)) = (\lambda_1(\varepsilon), \dots, \lambda_{r+s}(\varepsilon))$.

Číslu $vol(\lambda(\mathbb{Z}_K^*))/\sqrt{(r+s)}$ se říká *regulátor* K a značívá se R. Jeho hodnota má značný význam při práci s Dedekindovou zeta–funkcí.

IV.3.7 Tvrzení. *Ať* K *je číselné těleso a ať* $\varepsilon_1, \dots, \varepsilon_{r+s-1}$ *je nějaký systém jeho fundamentálních jednotek. Položme* $\Lambda = (\lambda_i(\varepsilon_j))$, *kde* $1 \le i \le r+s$ *a* $1 \le j \le r+s-1$. *Potom je regulátor* R *roven absolutní hodnotě libovolného* $(r+s-1) \times (r+s-1)$ *minoru* Λ.

Důkaz. Potřebujeme znát objem rovnoběžnostěnu v $\mathbb{R}^{r+s}$, který je tvořen obrazy jednotek $\varepsilon_1, \dots, \varepsilon_{r+s-1}$ a jednotkovým vektorem kolmým na nadrovinu vektorů nulové stopy. Tímto vektorem je $(r+s)^{-1/2}(1, \dots, 1)$ a determinant matice, kterou obdržíme z Λ přidáním jedničkového sloupce budeme, až na znaménko, $(r+s)$–násobkem uvedených minorů. Důvodem je skutečnost, že přičtením k vybranému řádku všech řádků ostatních dostaneme řádek, který má na pozici jedničkového sloupce $r+s$ a jinde nuly, neboť obrazy jednotek mají nulovou stopu. Vidíme, že $vol(\lambda(\mathbb{Z}_K^*)) = (r+s)^{-1/2}(r+s)d = \sqrt{(r+s)}d$, kde d je absolutní hodnota determinantu kteréhokoliv z minorů. Proto $d = R$. $\square$

V

V.1 Afinní variety

Mějme dáno komutativní těleso K a ať je $n \geq 1$ přirozené číslo. Nejprve sestrojíme zobrazení $\mathbb{V}$ a $\mathbb{I}$, která převádějí podmnožiny $K[x_1, \ldots, x_n]$ na podmnožiny K^n (zobrazení $\mathbb{V}$) a zpět (zobrazení $\mathbb{I}$).

Pro $J \subseteq K[x_1, \ldots, x_n]$ budiž

$$\mathbb{V}(J) = \{(\alpha_1, \ldots, \alpha_n) \in K^n;\ p(\alpha_1, \ldots, \alpha_n) = 0 \text{ pro všechna } p \in J\}$$

a pro $C \subseteq K^n$ mějme

$$\mathbb{I}(C) = \{p \in K[x_1, \ldots, x_n];\ p(\alpha_1, \ldots, \alpha_n) = 0 \text{ pro všechna } (\alpha_1, \ldots, \alpha_n) \in C\}.$$

Některé základní vlastnosti $\mathbb{V}$ a $\mathbb{I}$ lze snadno ověřit, a proto je uvedeme bez důkazu.

V.1.1 Lemma. *(i) Ať $C_i \subseteq K^n$ a $J_i \subseteq K[x_1, \ldots, x_n]$, $i \in I$. Pak*

$$\mathbb{I}(\cup C_i) = \cap \mathbb{I}(C_i) \quad a \quad \mathbb{V}(\cup J_i) = \cap \mathbb{V}(J_i).$$

(ii) $C_1 \subseteq C_2 \Rightarrow \mathbb{I}(C_1) \supseteq \mathbb{I}(C_2)$ *a* $J_1 \subseteq J_2 \Rightarrow \mathbb{V}(J_1) \supseteq \mathbb{V}(J_2)$.

(iii) $\mathbb{I}\mathbb{V}(J) \supseteq J$ *a* $\mathbb{V}\mathbb{I}(C) \supseteq C$. □

Z bodů (ii) a (iii) máme okamžitý důsledek

V.1.2 Důsledek. *Dvojice $(\mathbb{I}, \mathbb{V})$ tvoří Galoisovu korespondenci mezi podmnožinami K^n a podmnožinami $K[x_1, \ldots, x_n]$.*

Množiny $\mathbb{I}(C)$ jsou ideály okruhu $K[x_1, \ldots, x_n]$. Ne každý ideál je ovšem možné vyjádřit ve tvaru $\mathbb{I}(C)$. Ty ideály, které takto vyjádřit lze, se nazývají *uzavřené*.

Množiny tvaru $\mathbb{V}(J)$, kde $J \subseteq K[x_1, \ldots, x_n]$, se nazývají *algebraické*. Připomeňme, že z vlastností Galoisovy korespondence vyplývají rovnosti $\mathbb{I}\mathbb{V}\mathbb{I} = \mathbb{I}$ a $\mathbb{V}\mathbb{I}\mathbb{V} = \mathbb{V}$. Rovněž na této obecné úrovni můžeme konstatovat, že $\mathbb{I}\mathbb{V}$ je uzávěrový operátor na $K[x_1, \ldots, x_n]$ a $\mathbb{V}\mathbb{I}$ je uzávěrový operátor na K^n.

Každý uzávěrový operátor poskytuje uzávěrový systém (množiny, na kterých je konstantní). V našem případě tedy máme uzávěrový systém algebraických množin a uzávěrový systém uzavřených ideálů.

Uzávěrový systém poskytuje topologii uzavřených množin, jsou-li jeho množiny uzavřené na sjednocení. To ovšem pro algebraické množiny zjevně platí, neboť máme

V.1.3 Lemma. *Buď J_1 a J_2 dva ideály $K[x_1, \dots, x_n]$. Pak $\mathbb{V}(J_1J_2) = \mathbb{V}(J_1) \cup \mathbb{V}(J_2)$.*

Důkaz. Z $J_1 \supseteq J_1J_2$ plyne $\mathbb{V}(J_1) \subseteq \mathbb{V}(J_1J_2)$, takže $\mathbb{V}(J_1) \cup \mathbb{V}(J_2) \subseteq \mathbb{V}(J_1J_2)$. Uvažme naopak $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{V}(J_1J_2)$. Pak pro $p_1 \in J_1$ a $p_2 \in J_2$ máme $(p_1p_2)(\alpha) = p_1(\alpha)p_2(\alpha) = 0$, takže musí být $p_1(\alpha) = 0$ nebo $p_2(\alpha) = 0$. Odtud $\alpha \in \mathbb{V}(J_1) \cup \mathbb{V}(J_2)$. □

V algebraické geometrii se často píše $\mathbb{V}_J$ místo $\mathbb{V}(J)$ a $\mathbb{I}_C$ místo $\mathbb{I}(C)$. Někdy se také píše $\mathbb{Z}(J)$.

Topologie daná algebraickými množinami se nazývá *Zariského.*

Zobrazení $\mathbb{I}$ a $\mathbb{V}$ poskytují (jako v každé Galoisově korespondenci) vzájemně inverzní antiisomorfismy svazu všech uzavřených ideálů a svazu všech algebraických množin. Okruh $K[x_1, \dots, x_n]$ je noetherovský, a proto v něm neexistují nekonečné rostoucí řetězce ideálů. Tudíž v Zariského topologii (na rozdíl od eukleidovské) neexistují nekonečné klesající řetězce uzavřených (tedy algebraických) množin.

Algebraická množina C se nazývá *nerozložitelná*, jestliže z vyjádření $C = C_1 \cup C_2$, kde C_1 i C_2 jsou algbraické, plyne $C_1 = C$ nebo $C = C_2$.

V.1.4 Tvrzení. *Každou algebraickou množinu lze jednoznačně vyjádřit jako ireducibilní sjednocení $C_1 \cup \dots \cup C_k$ nerozložitelných algebraických množin (ireducibilní zde znamená, že žádnou z množin C_i nelze vypustit).*

Důkaz. Ať C je nějaká neprázdná algebraická množina. Uvažme (případně nekonečný) orientovaný binární strom s kořenem v C, jehož hrany konstruujeme tak, že vrchol D (jenž je algebraickou množinou) spojíme s D_1 a D_2 takovými, že $D = D_1 \cup D_2$, přičemž $D_1 \subsetneq D$ a $D_2 \subsetneq D$. Pokud je získaný strom vskutku nekonečný, lze v něm zvolit nekonečnou orientovanou cestu. Ta by však dávala nekonečný klesající řetězec algebraických množin, což by byl spor. Vidíme, že C lze vyjádřit jako sjednocení konečně mnoha nerozložitelných množin.

Je-li $C = C_1 \cup \dots \cup C_k$ ireducibilní rozklad a $D \subseteq C$ je další nerozložitelná algebraická množina, bude $D = (D \cap C_1) \cup \dots \cup (D \cap C_k)$. Z nerozložitelnosti D vyplývá, že pro některé i, $1 \leq i \leq k$, je $D = D \cap C_i$, odkud $D \subseteq C_i$. To znamená, že když je $C = C'_1 \cup \dots \cup C'_k$ nějaký jiný ireducibilní rozklad, bude každé C'_i obsaženo v nějakém C_j. Protože současně každé C_j je obsaženo v nějakém C'_r, musí být C'_i rovno nějakému C_j, a odsud již jednoznačnost zápisu přímo plyne. □

V.1.5 Lemma. *Neprázdná algebraická množina C je nerozložitelná právě když $\mathbb{I}(C)$ je prvoideál.*

Důkaz. Ať je nejprve $C = C_1 \cup C_2$, kde $C_i = \mathbb{V}(J_i)$ je vlastní podmnožina C, $i \in \{1, 2\}$. Pak jsou množiny $C_1 \setminus C_2$ a $C_2 \setminus C_1$ neprázdné, a proto jsou neprázdné i množiny $J_1 \setminus J_2$ a $J_2 \setminus J_1$. Zvolme $p_1 \in J_1 \setminus J_2$ a $p_2 \in J_2 \setminus J_1$. Podle lemmatu V.1.3 je $C = \mathbb{V}(J_1J_2)$, takže $p_1p_2 \in \mathbb{I}(C)$. Současně ale existují body $\alpha_1 \in C_2$ a $\alpha_2 \in C_1$ takové, že $p_1(\alpha_1) \neq 0$ (neboť $p_1 \notin J_2$) a $p_2(\alpha_2) \neq 0$ (neboť $p_2 \notin J_1$). Proto nemůže být ani $p_1 \in \mathbb{I}(C)$ ani $p_2 \in \mathbb{I}(C)$.

Předpokládejme nyní, že C je nerozložitelné a že je $p_1p_2 \in \mathbb{I}(C)$ pro nějaká $p_i \in K[x_1, \dots, x_n]$, jež nepadnou do $\mathbb{I}(C)$, $i \in \{1, 2\}$. To znamená, že existují $\alpha_i \in C$ taková, že $p_i(\alpha_i) \neq 0$. Máme $C \subseteq \mathbb{V}(p_1p_2) = \mathbb{V}(p_1) \cup \mathbb{V}(p_2)$, takže $C = (C \cap \mathbb{V}(p_1)) \cup (C \cap \mathbb{V}(p_2))$, přičemž žádná z algebraických množin $C \cap \mathbb{V}(p_i)$ se nerovná C. $\square$

Obecně nemusí být každý prvoideál uzavřený. Nad algebraicky uzavřeným tělesem to ovšem platí. Z Hilbertovy věty o nulách totiž plyne, že

(1) maximální ideály v $K[x_1, \dots, x_n]$ jsou generovány polynomy $x-\alpha_1, \dots, x-\alpha_n$, kde $(\alpha_1, \dots, \alpha_n) \in K^n$ takový ideál plně určuje a že

(2) pro každý vlastní ideál J platí, že jeho uzávěr $\mathbb{IV}(J)$ je roven jeho radikálu $\sqrt{J}$.

Prvoideál je vždy roven svému radikálu, a proto jsou prvoideály nad algebraicky uzavřenými tělesy uzavřené. Pokud těleso K uzavřené není, tak v $K[x]$ (a potažmo i v $K[x_1, \dots, x_n]$) existují maximální ideály M, pro které je $\mathbb{V}(M) = \emptyset$ (nemají žádnou nulu). V $K[x]$ to samozřejmě jsou hlavní ideály generované ireducibilními polynomy.

V.1.6 Tvrzení. *Ať K je algebraicky uzavřené těleso a $n \geq 1$. Pak pro každý vlastní ideál J okruhu $S = K[x_1, \dots, x_n]$ platí*

$$\mathbb{I}(J) = \bigcap\{M;\ M \text{ maximální ideál } S,\ J \subseteq M\} = \bigcap\{P;\ P \text{ prvoideál } S,\ J \subseteq P\} = \sqrt{J}.$$

Důkaz. Z Hilbertovy věty o nulách máme $\mathbb{I}(J) = \sqrt{J}$. Současně je jejím důsledkem i fakt, že každý prvoideál je roven průniku maximálních ideálů, které ho obsahují. V každém komutativním okruhu je $\sqrt{J}$ rovno průniku prvoideálů (tvrzení I.3.12). $\square$

Při úvahách o algebraických množinách v K^n se používají různé konvence, z nichž některé nyní připomeneme. Algebraický uzávěr K se značí $\bar{K}$. Místo K^n se často píše $\mathbb{A}^n(K)$, kde $\mathbb{A}$ vyjadřuje skutečnost, že jde o afinní prostor (zkoumají se geometrické vlastnosti algebraických množin a ty nezávisí na volbě počátku). Místo $\mathbb{A}^n(\bar{K})$ se pak leckdy píše pouze $\mathbb{A}^n$.

