Časopis pro pěstování matematiky

Oldřich Kowalski

K teorii $\mathfrak{O}$-ideálů v nekomutativních okruzích

Časopis pro pěstování matematiky, Vol. 87 (1962), No. 4, 424--439

Persistent URL: `http://dml.cz/dmlcz/117453`

Časopis pro pěstování matematiky, roč. 87 (1962), Praha

K TEORII $\mathfrak{o}$-IDEÁLŮ V NEKOMUTATIVNÍCH OKRUZÍCH

OLDŘICH KOWALSKI, Brno

(Došlo dne 1. června 1961)

Multiplikativní teorie ideálů v komutativních oborech integrity byla v jistém smyslu dovršena teorií kvazidělitelnosti ideálů vybudovanou VAN DER WAERDENEM. V této práci je rozvinuta obecnější teorie kvazidělitelnosti oboustranných $\mathfrak{o}$-ideálů v nekomutativních okruzích.

ÚVOD

Základním výsledkem multiplikativní teorie ideálů v komutativních oborech integrity je věta objevená E. NOETHEROVOU:

V komutativním oboru integrity $\mathfrak{o}$ lze každý ideál rozložit právě jedním způsobem v součin prvoideálů, když a jen když jsou splněny tyto podmínky:

N1. *$\mathfrak{o}$ je celistvě uzavřený ve svém podílovém tělese.*

N2. *Platí minimální podmínka pro řetězce ideálů obsahujících pevný ideál $\neq \emptyset$.*

N3. *Platí maximální podmínka pro řetězce ideálů v $\mathfrak{o}$.*

Podmínka N2 může být přitom nahrazena tímto předpokladem:

N2'. *Každý prvoideál oboru integrity $\mathfrak{o}$ je maximální.* (Viz [3], kap. 6.)

Poznamenejme, že podmínky N1, 2, 3 resp. N1, 2', 3 jsou také nutné a dostatečné pro to, aby se dal obecněji každý *zlomkový ideál* příslušný k oboru $\mathfrak{o}$ jednoznačně rozložit v součin mocnin prvoideálů.

VAN DER WAERDEN ukázal, že když z předpokladů Noetherové ponecháme v platnosti pouze N1 a N3, pak lze na množině zlomkových ideálů příslušné danému komutativnímu oboru integrity $\mathfrak{o}$ definovat relaci *kvazirovnosti* tak, že *každý zlomkový ideál lze jednoznačně až na pořadí a kvazirovnost rozložit v součin mocnin prvoideálů.* (Viz [5], kap. XIV nebo [2] kap. I.)

Výsledky E. Noetherové byly z jiného hlediska zobecněny v teorii $\mathfrak{o}$-ideálů, jejíž axiomatické základy položil K. ASANO. Byly stanoveny nutné a postačující podmínky pro to, aby se dal každý oboustranný zlomkový $\mathfrak{o}$-ideál příslušný k danému nekomutativnímu okruhu $\mathfrak{o}$ jednoznačně rozložit v součin mocnin konečného počtu $\mathfrak{o}$-prvoideálů. (Viz [3], kap. 6 a § 5 této práce.)

V naší práci byly Waerdenovy myšlenky přeneseny z teorie ideálů v komutativních oborech integrity na teorii $\mathfrak{o}$-ideálů a tím byly dále zobecněny některé klasické výsledky.

Obecná teorie obsažená v §§ 1—4 je rozvíjena v abstraktní svazové formulaci, jaké užívají v multiplikativní teorii ideálů někteří novější autoři (viz např. práci [4]). V § 5 jsou pak obecné závěry aplikovány na teorii $\mathfrak{o}$-ideálů.

1. POJEM l-POLOGRUPY — DOPLŇUJÍCÍ PODMÍNKY

Definice 1. *Nechť množina* $\mathbf{L}$ *má tyto vlastnosti:*

1) $\mathbf{L}$ *je svaz.*
2) $\mathbf{L}$ *je pologrupa s jednotkovým prvkem.*
3) *V* $\mathbf{L}$ *jsou splněny distributivní zákony*

$$a(b \cup c) = ab \cup ac\,, \quad (b \cup c)\,a = ba \cup ca\,. \tag{1}$$

Potom se množina $\mathbf{L}$ *nazývá svazově uspořádaná pologrupa, nebo krátce l-pologrupa.* (Viz [1], str. 280.)

Další označení: Jednotkový prvek pologrupy $\mathbf{L}$ budeme vždy označovat e. *Nulou* l-pologrupy $\mathbf{L}$ nazýváme takový prvek 0, že pro všechna $x \in \mathbf{L}$ platí $0 \,.\, x = x \,.\, 0 = 0$. Pro *horní částečné uspořádání* svazu $\mathbf{L}$ budeme užívat znaku $\leqq$. *Největším prvkem* částečně uspořádané množiny $\mathbf{M} \subset \mathbf{L}$ nazýváme takový prvek $m \in \mathbf{M}$, že platí $x \leqq m$ pro všechna $x \in \mathbf{M}$; podobně se definuje *nejmenší prvek* množiny $\mathbf{M}$.

Snadno se dokáže následující tvrzení (viz [1], str. 280):

1.1. *Nechť* $\mathbf{L}$ *je l-pologrupa. Je-li* $a \leqq b$, *pak pro libovolné prvky* $x, y \in \mathbf{L}$ *platí* $ax \leqq bx$, $ya \leqq yb$.

Definice 2. *Celými prvky l-pologrupy* $\mathbf{L}$ *nazýváme prvky* $x \leqq e$. *Jsou-li všechny prvky v* $\mathbf{L}$ *celé* (tj. *je-li* e *největším prvkem svazu* $\mathbf{L}$), *nazývá se l-pologrupa* $\mathbf{L}$ *celá; v opačném případě se nazývá necelá.*

1.2. *Jsou-li* a, b *celé prvky, pak platí* $ab \leqq a \cap b$.

Důkaz. Platí $a \leqq e$, $b \leqq e$ a tedy podle 1.1 $ab \leqq eb = b$, $ab \leqq ae = a$, odkud plyne dokazované tvrzení.