Zápis $\mathbb{V}(J)$ (či častěji $\mathbb{V}_J$) se bude nadále vztahovat k tělesu $\bar{K}$. Je-li tedy například J ideál v $K[x_1, \dots, x_n]$, tak je $\mathbb{V}(J)$ totéž jako $\mathbb{V}_{J'}$, kde J' je nejmenší ideál $\bar{K}[x_1, \dots, x_n]$, který obsahuje J, tedy $J' = J\bar{K}[x_1, \dots, x_n]$.

Nerozložitelné algebraické množiny $C \subseteq \mathbb{A}^n(\bar{K})$ se nazývají *varietami.* Variety obsažené v $\mathbb{A}^n(\bar{K})$ a prvoideály jsou ve vzájemně jednoznačném vztahu, takže se s nimi často zachází jako s různými vyjádřeními téhož objektu. Varieta se obvykle značí V, přičemž zápisem V/K se nedefinuje nový objekt, nýbrž se poskytuje informace, že $V = \mathbb{V}(I)$ pro nějaké $I \subseteq K[x_1, \dots, x_n]$.

Ideály $K[x_1, \dots, x_n]$ jsou konečně generované, takže varietu V/K lze (podobně jako algebraické množiny vůbec) popsat konečně mnoha polynomiálními rovnicemi.

Je-li V varieta, tak $V(K)$ označuje množinu všech K–*racionálních bodů* V, tedy množinu $\mathbb{A}^n \cap V$.

Funkce $f : V \to \bar{K}$ se nazývá *regulární*, jestliže existuje takový polynom $p \in \bar{K}[x_1, \dots, x_n]$, že $p(\alpha) = f(\alpha)$ pro každé $\alpha \in \mathbb{A}^n$. Vidíme, že regulární funkce jsou obrazem $\bar{K}[x_1, \dots, x_n]$ při homomorfismu který každému polynomu přiřazuje jeho funkční chování na V. Jádrem tohoto homomorfismu je prvoideál $\mathbb{I}(V) = \mathbb{I}_V$, takže je přirozené, že oboru integrity $\bar{K}[V] = \bar{K}[x_1, \dots, x_n]/\mathbb{I}(V)$ se říká *okruh regulárních funkcí* na V. Jindy se mu též říká *souřadnicový okruh* V.

Symbolem $\bar{K}(V)$ se označuje podílové těleso tohoto okruhu. Jeho prvky jsou *racionální funkce* f/g (kde $f, g \in \bar{K}[V]$), takže se mluví buď o *tělese racionálních funkcí* V nebo o *tělese funkcí* na V.

Těleso $\bar{K}$ se do $\bar{K}(V)$ a $\bar{K}[V]$ přirozeně vnořuje a odpovídá konstantním funkcím. *Stupeň transcendence* $\bar{K}[V]$ nad $\bar{K}$ se nazývá *dimenzí* variety V.

VI Normalizace, lokalizace, valuace

VI.1 Noetherovská normalizace

V této kapitole se budeme věnovat afinním K–algebrám, kde K je komutativní těleso. Připomeňme, že afinní K–algebrou A rozumíme každý komutativní okruh, který je současně konečně rozměrným vektorovým prostorem nad K. Přitom se K ztotožňuje s jednorozměrným podprostorem, který obsahuje 1.

VI.1.1 Lemma. *Ať $\varphi: A \to B$ je surjektivní homomorfismus K–algeber. Předpokládejme, že $y_1, \ldots, y_n \in A$ jsou nad K prvky algebraicky nezávislé a takové, že A je konečně generovaný $K[y_1, \ldots, y_n]$–modul. Předpokládejme dále, že pro nějaké $d \leq n$ platí*

$$\mathrm{Ker}(\varphi) \cap K[y_1, \ldots, y_n] = \sum_{i>d} y_i K[y_1, \ldots, y_n].$$

Potom $\varphi(y_1), \ldots, \varphi(y_d) \in B$ jsou nad K prvky algebraicky nezávislé a B je jako $K[\varphi(y_1), \ldots, \varphi(y_d)]$–modul konečně generovaný.

Důkaz. Označme ψ zúžení φ na $K[y_1, \ldots, y_n] \to B$. Prvky $y_{d+1}, \ldots, y_n$ leží v jádru ψ, a proto $\mathrm{Im}(\psi) = K[\varphi(y_1), \ldots, \varphi(y_d)]$. Víme, že existuje $M \subseteq A$ konečné takové, že každý prvek A je lineární kombinací prvků M s koeficienty v $K[y_1, \ldots, y_n]$. Ze surjektivity φ vyplývá, že každý prvek B je lineární kombinací prvků $\varphi(M)$ s koeficienty v $\mathrm{Im}(\psi)$. Vidíme, že B je konečně generovaný $K[\varphi(y_1), \ldots, \varphi(y_d)]$–modul.

Uvažme nyní $\mu: K[y_1, \ldots, y_n] \to K[y_1, \ldots, y_d]$, které je identické na $y_1, \ldots, y_d$ a které zobrazuje $y_{d+1}, \ldots, y_n$ do nuly. Jádro tohoto surjektivního homomorfismu je rovno $\mathrm{Ker}\, \psi = \sum_{i>d} y_i K[y_1, \ldots, y_n]$. Z $\mathrm{Ker}(\mu) = \mathrm{Ker}(\psi)$ ovšem plyne existence isomorfismu $\mathrm{Im}(\mu) \cong \mathrm{Im}(\psi)$, který zobrazuje y_i na $\varphi(y_i)$. Odsud algebraická nezávislost $\varphi(y_1), \ldots, \varphi(y_d)$. □

VI.1.2 Lemma. *Ať je K komutativní těleso a ať $u \in K[x_1, \ldots, x_n]$ není konstanta (tedy $u \notin K$). Potom existují $y_1, \ldots, y_{n-1} \in K[x_1, \ldots, x_n]$ takové, že $K[y_1, \ldots, y_{n-1}, x_n] = K[x_1, \ldots, x_n]$ a že pro nějaké $m \geq 1$ lze nalézt polynomy $a_1, \ldots, a_{m-1} \in K[y_1, \ldots, y_{n-1}]$ a nenulové $c \in K$, které splňují*

$$u = c x_n^m + \sum_{0 \leq i < m} a_i x_n^i$$

Důkaz. Vyjádřeme u ve tvaru $\sum u_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$. Zvolme přirozené číslo h tak, aby bylo $h > i_j$, $1 \leq j \leq n$, ve všech případech, kdy je $u_{i_1 \cdots i_n} \neq 0$. Protože

u nepadne do K, musí být $h \geq 2$. Všimněme si dále, že pro $u_{i_1 \cdots i_n} \neq 0$ a $u_{j_1 \cdots j_n} \neq 0$ máme

$$i_n + i_1 h + \cdots + i_{n-1} h^{n-1} = j_n + j_1 h + \cdots + j_{n-1} h^{n-1}$$

právě když $(i_1, \ldots, i_n) = (j_1, \ldots, j_n)$.

Nyní stačí položit $y_i = x_i - x_n^{h^i}$, $1 \leq i \leq n-1$, a

$$m = \max\{i_n + i_1 h + \cdots + i_{n-1} h^{n-1};\ u_{i_1 \cdots i_n} \neq 0\}.$$

Vskutku, $K[y_1, \ldots, y_{n-1}, x_n] = K[x_1, \ldots, x_n]$ plyne z $x_i = y_i + x_n^{h^i}$, a hledané vyjádření u obdržíme z

$$u = \sum u_{i_1 \cdots i_n} (x_n^h + y_1)^{i_1} \cdots (x_n^{h^{n-1}} + y_{n-1})^{i_{n-1}} x_n^{i_n}.$$

□

VI.1.3 Tvrzení. *Pro $n \geq 1$ uvažme vlastní hlavní ideál I okruhu $K[x_1, \ldots, x_n]$ generovaný prvkem u. Pak lze najít $y_1, \ldots, y_n \in K[x_1, \ldots, x_n]$ algebraicky nezávislé nad K takové, že $K[x_1, \ldots, x_n]$ je nad $K[y_1, \ldots, y_n]$ celistvé, $u = y_n$ a $I \cap K[y_1, \ldots, y_n] = y_n K[y_1, \ldots, y_n]$.*

Důkaz. Zvolme $y_1, \ldots, y_{n-1}$ jako v předchozím lemmatu a položme $y_n = u$. Z vyjádření $u = cx_n^m + \sum a_i x_n^i$ vyplývá, že x_n je celistvé nad $K[y_1, \ldots, y_n]$. Z $K[y_1, \ldots, y_{n-1}, x_n] = K[x_1, \ldots, x_n]$ tudíž plyne, že celistvý uzávěr $K[y_1, \ldots, y_n]$ v $K[x_1, \ldots, x_n]$ je roven $K[x_1, \ldots, x_n]$.

Každé x_i chápané jako prvek tělesa $K(x_1, \ldots, x_n)$ je proto algebraické nad tělesem $K(y_1, \ldots, y_n)$. Stupeň transcendence $K(y_1, \ldots, y_n)$ nad K je tedy roven n dle tvrzení II.6.8. Množina $\{y_1, \ldots, y_n\}$ proto nemůže obsahovat algebraicky ekvivalentní vlastní podmnožinu, a je tudíž algebraicky nezávislá (viz například lemma II.6.4).

Zbývá dokázat, že $I \cap K[y_1, \ldots, y_n] = y_n K[y_1, \ldots, y_n]$. Mějme tedy nějaké $w = uv$, $v \in K[x_1, \ldots, x_n]$, které padne do $K[y_1, \ldots, y_n]$. Z celistvosti okruhu $K[x_1, \ldots, x_n]$ nad okruhem $K[y_1, \ldots, y_n]$ vyplývá existence takových prvků $q_0, \ldots, q_{h-1} \in K[y_1, \ldots, y_n]$, že

$$v^h + q_{h-1} v^{h-1} + \cdots + q_1 v + q_0 = 0,$$

přičemž $h \geq 1$. Výraz na levé straně vynásobíme hodnotou $u^h = y_n^h$ a rovnost zapíšeme ve tvaru

$$w^h + q_{h-1} y_n w^{h-1} + \cdots + q_1 y_n^{h-1} w + q_0 y_n^h = 0.$$

Prvky w, y_n i $q_0, \ldots, q_{h-1}$ leží v $K[y_1, \ldots, y_n]$, což je Gaussův okruh (protože prvky $y_1, \ldots, y_n$ jsou algebraicky nezávislé). Vidíme, že $y_n = u$ dělí w, a proto $w \in y_n K[y_1, \ldots, y_n]$. □

VI.1.4 Tvrzení. *Uvažme vlastní ideál I okruhu $K[x_1, \ldots, x_n]$, $n \geq 1$. Potom existují $y_1, \ldots, y_n \in K[x_1, \ldots, x_n]$ a d, $0 \leq d \leq n$, taková, že*

(i) $y_1, \dots, y_n$ *jsou algebraicky nezávislá nad* K;

(ii) $K[x_1, \dots, x_n]$ *je celistvé nad* $K[y_1, \dots, y_n]$; *a*

(iii) $I \cap K[y_1, \dots, y_n] = \sum_{i>d} y_i K[y_1, \dots, y_n]$.

Důkaz. V případě $I = 0$ lze položit $y_i = x_i$, $1 \leq i \leq n$, a $d = n$. Ať je $I \neq 0$. Budeme postupovat indukcí dle n. V případě $n = 1$ lze použít tvrzení VI.1.3, neboť I je hlavním ideálem. Předpokládejme, že tvrzení platí pro každou hodnotu menší než $n > 1$. Vyberme $u \in I$, $u \neq 0$. Ideál I je vlastní, a proto u neleží v K.

Použijme tvrzení VI.1.3 pro ideál $uK[x_1, \dots, x_n]$. Uvažme prvky $z_1, \dots, z_n \in K[x_1, \dots, x_n]$ takové, že jsou nad K algebraicky nezávislé, že $K[x_1, \dots, x_n]$ je nad $K[z_1, \dots, z_n]$ celistvé, že $u = z_n$ a že $uK[x_1, \dots, x_n] \cap K[z_1, \dots, z_n] = z_n K[z_1, \dots, z_n]$.

Množina $I \cap K[z_1, \dots, z_{n-1}]$ je vlastním ideálem $K[z_1, \dots, z_{n-1}]$. Z indukčního předpokladu plyne existence $y_1, \dots, y_{n-1} \in K[z_1, \dots, z_{n-1}]$ takových, že jsou nad K algebraicky nezávislé, přičemž $K[z_1, \dots, z_{n-1}]$ je celistvé nad $K[y_1, \dots, y_{n-1}]$, a existuje d, $0 \leq d \leq n-1$, pro které platí

$$I \cap K[y_1, \dots, y_{n-1}] = \sum_{i>d} y_i K[y_1, \dots, y_{n-1}].$$

Položíme $y_n = z_n = u$ a dokážeme, že $y_1, \dots, y_n$ vyhovují podmínkám naší věty.

Protože $z_n = y_n$ leží v $K[y_1, \dots, y_n]$, tak je okruh $K[z_1, \dots, z_n]$ celistvý nad okruhem $K[y_1, \dots, y_n]$. Z tranzitivity celistvosti plyne celistvost $K[x_1, \dots, x_n]$ nad $K[y_1, \dots, y_n]$. Úvahou o stupni transcendence vidíme, že prvky $y_1, \dots, y_n$ jsou nad K algebraicky nezávislé.

Všechny prvky $y_1, \dots, y_n$ leží v I, a tak zbývá ukázat $I \cap K[y_1, \dots, y_n] \subseteq \sum_{i>d} y_i K[y_1, \dots, y_n]$.

Uvažme nějaké $w \in I$, jež leží v $K[y_1, \dots, y_n]$. Pišme w jako $w_1 + y_n w_2$, kde $w_1 \in K[y_1, \dots, y_{n-1}]$ a $w_2 \in K[y_1, \dots, y_n]$. Z $y_n \in I$ plyne $y_n w_2 \in I$, a tedy i $w_1 \in I \cap K[y_1, \dots, y_{n-1}]$. To ale podle předchozího znamená, že je $w_1 \in \sum_{i>d} y_i K[y_1, \dots, y_{n-1}]$, a proto vskutku $w \in \sum_{i>d} y_i K[y_1, \dots, y_n]$. □

VI.1.5 Věta (O normalizaci). *Buď A netriviální afinní algebra nad komutativním tělesem K, a ať I je nějaký vlastní ideál A. Potom existují n a d, $0 \leq d \leq n$, a $y_1, \dots, y_n \in A$ tak, že*

(i) $y_1, \dots, y_n$ *jsou nad* K *algebraicky nezávislá;*

(ii) A *je celistvé nad* $K[y_1, \dots, y_n]$; *a*

(iii) $I \cap K[y_1, \dots, y_n] = \sum_{i>d} y_i K[y_1, \dots, y_n]$.

Důkaz. Budeme kombinovat tvrzení VI.1.4 a lemma VI.1.1. Afinní algebra A je konečně generovaná, a proto pro dostatečně velké $h \geq 1$ existuje surjektivní homomorfismus $\varphi: K[x_1, \dots, x_h] \to A$. Položme $J = \varphi^{-1}(I)$.

Vycházejíce z tvrzení VI.1.4, uvážíme nejprve $z_1, \dots, z_h \in K[x_1, \dots, x_h]$, jež jsou nad K algebraicky nezávislá a taková, že $K[x_1, \dots, x_h]$ je nad $K[z_1, \dots, z_h]$ celistvé a pro vhodné n, $0 \leq n \leq h$, je

$$\operatorname{Ker}(\varphi) \bigcap \cap K[z_1, \dots, z_h] = \sum_{i>n} z_i K[z_1, \dots, z_h].$$

Podle lemmatu VI.1.1 jsou $\varphi(z_1), \dots, \varphi(z_n)$ algebraicky nezávislá nad K a afinní algebra A je nad $K[\varphi(z_1), \dots, \varphi(z_n)]$ celistvá (viz tvrzení III.2.4).

Nyní použijeme tvrzení VI.1.4 na $I \cap K[\varphi(z_1), \dots, \varphi(z_n)]$. Podle něj existují $y_1, \dots, y_n \in K[\varphi(z_1), \dots, \varphi(z_n)]$ algebraicky nezávislá nad K taková, že $K[\varphi(z_1), \dots, \varphi(z_n)]$ je celistvé nad $K[y_1, \dots, y_n]$ a pro vhodné d, $0 \leq d \leq n$, platí

$$I \cap K[y_1, \dots, y_n] = \sum_{i>d} y_i K[y_1, \dots, y_n].$$

Celistvost A nad $K[y_1, \dots, y_n]$ plyne z tranzitivity celistvosti. $\square$

O prvcích $y_1, \dots, y_n$ netriviální afinní K–algebry A řekneme, že tvoří *noetherovskou normalizaci* právě když A je nad $K[y_1, \dots, y_n]$ celistvé a $y_1, \dots, y_n$ jsou nad K algebraicky nezávislé.

VI.2 Konstrukce lokalizace

Mocným nástrojem mnohých algebraických a geometrických úvah je takzvaná *lokalizace*. Vybudování jejího základního aparátu je sice poměrně snadné, ale pochopení, proč byl zvolen právě pojem lokalizace, vyžaduje určitý geometrický náhled, jehož zprostředkování prozatím odložíme.

Připomeňme, že *multiplikativní množinou* (či přesněji multiplikativně uzavřenou množinou) se rozumí každá podmnožina S okruhu R, která neobsahuje nulu, obsahuje jedničku a je uzavřená na násobení. Jinými slovy, je to každý podmonoid $R(\cdot, 1)$, který neobsahuje nulu. V případě, kdy je R obor integrity, lze za S zvolit $R \setminus \{0\}$; obory integrity tak lze přímo definovat. Podobně lze definovat prvoideály okruhu R jako ty ideály I, pro které je $R \setminus I$ multiplikativní množina. Přitom předpokládáme, že R je komutativní okruh (tak budeme činit i nadále).

Ať tedy R je komutativní okruh a S jeho multiplikativní podmnožina. Definujme relaci $\sim$ na $R \times S$ tak, že

$$(a, s) \sim (b, t) \iff u(ta - sb) = 0 \text{ pro nějaké } u \in S.$$

Relace $\sim$ je zjevně reflexivní a symetrická. Pokud $uta = usb$ a $vrb = vtc$, kde $(c, r) \in R \times S$, tak $uvtra - uvtsc = uvsrb - uvrsb = 0$. Vidíme, že $\sim$ je ekvivalence na $R \times S$.

Množinu $R \times S$ lze považovat za komutativní monoid vzhledem k neutrálnímu prvku $(1, 1)$. Protože z $(a, s) \sim (b, t)$ jistě plyne $(ca, rs) \sim (cb, rt)$, je $\sim$ slučitelná s násobením tohoto monoidu.

Definujme na $R \times S$ sčítání vzorcem $(a, s) + (b, t) = (ta + sb, st)$. Potom $((a, s) + (b, t)) + (c, r) = (rta + rsb + stc, rst) = (a, s) + ((b, t) + (c, r))$, takže vidíme, že $R \times S$ lze považovat též za aditivní pologrupu. Je to dokonce monoid s neutrálním prvkem $(0, 1)$, neboť $(a, s) + (0, 1) = (a, s)$ pro každé $(a, s) \in R \times S$.

Jsou-li $(a, s), (b, t) \in R \times S$ taková, že $uat = ubs$ pro nějaké $u \in S$, pak pro všechna $(c, r) \in R \times S$ platí $(a, s) + (c, r) = (ar + sc, sr) \sim (br + tc, tr) = (b, t) + (c, r)$, neboť $u(ar + sc)tr = u(br + tc)sr$. Vidíme, že operace sčítání je slučitelná s ekvivalencí $\sim$.

Uvažme nyní kvocientní strukturu $R \times S / \sim$. Z předchozího plyne, že na $R \times S$ je definováno sčítání a násobení, přičemž obé je komutativní a asociativní, že $[(1, 1)]$ je neutrální prvek vůči násobení a $[(0, 1)]$ je neutrální prvek vůči sčítání.

Pro každé $(a, s) \in R \times S$ a $t \in S$ zjevně platí $(a, s) \sim (at, st) = (a, s) + (0, t)$. Buďte $(a, s), (b, t), (c, r) \in R \times S$. Pak $((a, s) + (b, t)) \cdot (c, r) = (tac + sbc, str)$ a $(a, s) \cdot (c, r) + (b, t) \cdot (c, r) = (trac + srbc, str^2) = (tac + sbc, str) + (0, r)$. V $(R \times S)/ \sim$ tudíž platí distributivní zákon, a proto je $(R \times S)/ \sim$ okruh.

Blok $\sim$, který obsahuje $(a, s) \in R \times S$, budeme značit, jak je zvykem, a/s nebo $\frac{a}{s}$. Okruh $(R \times S)/ \sim$ se označuje $S^{-1}R$. Jeho nulou je $0/1 = 0$ a jednotkou $1/1 = 1$. Pro $a, b \in R$ a $s, t \in S$ platí

$$\frac{a}{s} + \frac{b}{t} = \frac{ta + sb}{st}, \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} \quad \text{a} \quad \frac{a}{s} = \frac{at}{st}.$$

Zobrazení $r \mapsto r/1$ je zjevně okruhový homomorfismus (říká se mu *přirozený*). Obecně to však nemusí být monomorfismus, neboť pro některé $r \in R$, $r \neq 0$, může nastat $r/1 = 0/1$. Tato rovnost totiž platí právě když existuje $u \in S$ takové, že $ur = 0$, tedy když r leží v anihilátoru některého $u \in S$. Ovšem pak nesmí být $r \in S$, neboť S je multiplikativní množina. Jádro přirozeného homomorfismu má tedy s S triviální průnik.

V případě, kdy R je obor integrity a $S = R \setminus \{0\}$, tak je $S^{-1}R$ shodné s podílovým tělesem R. Víme, že podílové těleso oboru integrity lze charakterizovat jako nejmenší těleso, do kterého lze R vnořit. Obecně okruhy $S^{-1}R$ připouštějí podobnou charakterizaci — jde o nejmenší okruh do kterého lze R homomorfně zobrazit tak, aby se z prvků S staly prvky invertibilní (jednotky). Tuto skutečnost dokážeme v následujícím tvrzení.

VI.2.1 Tvrzení. *Buď R komutativní okruh a ať je $S \subset R$ multiplikativní množina. Označme $f : R \to S^{-1}R$ přirozený homomorfismus. Budiž $g : R \to U$ homomorfismus okruhů takový, že $g(s)$ je pro každé $s \in S$ v U invertibilní. Pak existuje právě jeden homomorfismus $h: S^{-1}R \to U$, který splňuje $g = h \circ f$.*

Důkaz. Pro $a/s \in R \times S$ máme $a/s = (a/1) \cdot (1/s)$, takže jedinou možností, jak h definovat, je položit $h(a/s) = g(a)g(s)^{-1}$ (z $h(1/s \cdot s) = h(1/s)h(s) = 1$ totiž máme $h(1/s) = h(1/s)h(s)h(s)^{-1} = h(s)^{-1}$). Je ovšem třeba ověřit korektnost definice. Ať tedy $(a, s) \sim (b, t)$, kde $uat = ubs$ pro nějaké $u \in S$. Pak $g(u)g(a)g(t) = g(u)g(b)g(s)$, přičemž $g(u)$, $g(t)$ a $g(s)$ jsou v U invertibilní. Poslední rovnost tedy dává $g(a)g(s)^{-1} = g(b)g(t)^{-1}$, a tím je korektnost definice ověřena.

Zjevně $h(a/s \cdot b/t) = g(ab)g(st)^{-1} = g(a)g(b)g(t)^{-1}g(s)^{-1} = h(a/s)g(b/t)$, pro všechna $a/s, b/t \in S^{-1}R$. Dále $h(a/s+b/t) = g(at+bs)g(st)^{-1} = (g(a)g(t)+g(b)g(s))g(s)^{-1}g(t)^{-1} = h(a/s) + h(b/t)$, takže h je vskutku homomorfismus. $\square$

Pro každou $M \subseteq R$ budeme psát $S^{-1}M$ ve významu $\{m/s;\ m \in M \text{ a } s \in S\}$.

VI.2.2 Lemma. *Buď R komutativní okruh a ať $S \subset R$ je multiplikativní množina. Pro každý ideál I okruhu R platí, že $S^{-1}I$ je ideál okruhu $S^{-1}R$. Přitom o vlastní ideál běží právě když $I \cap S = \emptyset$. Každý ideál J okruhu $S^{-1}R$ je roven ideálu $S^{-1}f^{-1}(J)$, kde $f\colon R \to S^{-1}R$ je přirozený homomorfismus. Přitom $f^{-1}(J) = \{a \in R;\ a/s \in J \text{ pro některé } s \in S\} = \{a \in R;\ a/1 \in J\}$.*

Důkaz. Skutečnost, že $S^{-1}I$ je ideál, vyplývá přímo z definice operací v $S^{-1}R$. Ideál $S^{-1}I$ je vlastní právě když $a/s \neq 1/1$ pro všechna a/s, $a \in I$, tedy právě když $ua \neq us$ pro všechna $a \in I$ a všechna $u, s \in S$. Pokud ovšem $ua = us$ pro nějaká taková u, a a s, tak $ua \in I$ padne do $us \in S$, a tím pádem je $I \cap S$ neprázdná. Je-li naopak $s \in I \cap S$, je $s/s = 1/1$.