Zřejmá je následující poučka:

1.3. *Množina* $\mathbf{C}$ *všech celých prvků z* $\mathbf{L}$ *je celá l-pologrupa.*

Definice 3. *Nechť* $\mathbf{I}(a)$ *je množina všech prvků* $x \in \mathbf{L}$, *pro které platí* $axa \leqq a$. *Je-li množina* $\mathbf{I}(a)$ *neprázdná a obsahuje-li největší prvek, nazýváme tento největší prvek inversním prvkem k* a *a označujeme jej symbolem* a^{-1}.

Poznámka. V dalším budeme požadovat aby l-pologrupa $\mathbf{L}$ splňovala některé doplňující podmínky z těch, které zde v souhrnu uvedeme:

(I) *Ke každému prvku $a \in \mathbf{L}$ existuje inversní prvek a^{-1}.*

(II) *Jestliže $ab \leqq a$ resp. $ca \leqq a$, pak $b \leqq e$ resp. $c \leqq e$.*

(III) *Platí maximální podmínka pro řetězce celých prvků v $\mathbf{L}$: Každý rostoucí řetězec $a_1 < a_2 < a_3 < \ldots \leqq e$ celých prvků l-pologrupy $\mathbf{L}$ je konečný.*

1.4. *Platí-li v $\mathbf{L}$ podmínka (II), pak inversní prvek a^{-1} k prvku a (pokud existuje) je jednoznačně určen těmito vlastnostmi:*

(J_1) *$aa^{-1} \leqq e$, $a^{-1}a \leqq e$.*

(J_2) *Kdykoliv $ac \leqq e$ resp. $da \leqq e$, pak $c \leqq a^{-1}$ resp. $d \leqq a^{-1}$.*

Důkaz. Protože $\mathbf{L}$ splňuje podmínku (II), je (J_1) ekvivalentní se vztahem $a^{-1} \in I(a)$ a (J_2) znamená, že kdykoliv $c \in I(a)$ resp. $d \in I(a)$, potom $c \leqq a^{-1}$ resp. $d \leqq a^{-1}$. Takto však byl zřejmě definován inversní prvek a^{-1}.

2. GRUPA TŘÍD

Předpokládejme všude v dalším, že l-pologrupa $\mathbf{L}$ splňuje podmínky (I) a (II).

Definice 4. *Prvky $a, b \in \mathbf{L}$ se nazývají kvazirovné, když $a^{-1} = b^{-1}$.* Označení: $a \sim b$. *Prvek a se nazývá kvazidělitelem (vlastním kvazidělitelem) prvku b, když platí $a^{-1} \leqq b^{-1}$ ($a^{-1} < b^{-1}$).* Označení: $a \gtrsim b$ ($a \succ b$). *Říkáme pak také, že b je kvazinásobkem (vlastním kvazinásobkem) prvku a a píšeme $b \lesssim a$ ($b \prec a$).*

Je zřejmé, že kvazirovnost je ekvivalence, která určuje rozklad $\mathfrak{S}$ množiny $\mathbf{L}$ *na třídy kvazirovných prvků* a kvazidělitelnost je částečné uspořádání definované na tomto rozkladu. Platí totiž $a \sim b$ právě tehdy, když současně $a \lesssim b$ a $a \gtrsim b$. Dokážeme si především několik vlastností kvazirovnosti a kvazidělitelnosti.

2.1. *Je-li $a \leqq b$, pak $a \lesssim b$.*

Důkaz. Platí $ab^{-1} \leqq bb^{-1} \leqq e$ a odtud podle (J_2) $b^{-1} \leqq a^{-1}$.

2.2. *Podmínka $a \lesssim b$ je ekvivalentní s každou z nerovností $ab^{-1} \leqq e$, $b^{-1}a \leqq e$.*

Důkaz. Je-li $a \lesssim b$, pak $b^{-1} \leqq a^{-1}$ a odtud plyne $ab^{-1} \leqq a \,.\, a^{-1} \leqq e$, $b^{-1}a \leqq a^{-1}a \leqq e$. Platí-li naopak $ab^{-1} \leqq e$ nebo $b^{-1}a \leqq e$, pak podle (J_2) $b^{-1} \leqq a^{-1}$.

2.3. *Je-li $a \lesssim b$, pak $a \leqq (b^{-1})^{-1}$.*

Důkaz. Podle 2.2 je $ab^{-1} \leqq e$ a podle (J_2) $a \leqq (b^{-1})^{-1}$ cbd.

2.4. *Prvek $b^* = (b^{-1})^{-1}$ je kvazirovný k b.*

Důkaz. Podle 2.3 platí $b \leqq b^*$ a tedy podle 2.1 $b \lesssim b^*$. Dále poněvadž $b^{-1}b^* \leqq e$, plyne z 2.2 $b^* \lesssim b$. Odtud $b^* \sim b$. Prvek b^* je zřejmě největším prvkem třídy prvku b; budeme jej nazývat *význačným prvkem* této třídy.

2.5. *Je-li $a \lesssim b$, pak $ca \lesssim cb$, $ac \lesssim bc$ pro libovolné $c \in \mathbf{L}$.*

Důkaz. Jelikož $(cb)^{-1}cb \leqq e$, máme podle (J_2) $(cb)^{-1}c \leqq b^{-1} \leqq a^{-1}$. Odtud $(cb)^{-1}ca \leqq a^{-1}a \leqq e$ a podle 2.2 $ca \lesssim cb$. Druhá nerovnost se odvodí obdobně.

2.6. *Je-li* $a \sim b$, *pak* $ac \sim bc$, $ca \sim cb$ *pro* $c \in \mathbf{L}$. (Důsledek 2.5.)

2.7. *Je-li* $a \sim c$, $b \sim d$, *pak* $ab \sim cd$ (plyne z 2.6 a z transitivity).

2.8. *Platí* $e = e^{-1} = e^*$.