Ať je nyní J ideál $S^{-1}R$. Potom z $a/s \in J$ plyne $a/1 \in J$, z čehož plyne uvedené vyjádření $f^{-1}(J)$. Zbytek je jasný, neboť vzor ideálu je ideálem v každém homomorfismu okruhů. $\square$

VI.2.3 Tvrzení. *Buď R komutativní okruh a ať $S \subseteq R$ je multiplikativní množina. Ať $f\colon R \to S^{-1}R$ označuje přirozený homomorfismus. Ideál okruhu $S^{-1}R$ je prvoideálem právě když má tvar $S^{-1}P$, kde P je prvoideál R, jenž splňuje $P \cap S = \emptyset$. V takovém případě $f^{-1}(S^{-1}P) = P$ a tento vztah určuje mezi prvoideály $S^{-1}R$ a prvoideály R disjunktními s S vzájemně jednoznačnou korespondenci.*

Důkaz. Dokažme nejprve, že $f^{-1}(S^{-1}P) = P$ pro každý prvodeál P okruhu R, $P \cap S = \emptyset$. Pro $a \in f^{-1}(S^{-1}P)$ máme $a/1 = b/s$ pro nějaké $b \in P$ a $s \in S$. To znamená $u(b - sa) = 0$ pro nějaké $u \in S$. Z $0 \in P$ a $u \notin P$ plyne $b - sa \in P$, tedy $sa \in P$ a $a \in P$.

Pro $a/s, b/t \in S^{-1}R$ proto z $a/s \cdot b/t = ab/(st) \in S^{-1}P$ plyne $ab \in P$, odkud $a \in P$ nebo $b \in P$. Vidíme, že $S^{-1}P$ je vskutku prvoideál.

Je-li J prvoideál $S^{-1}R$ a $I = f^{-1}(J)$, tak $J = S^{-1}I$, dle lemmatu VI.2.2. Pro $a, b \in R$ z $ab \in I$ plyne $(a/1) \cdot (b/1) = ((ab)/1) \in P$, takže $a/1 \in J$ nebo $b/1 \in J$, což znamená $a \in I$ nebo $b \in I$. $\square$

Pokud je $R \setminus S$ ideál (a tedy prvoideál), je $S^{-1}P$, $P = R \setminus S$, vlastním ideálem $S^{-1}R$, který obsahuje všechny vlastní ideály $S^{-1}R$. Vskutku, každý takový vlastní ideál je dle lemmatu VI.2.2 tvaru $S^{-1}I$, kde $I \cap S = \emptyset$, což značí $I \subseteq P$.

Okruhy, které mají největší vlastní ideál, se nazývají *kvazilokální.* Dokázali jsme, že okruh $S^{-1}R$, kde $P = R \setminus S$ je prvoideál R, je vždy kvazilokální. Tento okruh se obvykle označuje R_P a nazývá se lokalizací R v P.

Lokálním okruhem se rozumí každý noetherovský kvazilokální okruh.

Lokalizaci je možné přenést i na úroveň modulů. Uvažme opět komutativní okruh R a multiplikativní množinu S. Ať M je R–modul. Definujme na $M \times$

S operaci $(m,s)+(n,t)=(tm+sn,st)$. Tato operace je asociativní, neboť $((m,s)+(n,t))+(p,r)=(rtm+rsn+rst,rst)=(m,s)+((n,t)+(p,r))$ a $(0,1)$ je jejím neutrálním prvkem. Přitom $(m,s)+(-m,s)=(0,s^2)$.

Definujme na $M\times S$ relaci $\sim$ tak, že $(m,s)\sim(n,t)$ právě když $u(tm-sn)=0$ pro nějaké $u\in S$. Z $utm=usn$ a $vtp=vrn$ plyne $uvtrm=uvsrn=uvtsp$ a odtud plyne, že $\sim$ je ekvivalence. Je-li $utm=usn$, tak je též $(m,s)+(p,r)=(rm+sp,rs)\sim(rn+tp,rt)=(n,t)+(p,r)$, takže $\sim$ je kongruence aditivního monoidu $M\times S$. Jeho neutrální prvek je tvořen třídou obsahující $(0,1)$. Do té padnou všechny prvky tvaru $(0,m)$, takže kvocientní monoid je Abelovou grupou. Jeho prvky budeme opět zapisovat ve tvaru $\frac{m}{s}$ a příslušnou Abelovu grupu označíme $S^{-1}M$.

Ukážeme, že $S^{-1}M$ lze považovat za modul nad $S^{-1}R$. Definujme skalární násobení tak, že $\frac{a}{r}\cdot\frac{n}{t}=\frac{an}{rt}$. Nejprve je třeba ověřit korektnost definice. Je-li $u(tm-sn)=0$, je $u(rtam-rsan)=0$, a z $v(br-as)=0$ plyne $v(brnt-asnt)=0$. Odtud je korektnost již zřejmá. Rovnosti

$$\frac{1}{1}\cdot\frac{n}{t}=\frac{n}{t},\quad \left(\frac{a}{r}\cdot\frac{b}{s}\right)\left(\frac{n}{t}\right)=\frac{a}{r}\left(\frac{b}{s}\cdot\frac{n}{t}\right),$$

$$\left(\frac{a}{r}+\frac{b}{s}\right)\cdot\frac{n}{t}=\frac{a}{r}\cdot\frac{n}{t}+\frac{b}{s}\cdot\frac{n}{t}\ \text{ a }\ \frac{a}{r}\left(\frac{m}{s}+\frac{b}{t}\right)=\frac{a}{r}\cdot\frac{m}{s}+\frac{a}{r}\cdot\frac{b}{t}$$

lze rovněž bez potíží ověřit přímo.

Vidíme, že pro každý R–modul M lze sestrojit $S^{-1}R$–modul $S^{-1}M$. Ukážeme, že tato vazba je funktoriální. Pro $f\colon M\to N$ homomorfismus R–modulů sestrojíme homomorfismus $S^{-1}f\colon S^{-1}M\to S^{-1}N$ tak, že

$$(S^{-1}f)(m/s)=f(m)/s\ \text{ pro všechna } m\in M \text{ a } s\in S.$$

Je-li $m/s=n/t$, tedy $utm=usn$ pro nějaké $u\in S$, je $utf(m)=usf(n)$. Odsud korektnost definice. Dále $(S^{-1}f)(m/s+n/t)=f(tm+sn)/st=(tf(m)+sf(n))/st=(S^{-1}f)(m/s)+(S^{-1}f)(n/s)$. Konečně máme $(S^{-1}f)(a/r\cdot m/s)=f(am)/rs=af(m)/rs=a/r\cdot(S^{-1}f)(m/s)$. Dokázali jsme, že $S^{-1}f$ je vskutku homomorfismus.

Každý $S^{-1}R$–modul lze pokládat za R–modul, stačí položit $r\cdot(\frac{s}{n})=\frac{r}{1}\cdot\frac{s}{n}=\frac{rs}{n}$. Jsou-li M a N dva R–moduly, tak je $\mathrm{Hom}(M,N)=\{f:M\to N,\ f$ je homomorfismus R–modulů$\}$ možno chápat jako R–modul. Je-li $M=N$ je $\mathrm{Hom}(M,N)=\mathrm{End}(M)$ také okruh, takže jde o R–algebru (nikoliv však komutativní).

VI.2.4 Tvrzení. *Ať R je komutativní okruh a S jeho multiplikativní množina.*

(i) Pro každé dva R–moduly M a N je zobrazení

$$\mathrm{Hom}(M,N)\to\mathrm{Hom}(S^{-1}M,S^{-1}N),\quad f\mapsto S^{-1}f,$$

homomorfismem R–modulů.

(ii) Jsou-li $f\colon M\to N$ a $g\colon N\to L$ homomorfismy R–modulů, je $S^{-1}(g\circ f)=S^{-1}g\circ S^{-1}f$.

(*iii*) *Pro každý R–modul M je zobrazení* $\mathrm{Aut}(M) \to \mathrm{Aut}(S^{-1}M)$, $f \mapsto S^{-1}f$, *homomorfismem R–algeber.*

Důkaz. Pro $f, g \in \mathrm{Hom}(M, N)$ a $m/s \in S^{-1}M$ je $S^{-1}(f + g)(m/s) = (f + g)(m)/s = f(m)/s + g(m)/s = (S^{-1}(f) + S^{-1}(g))(m/s)$. Dále pro $a \in R$ máme $S^{-1}(af)(m/s) = (af)(m)/s = af(m)/s = a/1 \cdot f(m)/s = a(S^{-1}f)(m/s)$. Tím je dokázáno ($i$). Všimněme si, že v případě $M = N$ a $f = \mathrm{id}_M$ je $S^{-1}f$ opět identita. K důkazu (iii) proto stačí ověřit (ii).

Buďte tedy $f\colon M \to N$ a $g\colon N \to L$ příslušné homomorfismy. Pak pro každé $m/s \in S^{-1}M$ je $S^{-1}(g \circ f)(m/s) = g(f(m))/s = (S^{-1}g)(f(m)/s) = (S^{-1}g \circ S^{-1}f)(m/s)$. □

Připomeňme, že posloupnost f_i, $1 \leq i \leq n$, homomorfismů R–modulů se nazývá *exaktní*, pokud existují moduly M_i, $0 \leq i \leq n$, takové, že $f_i\colon M_{i-1} \to M_i$, $1 \leq i \leq n$, a $\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$, $1 \leq i < n$.

VI.2.5 Tvrzení. *Ať R je komutativní okruh a S jeho multiplikativní množina. Je-li $M \xrightarrow{f} N \xrightarrow{g} L$ exaktní posloupnost homomorfismů R–modulů, je*

$$S^{-1}M \xrightarrow{S^{-1}f} S^{-1}N \xrightarrow{S^{-1}g} S^{-1}L$$

exaktní posloupnost homomorfismů $S^{-1}R$–modulů.

Důkaz. Máme $g \circ f = 0$, takže z tvrzení VI.2.4 plyne $S^{-1}(g \circ f) = S^{-1}g \circ S^{-1}f = 0$. Zbývá ukázat, že každé $n/s \in \mathrm{Ker}(S^{-1}g)$ leží v $\mathrm{Im}(S^{-1}f)$. Ovšem $g(n)/s = 0$ značí existenci $u \in S$, jež splňuje $ug(n) = g(un) = 0$. Je tedy $un = f(m)$ pro nějaké $m \in M$, a tedy $(S^{-1}f)(m/us) = un/us = n/s$. □

Injektivitu $f\colon M \to N$ lze vyjádřit jako exaktnost $0 \longrightarrow M \xrightarrow{f} N$. Podobně surjektivitě $f\colon M \to N$ odpovídá exaktnost $M \xrightarrow{f} N \longrightarrow 0$. Proto z tvrzení VI.2.5 okamžitě vyplývá, že funktor S^{-1} převádí monomorfismy na monomorfismy a epimorfismy na epimorfismy.

Typickou (krátkou) exaktní posloupností je

$$0 \longrightarrow L \xrightarrow{i} M \xrightarrow{\pi} M/L \longrightarrow 0,$$

kde i je vložení podmodulu L od M a π je projekce modulo L. Z ní dostaneme posloupnost

$$0 \longrightarrow S^{-1}L \xrightarrow{S^{-1}i} S^{-1}M \xrightarrow{S^{-1}\pi} S^{-1}(M/L) \longrightarrow 0,$$

Ta je opět exaktní a $\{m/s;\ m \in L \text{ a } s \in S\} = \mathrm{Im}(S^{-1}i)$ je podmodul $S^{-1}M$. V tomto smyslu je možno $S^{-1}L$ považovat za podmodul $S^{-1}M$. Prvky podmodulu ovšem mohou mít i vyjádření m/s, kde m neleží v L.

Z exaktnosti posloupnosti dále vyplývá

VI.2.6 Důsledek. *Ať S je multiplikativní množina komutativního okruhu R a ať L je podmodul R–modulu M. Pak*

$$S^{-1}(M/L) \cong S^{-1}M/S^{-1}L,\ (m + L)/s \mapsto (m/s) + S^{-1}L.$$

Je-li A modul nad komutativním okruhem R, tak jeho *nosič* $\mathrm{Supp}(A)$ definujeme jako $\{P \in \mathrm{Spec}(R);\ A_P \neq 0\}$. Přitom $\mathrm{Spec}(R)$ značí množinu všech prvoideálů R a A_P je modul $(R \setminus P)^{-1}A$.

VI.2.7 Lemma. *Modul A nad komutativním okruhem R je nulový právě když $A_P = 0$ pro každé $P \in \mathrm{Spec}(R)$. Přitom toto nastane právě když $A_M = 0$ pro každý maximální ideál M okruhu R.*

Důkaz. Je-li A nulový, je $A_P = 0$ pro všechna $P \in \mathrm{Spec}(R)$. Maximální ideály jsou prvoideály. Je tedy třeba ukázat, že pokud $A_M = 0$ pro každé M maximální, tak $A = 0$. Postupujme sporem a uvažme nenulové $a \in A$. Jeho anihilátor $(0 : a)$ je vlastní ideál, a tedy je obsažený v nějakém maximálním, řekněme M. Rovnost $a/1 = 0/1$ nastat nemůže, neboť ta by znamenala existenci $u \in R \setminus M$, jež splňuje $ua = 0$. Takové u by totiž padlo do $(0 : a)$ a nemohlo by ležet mimo M. □

Je-li P prvoideál a $f : L \to A$ homomorfismus modulů, tak místo $(R \setminus P)^{-1}f$ píšeme f_P.

VI.2.8 Důsledek. *Ať $f : L \to A$ je homomorfismus modulů komutativního okruhu R. Následující je ekvivalentní:*

(i) homomorfismus f je injektivní (resp. surjektivní);

(ii) $f_P : L_P \to A_P$ je injektivní (resp. surjektivní) pro každé $P \in \mathrm{Spec}(R)$; a

(iii) $f_M : L_M \to A_M$ je injektivní (resp. surjektivní) pro každý maximální ideál M okruhu R.

Důkaz. Implikace $(i) \Rightarrow (ii)$ plyne z tvrzení VI.2.5 a implikace $(ii) \Rightarrow (iii)$ je triviální. Důkaz $(iii) \Rightarrow (i)$ provedeme zvlášť pro injektivitu a surjektivitu.

Předpokládejme nejprve, že všechny homomorfismy f_M jsou injektivní. Exaktní posloupnost $0 \longrightarrow \mathrm{Ker}(f) \xrightarrow{i} L \xrightarrow{f} A$ přejde na exaktní posloupnost

$$0 \longrightarrow (\mathrm{Ker}(f))_M \xrightarrow{i_M} L_M \xrightarrow{f_M} A_M.$$

Přitom i_M je injektivní a $\mathrm{Ker}(f_M)$ nulové. Je tedy $(\mathrm{Ker}(f))_M = 0$ pro všechna M, a tedy $\mathrm{Ker}(f) = 0$, dle lemmatu VI.2.7.

Pro surjektivitu se podobně uváží exaktní posloupnost

$$L \xrightarrow{f} A \xrightarrow{\pi} A/\,\mathrm{Im}(f) \longrightarrow 0.$$

□

VI.3 Lokalizace a celistvost

Uvažme komutativní okruhy $R \subseteq S$ a ať $U \subseteq R$ je multiplikativní množina. Pak je možné zkonstruovat okruhy $U^{-1}R$ i $U^{-1}S$. Z definice sčítání a násobení v $U^{-1}R$ vyplývá, že $U^{-1}R$ lze přirozeně homomorfně zobrazit do $U^{-1}S$ (to jest zlomek r/u v $U^{-1}R$ přejde na zlomek r/u v $U^{-1}S$). Toto zobrazení je injektivní, neboť podmínka $r_1/u_1 = r_2/u_2$ značí existenci $v \in U$, jež splňuje $v(r_1u_2 - r_2u_1) = 0$, a tato podmínka je stejná v $U^{-1}R$ i $U^{-1}S$. Můžeme tedy $U^{-1}R$ ztotožňovat s podokruhem $U^{-1}S$.

VI.3.1 Lemma. *Je-li $S \supseteq R$ celistvé rozšíření R, je $U^{-1}S$ celistvé rozšíření $U^{-1}R$, a to pro každou multiplikativní množinu $U \subseteq R$.*

Důkaz. Uvažme $s/u \in U^{-1}S$ a ať $r_0, \dots, r_{n-1} \in R$ jsou takové, že $s^n + r_{n-1}s^{n-1} + \dots + r_1s + r_0 = 0$. Pak

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

□

VI.3.2 Tvrzení. *Ať $R \subseteq S$ jsou komutativní okruhy a ať je R' celistvý uzávěr R v S. Buď ještě $U \subseteq R$ multiplikativní množina. Pak je $U^{-1}R'$ celistvý uzávěr $U^{-1}R$ v $U^{-1}S$.*

Důkaz. Z lemmatu VI.3.1 plyne, že $U^{-1}R'$ je nad $U^{-1}R$ celistvé. Uvažme $s/u \in U^{-1}S$, které je celistvé nad $U^{-1}R$. Existují tedy $r_0, \dots, r_{n-1} \in R$ a $u_0, \dots, u_{n-1} \in U$ takové, že

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

Položme $v = u_0 \cdots u_{n-1}$. Vynásobením $v^nu^n/1$ dostaneme $r'_0, \dots, r'_{n-1} \in R$ taková, že

$$(v^ns^n + r'_{n-1}(vs)^{n-1} + \dots + r'_1(vs) + r'_0)/1 = 0,$$

takže $w(v^ns^n + r'_{n-1}(vs)^{n-1} + \dots + r'_1(vs) + r'_0) = 0$ pro nějaké $w \in U$. Vidíme, že wvs je celistvé nad R. To ovšem znamená $wvs \in R'$ a $s/u = (wvs)/(wvu) \in U^{-1}R'$. □

VI.3.3 Tvrzení. *Ať je R obor integrity. Potom je ekvivalentní:*

(i) R je celistvě uzavřené;

(ii) R_P je celistvě uzavřené pro každý prvoideál $P \subseteq R$;

(iii) R_M je celistvě uzavřené pro každý maximální ideál $M \subseteq R$.

Důkaz. Označme T podílové těleso oboru integrity R. Okruh R_P, $P \in \operatorname{Spec}(R)$, je podokruh T. Současně je R_P možno vnořit do T, takže T lze považovat za podílové těleso R_P. Označme S celistvý uzávěr R v T a ať $i\colon R \to S$ je vložení. Podle tvrzení VI.3.2 je S_P celistvý uzávěr R_P. Přitom R je celistvě uzavřené právě když i je surjektivní. Zbytek plyne z důsledku VI.2.8. □

VI.3.4 Tvrzení. *Ať $R \subseteq S$ jsou komutativní okruhy, přičemž S je celistvý nad R. Jsouli $Q_1, Q_2 \in \operatorname{Spec}(S)$ takové, že $Q_1 \cap R = Q_2 \cap R$, tak $Q_1 = Q_2$.*

Důkaz. Položme $Q = Q_1 \cap Q_2$, $P = Q \cap R = Q_1 \cap R = Q_2 \cap R$ a $U = R \setminus P$. Okruh $U^{-1}R = R_P$ lze přirozeným způsobem chápat jako podokruh $U^{-1}S$. Podle tvrzení VI.2.3 je $U^{-1}Q$ prvoideál okruhu $U^{-1}S$. Prvek $r/u \in R_P$ padne do $U^{-1}Q$ právě když $r/u = q/v$ pro nějaká $u, v \in U$ a $q \in Q$. V takovém případě existuje $w \in U$, jež splňuje $wvr = wuq$. Máme $wuq \in Q$ a $wv \notin Q$. Proto $r \in Q \cap R = P$. Vidíme, že $(U^{-1}Q) \cap R_P = U^{-1}P = PR_P$. Ovšem PR_P je jediný maximální ideál kvazilokálního okruhu R_P. To podle tvrzení III.2.12 znamená, že $U^{-1}Q$ je maximální ideál okruhu $U^{-1}S$, neboť $U^{-1}S$ je podle tvrzení VI.3.2 nad $U^{-1}R$ celistvý. Ideály $U^{-1}Q \subseteq U^{-1}Q_1$ se podle tvrzení VI.2.3 rovnají právě když $Q = Q_1$. Ovšem $U^{-1}Q = U^{-1}Q_1$ plyne z maximality $U^{-1}Q$, a tím pádem $Q = Q_1 = Q_2$. □

VI.3.5 Tvrzení. *Ať $R \subseteq S$ jsou komutativní okruhy, přičemž S je nad R celistvé. Pak pro každé $P \in \mathrm{Spec}(R)$ existuje $Q \in \mathrm{Spec}(S)$, jež splňuje $P = Q \cap R$.*

Důkaz. Položme opět $U = R \setminus P$ a uvažme $R_P = U^{-1}R$ jako podokruh $U^{-1}S$. V $U^{-1}S$ zvolme nějaký maximální ideál, dle tvrzení VI.2.3 má tvar $U^{-1}Q$, kde $Q \in \mathrm{Spec}(S)$. Podle tvrzení VI.3.2 a III.2.12 je maximalita $U^{-1}Q$ ekvivalentní maximalitě $(U^{-1}Q) \cap R_P$. Ovšem v R_P je jediný maximální ideál, a to $PR_P = U^{-1}P$. Máme tedy $(U^{-1}Q) \cap R_P = U^{-1}P$. Prvek $r/u \in R_P$ leží v $U^{-1}Q$ právě když $r \in Q \cap R$. takže $(U^{-1}Q) \cap R_P = U^{-1}(Q \cap R)$. Dostáváme $P = Q \cap R$, vše dle lemmatu VI.2.3. □

Bylo by příjemné tvrzení VI.3.4 a VI.3.5 zesílit tak, abychom pro libovolné prvoideály $P_1 \subsetneq P_2$ okruhu R uměli doplnit jeden z prvoideálů $Q_1 \subsetneq Q_2$ okruhu S, kde $Q_1 \cap R = P_1$ a $Q_2 \cap R = P_2$, je-li druhý z nich zadán. Případ, kdy je zadáno Q_2, je těžší a v tvrzení VI.3.9 ho vyřešíme pro R celistvě uzavřený obor integrity, který je obsažen v oboru integrity S.

Uvažme nyní situaci, kdy je zadán ideál Q_1. Okruh S/Q_1 je zjevně celistvý nad $(R + Q_1)/Q_1 \cong R/P_1$, takže podle tvrzení VI.3.5 existuje provideál $Q_2 \in \mathrm{Spec}(S)$ takový, že $Q_2 \supseteq Q_1$ a $(Q_2/Q_1) \cap ((P + Q_1)/Q_1) = (P_2 + Q_1)/Q_1$. To znamená $Q_2 \cap (R+Q_1) = P_2+Q_1$, a tedy $P_2 = R \cap (P_2+Q_1) = R \cap Q_2 \cap (R+Q_1) = R \cap Q_2 \cap P_1 = R \cap Q_2$.

Je-li zadán řetězec $P_1 \subseteq P_2 \subseteq \cdots \subseteq P_m$ prvoideálů z R a jeden prvoideál $Q_1 \in \mathrm{Spec}(S)$, $Q_1 \cap R = P_1$, tak lze induktivním postupem získat $Q_i \in \mathrm{Spec}(S)$. $1 \leq i \leq m$, tak, aby $Q_i \cap R = P_i$. Toto pozorování zaznamenáme jako

VI.3.6 Tvrzení. *Ať $R \subseteq S$ jsou komutativní okruhy, přičemž S je nad R celistvé. Ať $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ je řetězec prvoideálů okruhu R a ať $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_h$, $h \leq n$, je takový řetězec prvoideálů okruhu S, že $Q_i \cap R = P_i$ pro každé i, $1 \leq i \leq h$. Pak v S lze nalézt prvoideály Q_j, $1 \leq j \leq n$, takové, že $Q_h \subsetneq Q_{h+1} \subsetneq \cdots \subsetneq Q_n$ a $Q_j \cap R = P_j$.*

VI.3.7 Lemma. *Ať $R \subseteq S$ jsou komutativní okruhy, přičemž S je nad R celistvé. Je-li I ideál R, tak*

$$\sqrt{IS} = \{s \in S; s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0 = 0$$

pro nějaké $n \geq 1$ a $a_0, a_1, \ldots, a_{n-1} \in I\}$.

Důkaz. Uvažme $s \in \sqrt{IS}$. Pak $s^h = \sum a_i s_i$, $1 \leq i \leq n$, kde $a_i \in I$ a $s_i \in S$, pro nějaká $h, n \geq 1$. Okruh $M = R[s, s_1, \ldots, s_n]$ je podle tvrzení III.2.5 konečně generovaný R–modul a $s^h M$ leží v IM, neboť každé $a_i s_i$ leží v IM. Okruh M je věrný jako M–modul, a protože obsahuje R, je věrný také jako R–modul. Proto z tvrzení III.2.2 můžeme odvodit existenci $b_0, \ldots, b_{m-1} \in I$ takových, že

$$(s^h)^m + b_{m-1}(s^h)^{m-1} + \cdots + b_1 s^h + b_0 = 0,$$

pro nějaké $m \geq 1$. Tím jsme ovšem současně dostali hledaný monický polynom.

Naopak, ať $s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0 = 0$ pro nějaké $n \geq 1$ a $a_0, a_1, \ldots, a_{n-1} \in I$. Potom $s^n = -(a_0 + a_1 s + \cdots + a_{n-1}s^{n-1}) \in IS$. □

VI.3.8 Tvrzení. *Ať $R \subseteq S$ jsou komutativní okruhy, přičemž S je nad R celistvé a R je celistvě uzavřené. Ať je dále T podílové těleso R a I ideál R. Pak pro každé $s \in IS$ platí, že je nad T algebraické, a že všechny koeficienty jeho minimálního polynomu (s výjimkou koeficientu vedoucího) leží v $\sqrt{I}$.*

Důkaz. O s předpokládáme, že je celistvé nad R. Tím spíše je samozřejmě algebraické nad T. Buď $a = \sum a_i x^i$ minimální polynom s. Podle tvrzení VI.3.6 existuje monický polynom b, jenž má kořen s a jehož koeficienty, kromě vedoucího, leží v I. Uvažme nějaké rozšíření T, řekněme V, ve kterém se a rozkládá na lineární činitele. Ať $s = s_1, \ldots, s_h$ jsou všechny kořeny a v tomto rozkladu. Protože a dělí b, jsou $s_1, \ldots, s_h$ také kořeny b. Tím pádem jsou $s_1, \ldots, s_h \in V$ celistvé nad R a okruh $M = R[s_1, \ldots, s_h]$ je jako R–modul konečně generovaný. Přitom všechny koeficienty a_i padnou do M. To znamená, že a_i jsou nad R celistvé, a z celistvé uzavřenosti R v T vyplývá, že $a_i \in R$, a tedy $a \in R[x]$ (zde víceméně opakujeme argumentaci tvrzení III.2.9).