Důkaz. Především platí $e^{-1} = ee^{-1} \leqq e$ a ze vztahu $ee \leqq e$ plyne $e \leqq e^{-1}$, celkem tedy $e = e^{-1}$, $e^* = (e^{-1})^{-1} = e^{-1} = e$.

2.9. *Ze vztahu* $a \lesssim e$ *plyne* $a \leqq e$.

Důkaz. Podle 2.8 je $e^* = e$ a podle 2.3 $a \leqq e^*$.

Z 2.7 vidíme, že třída součinu ab závisí jen na třídách obou činitelů a, b; lze proto na rozkladu $\mathfrak{S}$ definovat jednoznačné *násobení*: Označíme-li $\langle x \rangle$ třídu, do níž náleží prvek x, je toto násobení dáno vzorcem

$$\langle a \rangle \langle b \rangle = \langle ab \rangle . \tag{2}$$

Věta 1. *Množina $\mathfrak{S}$ tříd kvazirovných prvků tvoří grupu vzhledem k násobení* (2).

Důkaz. Je zřejmé, že násobení (2) je asociativní a že jeho jednotkovým prvkem je třída $\langle e \rangle$ – tzv. *jednotková třída*. Označme dále $b = (a^{-1}a)^{-1}$; platí $b(a^{-1}a) \leqq e$ a odtud $ba^{-1} \leqq a^{-1}$ podle (J_2), z podmínky (II) plyne $b \leqq e$. Platí tedy $(a^{-1}a)^{-1} \leqq$ $\leqq e = e^{-1}$ a z definice kvazidělitelnosti dostáváme $e \lesssim a^{-1}a$. Na druhé straně platí $a^{-1}a \leqq e$, tedy $a^{-1}a \lesssim e$. Spojení obou nerovností dává vztah $a^{-1}a \sim e$. Podobně se ukáže vztah $aa^{-1} \sim e$. Součin třídy prvku a a třídy inversního prvku a^{-1} je tedy roven jednotkové třídě. Tím je věta dokázána. Předchozí konstrukce doplníme touto existenční větou:

Věta 2. *Nechť l-pologrupa* $\mathbf{L}$ *je necelá (tj. nechť obsahuje aspoň jeden prvek* a, *pro který neplatí* $a \leqq e$). *Potom platí:*

1) *V* $\mathbf{L}$ *neexistuje nula ani největší a nejmenší prvek.*

2) *Příslušná grupa* $\mathfrak{S}$ *tříd je nekonečná.*

Důkaz. *Ad* 1): Důkaz provedeme sporem. Nechť prvek 0 je nulou v $\mathbf{L}$. Pak pro každé $x \in \mathbf{L}$ platí $0x = 0$ a podle (II) $x \leqq e$, $\mathbf{L}$ je tedy celá proti předpokladu. Nechť h je nejmenší prvek v $\mathbf{L}$. Pak platí $h \leqq e$ a z 1.1 plyne $hh = h$. Podle věty 1 platí $h \sim e$, tedy $h^{-1} = e$. Je-li $x \in \mathbf{L}$ libovolné, pak $x^{-1} \geqq h$ a odtud podle 2.3 a 2.1 $x \leqq$ $\leqq (x^{-1})^{-1} \leqq h^{-1}$, tedy $\mathbf{L}$ je opět celá proti předpokladu. Nechť m je největší prvek v $\mathbf{L}$. Pak je $e \leqq m$ a podle 1.1 $mm = m$. Odtud plyne podle věty 1 $m \sim e$, tedy podle 2.9 $m \leqq e$, což je spor.

Ad 2: Nechť $a \in \mathbf{L}$ je necelý prvek. Pak platí $b = a \cup e > e$ a za předpokladu, že $b^n > e$ dostáváme $b^{n+1} = bb^n \geqq b > e$. Tím je dokázáno indukcí, že platí $b^n > e$ pro každé $n \geqq 1$. Podle 2.9 je $\langle b^n \rangle \neq \langle e \rangle$ pro $n = 1, 2, 3, \ldots$ a odtud plyne, že $\langle b^m \rangle \neq \langle b^n \rangle$ pro libovolné celé $m \neq n$. Třídy $\ldots, \langle b^{-2} \rangle, \langle b^{-1} \rangle, \langle e \rangle, \langle b \rangle, \langle b^2 \rangle, \ldots$ tvoří tedy nekonečnou cyklickou podgrupu grupy $\mathfrak{S}$.

V dalším budeme potřebovat ještě následující poučky:

2.10. *Je-li* $a \lesssim b$, *pak existuje prvek* $c \leqq e$ *takový, že platí* $a \sim bc$, $bc \leqq a$ *a prvek* $d \leqq e$ *takový, že platí* $a \sim db$, $db \leqq a$.

Důkaz. Volme $c = b^{-1}a$, pak je podle 2.2 $c \leqq e$ a zřejmě platí $a \sim bc$, $bc = b(b^{-1}a) = (bb^{-1})\, a \leqq a$. Podobně je možno položit $d = ab^{-1}$.

2.11. *Je-li $a \sim b$, pak existují prvky $\varepsilon \sim e$, $\delta \sim e$ takové, že $a\varepsilon = \delta b$.*

Důkaz. Platí $a(a^{-1}b) = (aa^{-1})\, b$.

2.12. *Je-li $a \lesssim b$, pak existují prvky $\varepsilon \sim e$, $\varepsilon' \sim e$ takové, že $\varepsilon a \leqq b$, $a\varepsilon' \leqq b$.*

Důkaz. Z 2.3 a 2.4 plyne $a \leqq b^*$, $b \sim b^*$. Podle 2.11 existují prvky ε, δ, ε', δ' z jednotkové třídy, pro něž platí $b\delta = \varepsilon b^*$, $\delta' b = b^*\varepsilon'$; odtud plyne

$$\varepsilon a \leqq \varepsilon b^* = b\delta \leqq b\,, \quad a\varepsilon' \leqq b^*\varepsilon' = \delta' b \leqq b\,.$$

2.13. *Je-li $a \lesssim b$, $c \lesssim d$, pak $a \cup c \lesssim b \cup d$.*

Důkaz. Podle 2.12 existují prvky $\varepsilon \sim e$, $\delta \sim e$ takové, že $a\varepsilon \leqq b$, $c\delta \leqq d$. Odtud plyne $(a \cup c)\, \varepsilon\delta \leqq a\varepsilon \cup c\delta \leqq b \cup d$ a protože $\varepsilon\delta \sim e$, máme $a \cup c \lesssim b \cup d$ cbd.