Použijeme-li lemma VI.3.7 na $s_1, \ldots, s_h$, vidíme, že všechny tyto prvky leží v $\sqrt{IM}$. Je-li a_i koeficient a, který není vedoucím koeficientem, tak a_i padne do $\sqrt{IM}$ také. Z toho vyplývá, opět použitím tvrzení VI.3.6, že a_i lze získat jako kořen monického polynomu, jehož koeficienty (vyjma vedoucího) leží v I. Ovšem $a_i \in R$, takže zpětným uplatněním lemmatu VI.3.7 (pro případ $R = S$) dostaneme $a_i \in \sqrt{I}$. □

VI.3.9 Tvrzení. *Ať $R \subseteq S$ jsou obory integrity, přičemž S je nad R celistvé a R je celistvě uzavřené. Ať*

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

je řetězec prvoideálů oboru R. Ať m a h jsou celá čísla, $n \geq m \geq h \geq 0$ a ať

$$Q_h \subsetneq Q_{h+1} \subsetneq \cdots \subsetneq Q_{m-1} \subsetneq Q_m$$

jsou prvoideály S, jež splňují $Q_i \cap R = P_i$, $h \leq i \leq m$. Pak pro i takové, že $0 \leq i < h$ a $m < i \leq n$ lze sestrojit prvoideály Q_i oboru S, jež splňují $Q_i \cap R = P_i$ a tvoří řetězec

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

Důkaz. Připomeňme si situaci uvažovanou mezi tvrzeními VI.3.5 a VI.3.6. K prvoideálům $P_1 \subsetneq P_2$ okruhu R je třeba doplnit jeden z prvoideálů $Q_1 \subsetneq Q_2$ okruhu S, je-li druhý z nich zadán, přičemž $Q_1 \cap R = P_1$ a $Q_2 \cap R = P_2$. Případ zadaného Q_1 jsme vyřešili, což vedlo na tvrzení VI.3.6, které lze zde použít pro doplnění prvoideálů směrem vzhůru. Vyřešíme-li za daných předpokladů případ, kdy je zadáno Q_2, bude možné doplnit i prvoideály směrem dolů. Budeme tedy hledat Q_1.

Položme $U = S \setminus Q_2$ a $V = R \setminus P_1$. Jde o multiplikativní množiny, a proto je multiplikativní množinou i $W = UV = \{uv;\ u \in U \text{ a } v \in V\}$ (v W neleží nula, protože S je obor integrity).

Označme T podílové těleso R (přitom T chápeme jako podtěleso podílového tělesa S). Ať s je prvek ležící v $P_1S \cap W$. Z $s \in P_1S$ vyplývá, že s je algebraické nad K a má minimální polynom $a = x^h + a_{h-1}x^{h-1} + \cdots + a_1x + a_0$, pro který platí $a_i \in P_1 = \sqrt{P_1}$, $0 \leq i < h$, a to dle tvrzení VI.3.8. Z $s \in W$ plyne existence $u \in U$ a $v \in V$ takových, že $s = uv$. Máme

$$u^h v^h + a_{h-1}u^{h-1}v^{h-1} + \cdots + a_1uv + a_0 = 0,$$

takže $u = s/v$ je kořenem polynomu

$$b = x^h + \frac{a_{h-1}}{v}x^{h-1} + \cdots + \frac{a_1}{v^{h-1}}x + \frac{a_0}{v^h} \in K[x].$$

Pokud by bylo $b = \left(\sum_{i=0}^k \alpha_i x^i\right)\left(\sum_{j=0}^m \beta_j x^j\right)$, kde α_i a β_j leží v K a $k+m=n$, tak součin

$$\left(\sum_{i=0}^{k} \alpha_i v^{-i} x^i\right) \cdot \left(\sum_{j=o}^{m} \beta_j v^{h-j} x^j\right)$$

by poskytoval polynom, jehož r–tý koeficient, $0 \leq r \leq h$, by se rovnal

$$\left(\sum_{i+j=r} \alpha_i \beta_j\right) v^{h-r} = (a_r/v^{h-r})v^{h-r} = a_r,$$

takže bychom obdrželi rozklad ireducibilního polynomu a. Vidíme, že $b \in K[x]$ je ireducibilní, takže b je minimálním polynomem prvku $u \in S$ nad K. Koeficienty b ovšem leží v R (použij tvrzení III.2.9 nebo tvrzení VI.3.8 pro $I = R$). Tudíž pro každé i, $0 \leq i < h$, existuje $\rho_i \in R$ takové, že $a_i = v^{h-i}\rho_i$. Jelikož $a_i \in P_1$ a $v^{h-i} \notin P_1$, je $\rho_i \in P_1$. Máme $\rho_{h-2} = a_{h-i}/v^i$, takže symetrickou úvahou jako výše (po záměně u a v) zjistíme, že $x^h + \rho_{h-1}x^{h-1} + \cdots + \rho_1 x + \rho_0$ je minimální polynom u nad K. Z lemmatu VI.3.7 plyne $u \in \sqrt{P_1S} \subseteq \sqrt{P_2S} \subseteq \sqrt{Q_2} = Q_2$. Současně $u \in U = S \setminus Q_2$, a to je spor. Dokázali jsme, že je $P_1S \cap W = \emptyset$.

Podle tvrzení I.3.7 existuje $Q_1 \in \operatorname{Spec}(S)$ takové, že $Q_1 \cap W = \emptyset$ a $P_1S \subseteq Q_1$. Jistě $P_1 \subseteq P_1S \cap R \subseteq Q_1 \cap R$ a z $Q_1 \cap W = \emptyset$ plyne $P_1 = Q_1 \cap R$, neboť $V = R \setminus P_1 \subseteq W$. Podobně musí být $Q_1 \subseteq Q_2$, neboť $U = S \setminus Q_2$ leží také v W. Důkaz je u konce. $\square$

Tuto kapitolu uzavřeme další aplikací lokalizace, tentokrát ji použijeme pro rozšiřování homomorfismů. Začneme lemmatem VI.3.10, které v sobě zahrnuje několik obratů, jež jsme již dříve použili. Připomeňme, že pro komutativní okruhy $R \subseteq S$, $U \subseteq R$ multiplikativní množina, lze ztotožňovat zlomky r/u z $U^{-1}R$ se stejnými zlomky z $U^{-1}S$.

VI.3.10 Lemma. *Ať $R \subseteq S$ jsou komutativní okruhy, přičemž S je nad R celistvé, a ať $P \in \mathrm{Spec}(R)$ a $Q \in \mathrm{Spec}(S)$ jsou taková, že $Q \cap R = P$. Položme $U = R \setminus P$. Pak $U^{-1}Q \cap U^{-1}R = U^{-1}P$ a $U^{-1}Q$ je maximální ideál $U^{-1}S$. Diagram*

$$\begin{tikzcd}
0 \arrow[r] & U^{-1}P \arrow[r] \arrow[d] & U^{-1}R \arrow[r] \arrow[d] & U^{-1}R/U^{-1}P \arrow[r] \arrow[d, "j"] & 0 \\
0 \arrow[r] & U^{-1}Q \arrow[r] & U^{-1}S \arrow[r] & U^{-1}S/U^{-1}Q \arrow[r] & 0
\end{tikzcd}$$

je komutativní a oba jeho řádky jsou exaktní. Přitom

$$j{:}U^{-1}R/U^{-1}P \to U^{-1}S/U^{-1}Q,\ (u/r + U^{-1}P) \mapsto (u/r + U^{-1}Q)$$

je injektivní homomorfismus těles. Těleso $U^{-1}S/U^{-1}Q$ je nad $\mathrm{Im}(j)$ *algebraické.*

Důkaz. Jistě je $U^{-1}P \subseteq U^{-1}Q \cap U^{-1}R$. Ať $a/u \in U^{-1}R$ je rovno $r/v \in U^{-1}R$. Pak pro nějaké $w \in U$ máme $wva \in Q$ rovno wur. OVšem z $wur \in Q$ a $wu \in U \subseteq S \setminus Q$ plyne $r \in Q \cap R = P$. Okruh $U^{-1}R = R_P$ je kvazilokální a $U^{-1}P = P_P$ je jeho jediný maximální ideál. Z $U^{-1}Q \cap U^{-1}R = U^{-1}P$ plyne, že $U^{-1}Q$ je maximální ideál $U^{-1}S$, dle tvrzení $III.2.12$.

Máme $U^{-1}R/U^{-1}P = U^{-1}R/(U^{-1}Q \cap U^{-1}R) \cong (U^{-1}R + U^{-1}Q)/U^{-1}Q$, což je podokruh $U^{-1}S$. Vidíme, že homomorfismus J je určen třetí větou o isomorfismu pro okruhy. Z maximality $U^{-1}P$ a $U^{-1}Q$ vyplývá, že oba faktorokruhy jsou tělesa. Podle lemmatu VI.3.1 je $U^{-1}S$ nad $U^{-1}R$ celistvé, z čehož okamžitě plyne, že jde o algebraické rozšíření těles. □

VI.3.11 Tvrzení. *Ať $R \subseteq S$ jsou komutativní okruhy, přičemž S je nad R celistvé, a ať K je komutativní těleso algebraicky uzavřené. Každý homomorfismus $\varphi{:}R \to K$ lze alespoň jedním způsobem prodloužit na homomorfismus $\psi{:}S \to K$.*

Důkaz. Ideál $P = \mathrm{Ker}(\varphi)$ okruhu R je jeho prvoideálem, neboť R/P je jakožto podokruh K oborem integrity. Podle tvrzení VI.3.5 existuje $Q \in \mathrm{Spec}(S)$ takové, že $Q \cap R = P$. Exaktní posloupnost

$$0 \longrightarrow P \longrightarrow R \xrightarrow{\varphi} T$$

přejde podle tvrzení VI.2.5 na exaktní posloupnost

$$0 \longrightarrow U^{-1}P \longrightarrow U^{-1}R \xrightarrow{U^{-1}\varphi} T,$$

takže existuje $\mu{:}U^{-1}R/U^{-1}P \to T$ homomorfismus těles takový, že $\mu\pi = U^{-1}\varphi$, kde $\pi: U^{-1}R \to U^{-1}R/U^{-1}P$ je přirozená projekce. Označíme-li $f: R \to U^{-1}R$ kanonický homomorfismus, je $\varphi = \mu\pi f$.

Uvažme nyní diagram dle lemmatu VI.3.10 a ať $\sigma : U^{-1}S \to U^{-1}S/U^{-1}Q$ označuje přirozenou projekci a $g{:}S \to U^{-1}S$ kanonický homomorfismus (přitom g chápeme jako rozšíření f). Protože $U^{-1}S/U^{-1}Q$ je nad $\mathrm{Im}(j) \cong U^{-1}R/U^{-1}P$ algebraické, existuje $\nu : U^{-1}S/U^{-1}Q \to K$ takové, že $\nu j = \mu$. Homomorfismus $\mu\sigma g{:}S \to K$ je hledaným rozšířením φ, neboť pro $r \in R$ je $\mu\sigma g(r) = \mu j \pi f(r) = \varphi(r)$. □

VI.3.12 Tvrzení. *Ať R je je podokruh tělesa T a ať a je nenulový prvek T. Každý homomorfismus $\varphi{:}R \to K$, kde K je alebraicky uzavřené těleso, lze rozšířit na homomorfismus $S \to K$, kde $S \subseteq T$ je rovno $R[a]$ nebo $R[a^{-1}]$.*

Důkaz. Položme $P = \mathrm{Ker}(\varphi)$. Pak $\varphi_P{:}R_P \to K$ a R_P lze pokládat za meziokruh $R \subseteq R_P \subseteq T$. Tvrzení proto stačí dokázat za předpokladu, že $R = R_P$, tedy za předpokladu, že $P = \mathrm{Ker}(\varphi)$ je jediným maximálním ideálem R. Rozlišíme případy $PR[a] = R[a]$ a $R[a] \supsetneq PR[a]$. V prvém z nich z $1 \in PR[a]$ dostaneme $1 = \sum c_i a^i$, $0 \le i \le n$, kde $c_i \in P$. To znamená $a^{-n} = \sum c_i a^{i-n}$, a tedy $(1 - c_0)a^{-n} = \sum c_{n-j}(a^{-1})^j$, $0 \le j \le n-1$. Z $c_0 \in P$ plyne $1 - c_0 \in R \setminus P$, takže $1 - c_0$ je invertibilní (neleží v žádném vlastním ideálu), a proto je a^{-1} nad R celistvé. Homomorfismus φ lze proto podle tvrzení VI.3.11 prodloužit na homomorfismus $R[a^{-1}] \to K$.