3. KVAZIFAKTORISACE V *l*-POLOGRUPĚ

Předně zavedeme několik dalších pojmů:

Definice 5. *Prvek $p \prec e$ se nazývá kvazirozložitelný, jestliže ze vztahů $a \lesssim e$, $b \lesssim e$, $p \sim ab$ plyne buď $a \sim e$ nebo $b \sim e$.*

Definice 6. *Prvek $p < e$ se nazývá prvoelement, jestliže ze vztahů $a \leqq e$, $b \leqq e$, $ab \leqq p$ plyne buď $a \leqq p$ nebo $b \leqq p$.*

Definice 7. *Prvek $q < e$ se nazývá maximální, jestliže neexistuje prvek r různý od q i e, pro který by platilo $q \leqq r \leqq e$.*

Následující poučka platí pro libovolnou *l*-pologrupu (která nemusí splňovat žádnou z podmínek (I), (II)):

3.1. *Každý maximální prvek v $\mathbf{L}$ je prvoelement.*

Důkaz. Nechť p je maximální prvek a nechť platí $a \leqq e$, $b \leqq e$, $ab \leqq p$. Pak také $(a \cup p)(b \cup p) \leqq p$. Kdyby nebyl splněn žádný ze vztahů $a \leqq p$, $b \leqq p$, plynulo by snadno z definice maximálního prvku $a \cup p = b \cup p = e$ a tedy $e \leqq p$, což je spor. Podle definice 6 je tedy p prvoelement.

V následujícím lemmatu podáme jinou charakteristiku kvazinerozložitelných prvků:

Lemma 1. *Prvek $p \prec e$ je kvazinerozložitelný tehdy a jen tehdy, když ze vztahu $p \lesssim q \lesssim e$ plyne buď $q \sim p$ nebo $q \sim e$.*

Důkaz. 1. Nechť prvek $p \prec e$ má vlastnost uvedenou ve znění lemmatu; předpokládejme, že platí $p \sim ab$, kde $a \lesssim e$, $b \lesssim e$. Potom $ab \lesssim a$, $ab \lesssim b$ a odtud $p \lesssim a \lesssim e$, $p \lesssim b \lesssim e$. Nemůže platit současně $a \sim p$, $b \sim p$, neboť by z toho plynulo $p \sim e$, což je spor. Platí proto aspoň jeden ze vztahů $a \sim e$, $b \sim e$ a prvek p je tedy kvazinerozložitelný.

2. Nechť p je kvazinerozložitelný a předpokládejme, že platí $p \precsim q \precsim e$. Pak podle 2.10 existuje prvek $c \leqq e$ takový, že $p \sim qc$. Z definice 5 vyplývá, že buď $c \sim e$ a odtud $q \sim p$, nebo že platí $q \sim e$.

Lemma 2. *Nechť p je kvazinerozložitelný prvek a p^* význačný prvek jeho třídy, pak ze vztahu $p^* < q \leqq e$ plyne $q \sim e$.*

Důkaz. Platí $p \precsim q \precsim e$ a podle lemmatu 1 je buď $q \sim p$ nebo $q \sim e$. Ze vztahu $q \sim p$ by však plynulo $q \leqq p^*$, což je spor. Platí proto $q \sim e$, cbd.

Věta 3. *Je-li p kvazinerozložitelný prvek, pak příslušný p^* je prvoelement.*

Důkaz. Z předpokladů plyne, že $p^* < e$. Nechť $a \leqq e$, $b \leqq e$ a $ab \leqq p^*$, pak $p^* \leqq p^* \cup a \leqq e$. Jestliže $p^* = p^* \cup a$, plyne odtud $a \leqq p^*$, jestliže však $p^* < p^* \cup a \leqq e$, pak podle lemmatu 2 je $p^* \cup a \sim e$. Z toho $b = eb \sim (p^* \cup a)\, b = p^*b \cup ab$ a dále $p^*b \cup ab \leqq p^* \cup p^* = p^*$, tedy platí $p^*b \cup ab \precsim p^*$. Odtud plyne $b \precsim p^*$ a $b \leqq p^*$. Podle definice 6 je tedy p^* prvoelement.

Lemma 3. *Nechť p je kvazinerozložitelný prvek; pak ze vztahů $a \precsim e$, $b \precsim e$, $ab \precsim p$ plyne buď $a \precsim p$ nebo $b \precsim p$.*

Důkaz. Nechť prvky a, b, p vyhovují hořejším relacím, pak platí $a \leqq e$, $b \leqq e$, $ab \leqq p^*$ a jelikož p^* je podle věty 3 prvoelement, máme buď $a \leqq p^*$, nebo $b \leqq p^*$; odtud plyne, že buď $a \precsim p$ nebo $b \precsim p$ cbd.

Věta 4. *Jsou-li p_1, p_2 kvazinerozložitelné prvky, pak platí $p_1p_2 \sim p_2p_1$.*

Důkaz. Položme $q = p_1 \cap p_2$; podle 1.2 platí $p_1p_2 \leqq q \leqq p_1$, $p_2p_1 \leqq q \leqq p_2$ a tedy

$$p_1p_2 \precsim q \precsim p_1\,, \quad p_2p_1 \precsim q \precsim p_2\,. \tag{3}$$

Vynásobíme-li první resp. druhý ze vztahů (3) zleva prvkem p_1^{-1} resp. p_2^{-1}, dostáváme po úpravě

$$p_2 \precsim p_1^{-1}q \precsim e\,, \quad p_1 \precsim p_2^{-1}q \precsim e\,. \tag{4}$$

Podle lemmatu 1 mohou nastat tyto možnosti:

A) Platí aspoň jeden ze vztahů $p_1^{-1}q \sim e$ nebo $p_2^{-1}q \sim e$, potom buď $p_1 \sim q$ nebo $p_2 \sim q$ a užitím vhodného ze vztahů (3) dostáváme buď $p_1 \precsim p_2$ nebo $p_2 \precsim p_1$. Z lemmatu 1 plyne v obou případech $p_2 \sim p_1$ a dokazované tvrzení je okamžitým důsledkem 2.7.

B) Platí $p_1^{-1}q \sim p_2$, $p_2^{-1}q \sim p_1$, pak vynásobením těchto vztahů zleva prvky p_1, p_2 dostáváme $q \sim p_1p_2 \sim p_2p_1$. Tím je důkaz proveden.

Předpokládejme dále v tomto odstavci a v odst. 4, že l-pologrupa $\mathbf{L}$ splňuje *podmínku* (III).

3.2. *Každý rostoucí řetězec tvaru*

$$a_1 \prec a_2 \prec a_3 \prec \ldots \precsim e \tag{5}$$

je konečný.

Důkaz. Podle 2.3 platí pro příslušné význačné prvky $a_1^* < a_2^* < a_3^* < \ldots \leqq e$, tento řetězec obsahuje podle podmínky (III) jen konečný počet prvků a tedy i řetězec (5) je konečný.

3.3. *Každý klesající řetězec tvaru*

$$a_1 \succ a_2 \succ a_3 \succ \ldots \geqq a \tag{6}$$

je konečný.

Důkaz. Platí $a_1^{-1} \prec a_2^{-1} \prec a_3^{-1} \prec \ldots \leqq a^{-1}$ a odtud podle 2.5 a věty 1 $a_1^{-1}a \prec \prec a_2^{-1}a \prec a_3^{-1}a \prec \ldots \leqq e$. Tento řetězec je podle 3.2 konečný a tedy i řetězec (6) je konečný, cbd.

O konečném řetězci $a_1 \prec a_2 \prec \ldots \prec a_n$ řekneme, že je *prostý*, jestliže pro $i = 1, 2, \ldots, n - 1$ ze vztahu $a_i \leqq b \leqq a_{i+1}$ plyne $b \sim a_i$ nebo $b \sim a_{i+1}$. Říkáme také, že prvky a_1, a_n jsou *spojeny prostým řetězcem.*

Lemma 4. *Je-li $a \prec b \leqq e$, pak lze prvky a, b spojit prostým řetězcem.*

Důkaz. *Intervalem* $[a, b]$ budeme rozumět množinu všech prvků $x \in \mathbf{L}$, pro které platí $a \leqq x \leqq b$. Interval $[c, d]$ nazveme *vlastní částí* intervalu $[a, b]$, jestliže $a \leqq c$, $d \leqq b$ a neplatí současně $a \sim c$, $d \sim b$. Interval $[a, b]$ nazveme *nekonečným*, jestliže prvky a, b nelze spojit prostým řetězcem. Je zřejmé, že v každém nekonečném intervalu $[a, b]$ je obsažen jako vlastní část nekonečný interval $[c, d]$.

Nechť $a \prec b \leqq e$ a předpokládejme, že interval $[a, b]$ je nekonečný. Pak lze sestrojit nekonečnou posloupnost nekonečných intervalů

$$[a, b] \supset [a_1, b_1] \supset [a_2, b_2] \supset \ldots, \tag{7}$$

z nichž každý je vlastní částí předchozího intervalu.

Platí

$$a \leqq a_1 \leqq a_2 \leqq a_3 \leqq \ldots \leqq b \leqq e\,; \quad b \geqq b_1 \geqq b_2 \geqq b_3 \geqq \ldots \geqq a\,.$$

Je zřejmé, že buď se dá z prvního řetězce vybrat nekonečný řetězec tvaru (5), nebo se dá z druhého řetězce vybrat nekonečný řetězec tvaru (6) a to je podle 3.2 a 3.3 spor s podmínkou (III). Interval $[a, b]$ tedy nemůže být nekonečný a prvky a, b lze proto spojit prostým řetězcem.

Lemma 5. *Ke každému prvku $a \prec e$ existují kvazinerozložitelné prvky p_1, $p_2, \ldots, p_k$ takové, že platí $a \sim p_1 p_2 \ldots p_k$.*

Důkaz. Spojme prvky a, e prostým řetězcem:

$$a = a_1 \prec a_2 \prec \ldots \prec a_k \prec a_{k+1} = e\,.$$

Užitím lemmatu 1 se snadno ukáže, že prvky $a_1 a_2^{-1}, a_2 a_3^{-1}, \ldots, a_{k-1} a_k^{-1}, a_k$ jsou vesměs kvazinerozložitelné; jejich součin je zřejmě kvazirovný k $a_1 = a$.

Věta 5. *Každý prvek $a \prec e$ je kvazirovný konečnému součinu $p_1 p_2 \ldots p_k$ kvazinerozložitelných prvků, které jsou až na pořadí a kvazirovnost určeny jednoznačně.*

Důkaz. Možnost takového vyjádření plyne z lemmatu 5. Nechť jsou dány dva různé rozklady $a \sim p_1 p_2 \ldots p_k$, $a \sim p'_1 p'_2 \ldots p'_r$ prvku a v součin kvazinerozložitelných prvků. Pak platí $p'_1 p'_2 \ldots p'_r \leqq p_1$ a podle lemmatu 3 platí aspoň pro jeden prvek p'_i vztah $p'_i \lesssim p_1$. Vzhledem k větě 4 můžeme předpokládat takové označení prvků p'_j, že platí $p'_1 \lesssim p_1$. Potom zřejmě $p'_1 \sim p_1$ a $p_1^{-1}a \sim p_2 \ldots p_k \sim p'_2 \ldots p'_r$. Po konečném počtu kroků dojdeme k závěru, že $r = k$ a že při vhodném označení platí $p'_i \sim p_i$ pro $i = 1, 2, \ldots, k$. Oba rozklady se tedy mohou lišit nanejvýš pořadím činitelů. Tím je věta dokázána.