Ať je nyní $PR[a]$ vlastním ideálem $R[a]$. Pak existuje maximální ideál M okruhu $R[a]$, který $PR[a]$ obsahuje. Jistě $P \subseteq M \cap R \subsetneq R$, a tedy $P = M \cap R$, z maximality P. Vidíme, že $R/P = R/(M \cap R) \cong (R + M)/M$ je těleso, které lze pokládat za podtěleso $R[a]/M$. Přitom $R[a]/M = ((R + M)/M)[a + M$, takže $R[a]/M$ je algebraickým rozšířením R/P. Označme $\pi : R \to R/P$ a $\sigma : R[a] \to R[a]/M$ po řadě přirozené projekce a ať $\mu : R/P \to K$ je takové, že $\varphi = \mu\pi$. Pak μ lze rozšířit na $\gamma : R[a]/M \to K$ a rozšíření φ na $\psi : R[a] \to K$ obdržíme tak, že položíme $\psi = \gamma\sigma$ (jde o obdobný postup jako v závěru důkazu lemmatu VI.3.10). □

VI.4 Dimenze a stupeň transcendence

Nechť R je komutativní okruh a P jeho prvoideál. Uvažme všechny posloupnosti $P_0, \dots, P_n$ prvoideálů z R takové, že $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = P$. Nejvyšší možné n, pokud existuje, nazveme *výškou* P. Pokud lze n zvolit libovolně velké, je výška n rovna ∞. Výšku P značíme $\mathrm{ht}\, P = \mathrm{ht}_R\, P$ (z anglického height).

Supremum všech $\mathrm{ht}\, P$, $P \in \mathrm{Spec}(R)$, se nazývá *dimenzí* R.

Každý prvoideál je obsažen v nějakém prvoideálu maximálním, takže dimenze R je vlastně rovna supremu výšek maximálních ideálů.

Některé základní vztahy výšky $\mathrm{ht}\, P$ a dimenze $\dim R$ je možno zmínit na úrovni víceméně samozřejmých pozorování. Tak například při určení $\dim R/I$ se zjevně vychází z řetězců prvoideálů, jež splňují $I \subseteq P_0 \subsetneq \cdots \subsetneq P_n$. Pro $P \in \mathrm{Spec}(R)$ tedy máme

$$\mathrm{ht}\, P + \dim R/P \le \dim R.$$

Je-li S multiplikativní podmnožina R, tak ze znalosti korespondence prvoideálů $S^{-1}R$ a prvoideálů R (viz tvrzení VI.2.3) dostáváme

$$\operatorname{ht} P = \operatorname{ht}_{S^{-1}R} S^{-1}P \text{ pro každé } P \in \operatorname{Spec}(R), P \cap S = \emptyset.$$

Pro R kvazilokální s maximálním ideálem M je zjevně $\dim R = \operatorname{ht}_R M$. Jelikož pro libovolný komutativní okruh R je R_P kvazilokální, $P \in \operatorname{Spec}(R)$, dostáváme

$$\dim R_P = \operatorname{ht}_R P \text{ pro každé } P \in \operatorname{Spec}(R).$$

VI.4.1 Tvrzení. *Ať $R \subseteq S$ jsou komutativní okruhy, přičemž S je nad R celistvé. Potom* $\dim R = \dim S$.

Důkaz. Je-li $Q_0 \subsetneq \cdots \subsetneq Q_n$ řetězec prvoideálů S, je $Q_0 \cap R \subsetneq \cdots \subsetneq Q_n \cap R$ podle tvrzení VI.3.4 řetězec prvoideálů stejné délky. Naopak, je-li $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$, tak dle tvrzení VI.3.5 můžeme zkonstruovat $Q_0 \in \operatorname{Spec}(S)$ takové, že $Q_0 \cap R = P_0$. Podle tvrzení VI.3.6 pak existují $Q_i \in \operatorname{Spec}(S)$, $1 \le i \le n$, jež splňují $Q_i \cap R = P_i$ a tvoří řetězec $Q_0 \subsetneq \cdots \subsetneq Q_n$. □

VI.4.2 Důsledek. *Ať $R \subsetneq S$ jsou komutivní okruhy, přičemž S je nad R celistvé. Pak pro každý vlastní ideál I okruhu S platí* $\dim R/(I \cap R) = \dim S/I$.

Důkaz. Jde skutečně o přímý důsledek tvrzení VI.4.1, neboť $R/I \cap R \cong (R+I)/I$ lze pokládat za podokruh S/I. □

VI.4.3 Tvrzení. *Buďte $R \subseteq S$ obory integrity, přičemž S je nad R celistvé a R je celistvě uzavřené. Potom $\operatorname{ht}_S Q = \operatorname{ht}_R(Q \cap R)$ pro každé $Q \in \operatorname{Spec}(S)$.*

Důkaz. Z tvrzení VI.3.4 vidíme, že $\operatorname{ht}_S Q \le \operatorname{ht}_R(Q \cap R)$ (to platí pro libovolné $R \subseteq S$, kde S je celistvé nad R). Je-li $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = Q \cap R$ řetězec prvoideálů R, lze podle tvrzení VI.3.9 nalézt $Q_0 \subsetneq \cdots \subsetneq Q_n$ takové, že $Q_i \in \operatorname{Spec}(S)$, $Q_n = Q$ a $Q_i \cap R = P_i$, $0 \le i \le n$. Odsud opačná nerovnost. □

VI.4.4 Věta. *Ať A je netriviální afinní algebra nad komutativním tělesem K. Pak všechny noetherovské normalizace A mají stejný počet prvků, a ten je roven dimenzi A.*

Důkaz. Z věty VI.1.5 víme, že noetherovské normalizace existují. Ať tedy $y_1, \dots, y_n \in A$ jsou nad K algebraicky nezávislé, přičemž A je nad $K[y_1, \dots, y_n]$ celistvé. Indukcí dle n dokážeme $n = \dim A$.

Případ $n = 0$ nastane právě když A je celistvé nad K, a pak lze použít tvrzeni VI.4.1. Ať je tedy $n > 0$, přičemž pro $n' < n$ výsledek platí.

V $K[y_1, \dots, y_n]$ lze nalézt řetězec prvoideálů $0 \subsetneq (y_1) \subsetneq (y_1, y_2) \subsetneq \cdots \subsetneq (y_1, y_2, \dots, y_n)$ tak, že dimenze A, která je podle tvrzení VI.4.1 rovna dimenzi $K[y_1, \dots, y_n]$, je alespoň n. Uvažme řetězec $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_m$ prvoideálů $K[y_1, \dots, y_n]$. Podle tvrzení VI.1.4 existuje noetherovská normalizace (z_i), $1 \le i \le n$, a číslo d, $0 \le d \le n$, takové, že

$$P_1 \cap K[z_1, \dots, z_n] = \sum_{i>d} z_i K[z_1, \dots, z_n] = (z_{d+1}, \dots, z_n).$$

Přitom podle VI.1.4 je $K[y_1, \dots, y_n]$ celistvé nad $K[z_1, \dots, z_n]$, takže $P_0 \subsetneq P_1$ implikuje $P_1 \cap K[z_1, \dots, z_n] \neq 0$, dle tvrzení VI.3.4. Proto $d < n$.

Uvažme nyní přirozenou projekci $K[y_1, \dots, y_n]$ modulo P_1. Z lemmatu VI.1.1 plyne, že $(\pi(z_1), \dots, \pi(z_d))$ je noetherovskou normalizací pro $K[y_1, \dots, y_n]/P_1$. Z indukčího předpokladu (je $d < n$) a z toho, že v uvažovaném kvocientním okruhu máme řetězec prvoideálů $P_1/P_1 \subsetneq \dots \subsetneq P_m/P_1$ vyplývá $m - 1 \leq d < n$, a tedy $m \leq n$. □

VI.4.5 Důsledek. *Předpokládejme, že obor integrity A je afinní algebrou nad komutativním tělesem K. Potom je dimenze A rovna transcendentnímu stupni L nad K, kde L je podílové těleso A (chápané jako rozšíření K).*

Důkaz. Ať $y_1, \dots, y_n$ je nějaká noetherovská normalizace A. Víme, že A je konečně generovaná, takže $A = K[b_1, \dots, b_h]$ pro nějaké $h > 0$, Z definice podílového tělesa okamžitě plyne $L = K(b_1, \dots, b_h)$. Každý z prvků $b_1, \dots, b_h$ je nad $K[y_1, \dots, y_h]$ celistvý, takže těleso L je algebraickým rozšířením tělesa $K(y_1, \dots, y_n)$. To ale znamená, že transcendentní stupeň L nad K je roven transcendentnímu stupni $K(y_1, \dots, y_n)$ nad K, což je n. □

V dalším ukážeme, že v afinní algebře dimenze n je n rovno délce každého maximálního řetězce prvoideálů.

O řetězci prvoideálů $Q_0 \subsetneq \dots \subsetneq Q_n$ říkáme, že je *nasycený*, jestliže pro žádné i, $1 \leq i \leq n$, nelze nalézt prvoideál P tak, aby bylo $Q_{i-1} \subsetneq P \subsetneq Q_i$.

VI.4.6 Lemma. *Ať $(y_1, \dots, y_n)$ je noetherovská normalizace afinní K–algebry A. Ať $Q_0 \subsetneq Q_1$ je nasycený řetězec prvoideálů A. Potom*

$$Q_0 \cap K[y_1, \dots, y_n] \subsetneq Q_1 \cap K[y_1, \dots, y_n]$$

je nasycený řetězec prvoideálů $K[y_1, \dots, y_n]$.

Důkaz. Položme $P_i = Q_i \cap K[y_1, \dots, y_n]$, $i \in \{0, 1\}$. Z tvrzení VI.3.4 plyne $P_0 \subsetneq P_1$. Uvažme existenci prvoideálu P, $P_0 \subsetneq P \subsetneq P_1$ a ať $(z_1, \dots, z_n)$ je noetherovská normalizce $K[y_1, \dots, y_n]$, jež splňuje

$$P_0 \cap K[z_1, \dots, z_n] = \sum_{i<d} z_i K[z_1, \dots, z_n].$$

Položme $P'_i = P_i \cap K[z_1, \dots, z_n]$, $i \in \{0, 1\}$ a $P' = P \cap K[z_1, \dots, z_n]$. Máme $P'_o \subsetneq P' \subsetneq P'_1$, neboť $K[y_1, \dots, y_n]$ je nad $K[z_1, \dots, z_n]$ celistvé. Z tranzitivity celistvosti plyne, že $(z_1, \dots, z_n)$ je noetherovská normalizace K–algebry A. Z $Q_0 \cap K[z_1, \dots, z_n] = Q_0 \cap K[y_1, \dots, y_n] \cap K[z_1, \dots, z_n] = P_0 \cap K[z_1, \dots, z_n] = P'_0 = \sum_{i>d} z_i K[z_1, \dots, z_n]$ vyplývá, že projekce $\pi: A \to A/Q_0$ se na $K[z_1, \dots, z_n]$ chová jako projekce modulo P'_0. Proto jsou $0 = \pi(P'_0) \subsetneq \pi(P') \subsetneq \pi(P'_1)$ prvoideály okruhu $K[\pi(z_1), \dots, \pi(z_d)]$. Tento okruh je Gaussův, takže je celistvě uzavřený. Současně A/Q_0 je podle lemmatu VI.1.1 nad tímto okruhem celistvé. Okruhy $R = K[\pi(z_1), \dots, \pi(z_d)]$ a $S = A/Q_0$ tedy splňují předpoklady tvrzení VI.3.9. Ideál Q_1/Q_0 je prvoideálem A/Q_0 a z $Q_1 \cap K[z_1, \dots, z_n] = P'_1$ plyne

$Q'_1/Q_0 \cap K[\pi(z_1), \ldots, \pi(z_d)] = \pi(P'_1)$. Podle trvzení VI.3.9 existuje $Q \in \mathrm{Spec}(A)$ takové, že je $0 = Q_0/Q_0 \subsetneq Q/Q_0 \subsetneq Q_1/Q_0$. Tedy $Q_0 \subsetneq Q \subsetneq Q_1$, což je spor s naším původním předpokladem. □

VI.4.7 Věta. *V oboru integrity A, který je afinní algebrou nad komutativním tělesem K a má dimenzi n, má každý maximální řetězec prvoideálů délku přesně n.*

Důkaz. Z důsledku VI.4.5 plyne, že délka maximálního řetězce prvoideálů nemůže přesáhnout n. Naším cílem je ověřit, že nemůže být ostře menší než n.

Podle věty VI.1.5 lze nalézt noetherovskou normalizaci $\{y_1, \ldots, y_n\}$ algebry A. Ať $Q_0 \subsetneq \cdots \subsetneq Q_m$, $m \leq n$, je maximální řetězec prvoideálů A. Z $n = 0$ plyne $m = 0$, což umožňuje pokračování indukce dle n.

Položme $P_i = Q_i \cap K[y_1, \ldots, y_m]$. Máme $P_0 = Q_0 = 0$, neboť A je obor integrity, a z maximality Q_m v A plyne maximalita P_m v $k[y_1, \ldots, y_m]$ (faktory jsou tělesa).

Z lemmatu VI.4.6 dostáváme, že řetězec $P_0 \subsetneq \cdots \subsetneq P_m$ je nasycený. Dokázali jsme, že tento řetězec je maximálním řetězcem prvoideálů v $K[y_1, \ldots, y_m]$.