Věta 6. 1. *Grupa $\mathfrak{G}$ tříd kvazirovných prvků je komutativní.* 2. *Každý prvek $a \in \mathbf{L}$ nepatřící do jednotkové třídy je kvazirovný některému symbolickému součinu $p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, kde $e_i \neq 0$ $(i = 1, 2, \ldots, k)$ jsou celá čísla a $p_1, p_2, \ldots, p_k$ jsou kvazinerozložitelné elementy patřící k různým třídám; toto vyjádření je až na pořadí činitelů a volbu representantů p_i z příslušných tříd určeno jednoznačně.*

Důkaz. Ad 1: Nechť $a \in \mathbf{L}$ je libovolný prvek; označme $b = a^{-1} \cap e$. Potom platí $b \leqq e$, $c = ab \leqq e$ a přitom $a \sim cb^{-1}$. Tedy každý prvek $a \in \mathbf{L}$ se dá vyjádřit ve tvaru $a \sim bc^{-1}$, kde b, c jsou celé prvky. Z věty 4 a z věty 5 plyne, že pro libovolné celé prvky b, c platí $bc \sim cb$, $b^{-1}c \sim cb^{-1}$, $b^{-1}c^{-1} \sim c^{-1}b^{-1}$ a grupa $\mathfrak{G}$ je tedy komutativní.

Ad 2: Při důkazu se využije právě dokázaného tvrzení 1), jinak se postup neliší od postupu užitého v důkazu věty 5.

4. PRVOELEMENTY A JEDNOZNAČNÁ FAKTORISACE

Níže jsou charakterisovány všechny prvoelementy l-pologrupy $\mathbf{L}$:

Věta 7. *Každý prvoelement $p \in \mathbf{L}$ je buď kvazirovný k e nebo je kvazinerozložitelný a roven příslušnému význačnému prvku p^*.*

Důkaz. Buď $a \prec e$ prvoelement. Potom existuje kvazinerozložitelný prvek p takový, že $a \leqq p^*$. Podle 2.10 existuje prvek $c \leqq e$ takový, že $a \sim p^*c$ a $p^*c \leqq a$. Podle definice prvoelementu platí buď $c \leqq a$ nebo $p^* \leqq a$. Z nerovnosti $c \leqq a$ by však plynulo $p^*c \lesssim p^*a$, tedy $a \lesssim p^*a$ a $p^* \gtrsim e$, což je spor. Platí proto $p^* \leqq a$ a odtud $a = p^*$. Z vět 3, 5, 6, 7 nyní plyne

Věta 8. 1. *Každý prvek $a \prec e$ je kvazirovný konečnému součinu $p_1^* p_2^* \ldots p_k^*$ kvazinerozložitelných prvoelementů, určenému až na pořadí činitelů jednoznačně.* 2. *Každý prvek $a \in \mathbf{L}$ nepatřící do jednotkové třídy je kvazirovný některému symbolickému součinu $p_1^{*e_1} p_2^{*e_2} \ldots p_m^{*e_m}$, kde $e_i \gtrless 0$ jsou celá čísla a $p_1^*, p_2^*, \ldots, p_m^*$ navzájem různé kvazinerozložitelné prvoelementy; toto vyjádření je až na pořadí činitelů jednoznačné.*

Uvažujme ještě dvě další doplňující podmínky pro l-pologrupu $\mathbf{L}$:

(IV) *Ke každému prvku $a \in \mathbf{L}$ existuje význačný prvek b^* takový, že $b^* \leqq a$.*

(V) *Každý prvoelement v $\mathbf{L}$ je maximální.*

Lemma 6. *Platí-li v* $\mathbf{L}$ *podmínka* (IV), *pak ke každému prvoelementu* $q \sim e$ *existuje kvazinerozložitelný prvoelement* p^* *takový, že* $p^* < q$.

Důkaz. Nechť $q \sim e$ je prvoelement, podle podmínky IV existuje význačný prvek a^* takový, že $a^* \leqq q$. Protože $a^* \prec e$, platí podle věty 8 $a^* \sim p_1^* p_2^* \dots p_k^*$, kde $p_1^*, p_2^*, \dots, p_k^*$ jsou kvazinerozložitelné prvoelementy. Podle 2.3 platí $p_1^* p_2^* \dots p_k^* \leqq$ $\leqq a^* \leqq q$ a protože q je prvoelement, platí podle definice 6 aspoň pro jeden p_i^* relace $p_i^* \leqq q$. Je zřejmé, že platí přesněji $p_i^* < q$ cbd.

Věta 9. *Nechť l-pologrupa* $\mathbf{L}$ *splňuje podmínky* (I–V). *Pak platí:*

1. *l-pologrupa* $\mathbf{L}$ *je komutativní grupa a platí* $\mathbf{L} \equiv \mathfrak{G}$.

2. *Každý prvek* $a < e$ *lze vyjádřit jako součin konečného počtu prvoelementů a to až na pořadí činitelů jednoznačně. Každý prvek* $a \neq e$ *lze vyjádřit jako symbolický součin* $a = p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}$, *kde* $e_i \gtrless 0$ *jsou celá čísla a* $p_1, p_2, \dots, p_m$ *navzájem různé prvoelementy; toto vyjádření je až na pořadí činitelů jednoznačné.*

Důkaz. Z lemmatu 6 a podmínky (V) plyne, že v $\mathbf{L}$ neexistují prvoelementy kvazirovné k e, tedy podle 3.1 je každý maximální prvek v $\mathbf{L}$ vlastním kvazinásobkem e. Je-li $a < e$ libovolný celý prvek, pak k němu existuje maximální prvek $q \geqq a$, odtud je zřejmé, že ze vztahu $a < e$ plyne vždy $a \prec e$. Jediným prvkem kvazirovným k e je tedy e. Podle 2.12 ze vztahu $a \preceq b$ plyne $a \leqq b$ a ze vztahu $a \sim b$ plyne $a = b$. Věta 9 je tedy důsledkem věty 8 a první části věty 6.