Je tedy $\mathrm{ht}(P_1) = 1$ a protože $K[y_1, \ldots, y_m]$ je Gaussův, je P_1 nutně shodné s hlavním ideálem nějakého ireducibilního polynomu p. Podle tvrzení VI.1.3 lze tento ideál, řekněme (p), vyjádřit jako $P_1 \cap K[z_1, \ldots, z_n] = z_1 K[z_1, \ldots, z_n]$, kde $(z_1, \ldots, z_n)$ je noetherovská normalizce $K[y_1, \ldots, y_n]$.

Označme π přirozenou projekci $K[y_1, \ldots, y_n]$ modulo P_1. Z tvrzení VI.4.1 plyne, že $(\pi(z_1), \ldots, \pi(z_n))$ je noetherovská normalizace $K[y_1, \ldots, y_n]/P_1$. Tento okruh ovšem má podle věty VI.4.4 dimenzi $n-1$. Současně je $P_1/P_1 \subsetneq \cdots \subsetneq P_m/P_1$ jeho maximální řetězec prvoideálů. Z indukčního předpokladu plyne $n - 1 = m - 1$, a tedy $n = m$. □

VI.5 Valuační obory integrity

Okruh R se nazývá *valuačním okruhem tělesa* $T \supseteq R$, je-li pro každé nenulové $a \in T$ alespoň jeden z prvků a a a^{-1} obsažen v R, přičemž T je komutativní.

Obor integrity R se nazývá *valuační obor* (nebo valuační okruh) právě když je valuačním okruhem svého podílového tělesa.

Obě definice popisují stejnou třídu objektů, neboť komutativní těleso, jež je valuačním okruhem R, je zjevně též jeho tělesem podílovým.

VI.5.1 Tvrzení. *V každém valuačním okruhu jsou ideály lineárně uspořádány inkluzí. Je-li naopak R obor integrity, jehož hlavní ideály jsou lineárně uspo-řádány inkluzí, je R valuační.*

Důkaz. Buďte I a J ideály valuačního oboru R a nechť a je prvek $J \setminus I$. Pak pro $b \in I$ není $b^{-1}a$ prvek R (neboť pak by bylo $a = b \cdot b^{-1}a \in I$), takže je $ba^{-1} \in R$, a tedy $b = ba^{-1} \cdot a \in J$.

Naopak, ať hlavní ideály R jsou lineárně uspořádány inkluzí a ať T je podílové těleso R. Předpokládejme, že $a/b \in T$ neleží v R, $a \neq 0$. Z $a/b \cdot b = a$

plyne, že není $a \in Rb$, takže $Rb \subseteq Ra$. Tedy $b = ra$ pro nějaké $r \in R$. Ovšem $r = b/a = (a/b)^{-1}$. □

Ve valuačním oboru R položme $P = \{a \in R;\ a = 0 \text{ nebo } a^{-1} \notin R\}$. Je-li $a \in P$, $r \in R$, tak je jistě, $ra \in P$. Pro $a, b \in P$ je $Ra \subseteq Rb$ nebo $Rb \subseteq Ra$. V obou případech je $a + b \in P$. Vidíme, že P je ideál R. Protože všechny prvky mimo P jsou invertibilní, musí R být okruh kvazilokální.

VI.5.2 Tvrzení. *Ať $R \subseteq T$ jsou komutativní okruhy, přičemž T je těleso. Následující podmínky jsou ekvivalentní.*

(i) *R je valuační okruh T;*

(ii) *R je kvazilokální s maximálním ideálem P, přičemž pro každý meziokruh S, $R \subseteq S \subseteq T$, platí $R = S$ kdykoliv $P = M \cap R$ pro nějaký maximální ideál M okruhu S;*

(iii) *existuje homomorfismus $\varphi\colon R \to K$, K algebraicky uzavřené komutativní těleso, který nelze rozšířit na žádné $\psi\colon S \to K$, $R \subsetneq S \subseteq T$.*

Důkaz. Předpokládejme, že R je valuační okruh T a že $P = M \cap R$ pro nějaký meziokruh S, M maximální ideál okruhu S. (Z úvahy před dokazovaným tvrzením již víme, že R je kvazilokální.) Předpokládejme existenci $a \in S \setminus R$. Z $a^{-1} \in R$ plyne $a^{-1} \in P$, neboť $(a^{-1})^{-1} = a$ do R nepatří. To ale znamená, že $a \in S$ je invertibilní, neboť S obsahuje jak a tak a^{-1}. Současně $a^{-1} \in P \subseteq M$, a to je spor.

Nyní dokážeme $(ii) \Rightarrow (iii)$. Obor integrity R/P lze vložit do algebraicky uzavřeného K. Budeme dokazovat, že za φ lze zvolit přirozenou projekci $R \to K$, $\varphi(r) = r + P$ pro každé $r \in R$. Každé $\psi\colon S \to K$ rozšiřující φ lze dále rozšířit na $\psi_I\colon S_I \to K$, $I = \mathrm{Ker}(\psi)$, kde $S \subseteq S_I \subseteq T$. Jádrem ψ_I je I_I, jediný maximální ideál S_I. Můžeme tedy předpokládat, že $S = S_I$ a že I je maximální. Máme $I \cap R \supseteq P$, a tedy $I \cap R = P$, takže $S = R$ a $\psi = \varphi$.

Zbývá ověřit $(iii) \Rightarrow (i)$. Ať $\varphi\colon R \to K$ nelze rozšířit. Pak pro každé $a \in T$ je $R[a] = R$ nebo $R[a^{-1}] = R$, dle tvrzení VI.3.12. □

VI.5.3 Tvrzení. *Nechť R je valuační obor integrity, který není tělesem, a ať P je jeho maximální ideál. Položme $I = \cap P^i$, $i \geq 1$, a předpokládejme, že P je konečně generován. Pak existuje $a \in R$, že*

$$I \subsetneq \cdots \subsetneq Ra^{i+1} \subsetneq Ra^i \subsetneq \cdots Ra^2 \subsetneq Ra \subsetneq R$$

jsou právě všechny ideály J, jež splňují $I \subseteq J \subseteq R$. Je-li navíc I konečně generovaný, tak $I = 0$.

Důkaz. Hlavní ideály R jsou do sebe vřazeny. Proto každý konečně generovaný ideál je roven hlavnímu ideálu, který je určen některým z generátorů. Vidíme, že $P = Ra$ pro nějaké $a \in R$, $a \neq 0$. Z $a^i \in Ra^{i+1}$ by plynulo $a^{-1} \in R$, což nelze. Proto je $P^{i+1} = Ra^{i+1}$ vlastní podmnožinou $P^i = Ra^i$ pro každé $i \geq 1$. Je-li $b \in Ra^i \setminus Ra^{i+1}$, tak $a^{-i}b$ leží v R. Pokud by $b^{-1}a^i$ v Rneleželo, měli bychom $a^{-1}b \in P$, tedy $a^{-1} = ar$ pro nějaké $r \in R$, čili $r = a^{-i-1}b \in R$. To by však bylo ve sporu s předpokladem $b \notin Ra^{i+1}$. Vidíme, že $a^{-i}b$ je v R invertibilní, a tedy $bR = a^iR$. Všechny ideály okruhu R/I jsou tudíž hlavní a rovny $(a+I)^i(R/I)$. Zbývá dokázat, že I je nulové, je-li konečně generované. Je-li konečně generované, je hlavní. Ať tedy $I = cR$. Z $c \in a^iR$ plyne $a^{-i}c \in R$ pro každé $i \geq 1$. To znamená $a^{-1}c = a^i(a^{-i-1}c) \in a^iR$ pro všechna $i \geq 1$, a tedy $a^{-1}c \in \cap a^iR = I = cR$. Z $a^{-1}c = cr$ obdržíme pro $c \neq 0$ příslušnost a^{-1} do R. Protože a^{-1} v R neleží, musí být $I = 0$. $\square$

Diskrétním valuačním oborem se míní každý valuační obor R, jehož maximální ideály P a $\cap P^i$, $i \geq 1$, jsou konečně generované. Z tvrzení VI.5.3 vyplývá, že to jsou právě všechny noetherovské valuační obory. Můžeme také použít tuto charakterizaci:

VI.5.4 Tvrzení. *Valuační okruh R je diskrétní právě když obsahuje ideál P takový, že 0, R a P^i, $i \geq 1$, jsou právě všechny ideály R.*

Důkaz. Z tvrzení VI.5.3 vyplývá, že diskrétní valuační obory uvedenou vlastnost mají. Pro důkaz opačným směrem je třeba ověřit, že maximální ideál P valuačního oboru R musí být při daných vlastnostech konečně generovaný. Pokud $P = P^2$ a pokud aR je nenulový vlastní ideál, $a \in R$, tak musí být $aR = P$, neboť z $P^2 = P$ plyne $P = P^i$ pro všechna $i \geq 1$. Ať je $P \setminus P^2$ neprázdné a obsahuje prvek a. Protože a není invertibilní a neleží v žádném P^i, $i \geq 2$, musí být $P = Ra$. $\square$

Zobrazení $\gamma : T^* \to \mathbb{Z}$, kde T je komutativní těleso a $\mathbb{Z}$ je okruh celých čísel, nazveme *diskrétní valuací T*, jestliže je to zobrazení surjektivní, které za předpokladu $\gamma(0) = \infty$ splňuje podmínky

(i) $\gamma(a+b) \geq \min\{\gamma(a), \gamma(b)\}$ pro všechna $a, b \in T$ a

(ii) $\gamma(ab) = \gamma(a) + \gamma(b)$ pro všechna $a, b \in T$.

VI.5.5 Lemma. *Ať R je diskrétní valuační okruh tělesa T, $R \subsetneq T$, a ať aR je maximální ideál R. Potom $0, T$ a a^iR, $i \in \mathbb{Z}$, jsou všechny R–podmoduly T (lomené ideály). Přitom*

$$0 \subsetneq \cdots \subsetneq a^{i+1}R \subsetneq a^iR \subsetneq \cdots \subsetneq aR \subsetneq R \subsetneq \\ a^{-1}R \subsetneq \cdots \subsetneq a^{-i}R \subsetneq a^{-i-1}R \subsetneq \cdots \subsetneq T.$$

Definujme $\nu : T \to \mathbb{Z}$ tak, že $\nu(b) = i$ právě když $b \in a^iR \setminus a^{i+1}R$. Pak je ν diskrétní valuací T.

Důkaz. Uvažme $b \in T$. Je-li $b \in R$, tak $bR = a^iR$ pro právě jedno $i \geq 0$, dle tvrzení VI.5.3. V takovém případě je $a^i = be$ pro $e \in R$ invertibilní. Je-li $b^{-1} \in R$, tak $b^{-1} = a^ie$ pro nějaké $i \geq 0$ a e invertibilní. To znamená $bR = a^{-i}R$. Z $a^{-i}R = a^{-i-1}R$, $i \geq 0$, by plynulo $aR = R$ (vynásobením a^{i+1}), takže v řetězci lomených ideálů žádné dva sousední nemohou splynout. Je-li I nějaký lomený ideál, tak buď $I = 0$, nebo $I = T$, nebo existuje nejmenší $i \in \mathbb{Z}$, jež má s I neprázdný průnik. Pak ale zjevně $I = a^i R$. Z $(a^i R)(a^j R) = a^{i+j} R$ vyplývá, že $\nu(bc) = \nu(b) + \nu(c)$ pro všechna $b, c \in R$. Je-li $b, c \in a^i R$, tak $b + c$ padne do $a^i R$ též. Proto $\nu(b + c) \geq \min\{\nu(b), \nu(c)\}$, pro všechna $b, c \in R$. □

VI.5.6 Tvrzení. *Ať $\nu : T \to \mathbb{Z}$ je diskrétní valuace tělesa T. Potom $R = \{a \in T;\ \nu(a) \geq 0\}$ je diskrétní valuační okruh a ν je jedinou diskrétní valuací T, která R takto určuje.*

Důkaz. Pro $a, b \in R$ je $\nu(a+b) \geq \min\{\nu(a), \nu(b)\} \geq 0$ a $\nu(ab) = \nu(a)+\nu(b) \geq 0$. Současně z $\nu(a \cdot 1) = \nu(a) + \nu(1)$ plyne $\nu(1) = 0$, takže R je opravdu okruh. Dále pro každé $a \in T$ nenulové máme $\nu(aa^{-1}) = \nu(1) = 0 = \nu(a) + \nu(a^{-1})$, a tedy $\nu(a^{-1}) = -\nu(a)$. Prvek $a \in R$ je tudíž invertibilní (splňuje $a^{-1} \in R$) právě když $\nu(a) = 0$. Pokud $\nu(a) = \nu(b)$, tak je $\nu(ab^{-1}) = 0$, a tedy $aR = bR$. Z $\nu(a) \geq \nu(b)$ plyne $ab^{-1} \in R$, a tedy $bR \subseteq aR$. Vybereme nějaké $a \in R$, jež splňuje $\nu(a) = 1$. Vidíme, že pro každé $i \geq 1$ platí $a^i R = \{b \in T;\ \nu(b) \geq i\}$ a že každý vlastní nenulový ideál R má takovýto tvar. Zbytek je zřejmý. □