5. IDEÁLY V NEKOMUTATIVNÍCH OKRUZÍCH

Je-li $\mathfrak{A}$ okruh, pak jeho prvek a se nazývá *regulární*, není-li pravým ani levým dělitelem nuly. Součin dvou regulárních prvků je zřejmě zase regulární prvek. Má-li okruh $\mathfrak{A}$ jednotkový prvek, a jestliže pro některé dva prvky $a, b \in \mathfrak{A}$ platí $ab = ba =$ $= 1$, nazýváme a *inversním prvkem* k b (b *inversním prvkem* k a) a označujeme $b =$ $= a^{-1}$, $a = b^{-1}$. Poněvadž v celém tomto odstavci budeme pojednávat pouze o prvcích okruhů, nemůže toto označování vést k nedorozumění.

V celém odstavci budeme předpokládat, že je dán okruh $\mathfrak{A}$ *s jednotkovým prvkem* 1, *ve kterém ke každému regulárnímu prvku existuje inversní prvek.*

Definice 8. *Podokruh* $\mathfrak{o}$ *okruhu* $\mathfrak{A}$ *se nazývá pořadatel tohoto okruhu, splňuje-li podmínky:*

*O*1) $1 \in \mathfrak{o}$.

*O*2) *Pro každé* $c \in \mathfrak{A}$ *existují prvky* $a, b \in \mathfrak{o}$ *takové, že* $c = ab^{-1}$.

Poznámka. Je-li okruh $\mathfrak{o}$ pořadatelem okruhu $\mathfrak{A}$, pak je $\mathfrak{A}$ tzv. *pravý podílový okruh* okruhu $\mathfrak{o}$.

Definice 9. *Buď* $\mathfrak{o}$ *pořadatel okruhu* $\mathfrak{A}$. *Podgrupa* $\mathfrak{a}$ *aditivní grupy okruhu* $\mathfrak{A}$ *se nazývá pravý* (*zlomkový*) $\mathfrak{o}$*-ideál, když platí:*

$R1)$ $\mathfrak{a}\mathfrak{o} \subset \mathfrak{a}$.

$R2)$ *$\mathfrak{a}$ obsahuje regulární prvek.*

$R3)$ *Existuje regulární prvek $a \in \mathfrak{A}$ takový, že $a\mathfrak{a} \subset \mathfrak{o}$.*

Obdobně definujeme levý $\mathfrak{o}$-ideál symetrickými podmínkami $L1, L2, L3$. Je-li podgrupa $\mathfrak{a}$ současně levým i pravým $\mathfrak{o}$-ideálem, budeme ji nazývat oboustranným $\mathfrak{o}$-ideálem, nebo krátce $\mathfrak{o}$-ideálem. Je zřejmé, že *každý pořadatel $\mathfrak{o}$ okruhu $\mathfrak{A}$ je $\mathfrak{o}$-ideál.*

Poznámka. Pro zkrácení zápisu budeme pravé $\mathfrak{o}$-ideály, levé $\mathfrak{o}$-ideály a $\mathfrak{o}$-ideály v souhrnu nazývat $\vec{\mathfrak{o}}$*-ideály.*

Definice 10. *Dva pořadatele $\mathfrak{o}_1$, $\mathfrak{o}_2$ okruhu $\mathfrak{A}$ se nazývají ekvivalentní, když existují regulární prvky a_1, b_1, a_2, b_2 takové, že $a_1\mathfrak{o}_1b_1 \subset \mathfrak{o}_2$, $a_2\mathfrak{o}_2b_2 \subset \mathfrak{o}_1$.* Takto definovaná ekvivalence je zřejmě logickou ekvivalencí.

V dalším budeme potřebovat toto kritérium:

Lemma 7. *Nechť $\mathfrak{o}'$ je podokruh okruhu $\mathfrak{A}$ obsahující 1 a nechť existuje pořadatel $\mathfrak{o}$ a regulární prvky a, b, a', b' takové, že $a\mathfrak{o}b \subset \mathfrak{o}'$, $a'\mathfrak{o}'b' \subset \mathfrak{o}$. Potom podokruh $\mathfrak{o}'$ je pořadatel ekvivalentní s pořadatelem $\mathfrak{o}$.*

Důkaz. Nechť $u \in \mathfrak{A}$, pak existují prvky $p, q \in \mathfrak{o}$ takové, že $a^{-1}ua = pq^{-1}$, neboť $\mathfrak{o}$ je pořadatel. Podle předpokladu platí $apb \in \mathfrak{o}'$, $aqb \in \mathfrak{o}'$ a $u = apq^{-1}a^{-1} = (apb) \,. \, (b^{-1}q^{-1}a^{-1}) = (apb)(aqb)^{-1}$; odtud je $\mathfrak{o}'$ pořadatel ekvivalentní s $\mathfrak{o}$.

Věta 10. *Buď $\mathfrak{a}$ $\vec{\mathfrak{o}}$-ideál; označme $\mathfrak{o}_l$ množinu prvků $x \in \mathfrak{A}$ takových, že $x\mathfrak{a} \subset \mathfrak{a}$ a $\mathfrak{o}_r$ množinu prvků $y \in \mathfrak{A}$ takových, že $\mathfrak{a}y \subset \mathfrak{a}$. Potom platí:*

1) *Množiny $\mathfrak{o}_l$, $\mathfrak{o}_r$ jsou pořadatele ekvivalentní k $\mathfrak{o}$,*

2) *ideál $\mathfrak{a}$ je levý $\mathfrak{o}_l$-ideál a pravý $\mathfrak{o}_r$-ideál.*

Důkaz. Buď předně $\mathfrak{a}$ pravý $\mathfrak{o}$-ideál. Množina $\mathfrak{o}_l$ je zřejmě podokruh obsahující 1. Podle podmínek $R1-R3$ existují regulární prvky a, b takové, že $b\mathfrak{o} \subset \mathfrak{a} \subset a\mathfrak{o}$, odtud $(b\mathfrak{o}a^{-1})\,\mathfrak{a} \subset (b\mathfrak{o}a^{-1})\,a\mathfrak{o} = b\mathfrak{o} \subset \mathfrak{a}$, tedy $b\mathfrak{o}a^{-1} \subset \mathfrak{o}_l$. Dále platí $\mathfrak{o}_l(b\mathfrak{o}) \subset \mathfrak{o}_l\mathfrak{a} \subset \subset \mathfrak{a} \subset a\mathfrak{o}$, tedy také $\mathfrak{o}_lb \subset a\mathfrak{o}$ a odtud $a^{-1}\mathfrak{o}_lb \subset \mathfrak{o}$. Podle lemmatu 7 je tedy $\mathfrak{o}_l$ pořadatel ekvivalentní s $\mathfrak{o}$.

Ukážeme, že $\mathfrak{a}$ je levý $\mathfrak{o}_l$-ideál. Vlastnosti $L1$, $L2$ vzhledem k pořadateli $\mathfrak{o}_l$ jsou zřejmě splněny. Dále protože $\mathfrak{a}$ je pravý $\mathfrak{o}$-ideál, existuje prvek c takový, že $c\mathfrak{a} \subset \mathfrak{o}$; odtud $\mathfrak{a}c\mathfrak{a} \subset \mathfrak{a}$ a tedy $\mathfrak{a}c \subset \mathfrak{o}_l$, což dává $L3$. Obdobně se ukáže, že je-li $\mathfrak{a}$ levý $\mathfrak{o}$-ideál, pak $\mathfrak{o}_r$ je pořadatel ekvivalentní k $\mathfrak{o}$ a $\mathfrak{a}$ je pravý $\mathfrak{o}_r$-ideál. Je-li $\mathfrak{a}$ pravý $\mathfrak{o}$-ideál, pak je $\mathfrak{a}$ také levý $\mathfrak{o}_l$-ideál, odtud je $\mathfrak{o}_r$ pořadatel ekvivalentní k $\mathfrak{o}_l$, tedy k $\mathfrak{o}$ a $\mathfrak{a}$ je pravý $\mathfrak{o}_r$-ideál. Tím je věta dokázána.

Definice 11. *Množiny $\mathfrak{o}_l$ a $\mathfrak{o}_r$ určené ve větě 10 se nazývají levý a pravý pořadatel $\vec{\mathfrak{o}}$-ideálu $\mathfrak{a}$.*

Definice 12. *Buď $\mathfrak{o}$ libovolný pořadatel. Potom se $\vec{\mathfrak{o}}$-ideál $\mathfrak{a}$ nazývá celý, platí-li $\mathfrak{a}\mathfrak{a} \subset \mathfrak{a}$.* Uvedeme několik pomocných tvrzení:

5.1. *Je-li* $\mathfrak{a}$ *pravý* (*levý*) $\mathfrak{o}$-*ideál, pak* $\mathfrak{o} \subset \mathfrak{o}_r$ $(\mathfrak{o} \subset \mathfrak{o}_l)$.

5.2. *Nechť* $\mathfrak{a}$ *je* $\vec{\mathfrak{o}}$-*ideál. Platí-li jeden ze vztahů* $\mathfrak{a} \subset \mathfrak{o}_r$, $\mathfrak{a} \subset \mathfrak{o}_l$, *platí i druhý a* $\mathfrak{a}$ *je celý* $\vec{\mathfrak{o}}$-*ideál. Je-li naopak* $\mathfrak{a}$ *celý* $\vec{\mathfrak{o}}$-*ideál, pak platí* $\mathfrak{a} \subset \mathfrak{o}_r$, $\mathfrak{a} \subset \mathfrak{o}_l$.

Důkaz plyne ihned z definice pořadatelů $\mathfrak{o}_l$ a $\mathfrak{o}_r$.

Buď $\mathfrak{a}$ $\vec{\mathfrak{o}}$-ideál, označme $\mathfrak{a}^{-1}$ množinu všech prvků $u \in \mathfrak{A}$ takových, že $\mathfrak{a}u\mathfrak{a} \subset \mathfrak{a}$.

Věta 11. *Nechť* $\mathfrak{a}$ *je* $\vec{\mathfrak{o}}$-*ideál s pravým pořadatelem* $\mathfrak{o}_r$ *a levým pořadatelem* $\mathfrak{o}_l$. *Potom množina* $\mathfrak{a}^{-1}$ *je levý* $\mathfrak{o}_r$-*ideál a pravý* $\mathfrak{o}_l$-*ideál.*

Důkaz. Především je zřejmé, že $\mathfrak{a}^{-1}$ je podgrupa aditivní grupy okruhu $\mathfrak{A}$. Ukážeme, že $\mathfrak{a}^{-1}$ splňuje vlastnosti $L1-3$ vzhledem k pořadateli $\mathfrak{o}_r$.

$L1$. Platí $\mathfrak{a}(\mathfrak{o}_r\mathfrak{a}^{-1})\,\mathfrak{a} = \mathfrak{a}\mathfrak{o}_r(\mathfrak{a}^{-1}\mathfrak{a}) \subset \mathfrak{a}\mathfrak{a}^{-1}\mathfrak{a} \subset \mathfrak{a} \Rightarrow \mathfrak{o}_r\mathfrak{a}^{-1} \subset \mathfrak{a}^{-1}$.

$L2$. Podle věty 10 a $R3$ existuje regulární prvek a takový, že $a\mathfrak{a} \subset \mathfrak{o}_r$; odtud $\mathfrak{a}a\mathfrak{a} \subset \mathfrak{a}\mathfrak{o}_r \subset \mathfrak{a}$ a tedy $a \in \mathfrak{a}^{-1}$.

$L3$. Podle $R2$ existuje regulární prvek b takový, že $b \in \mathfrak{a}$, odtud $\mathfrak{a}^{-1}b \subset \mathfrak{a}^{-1}\mathfrak{a} \subset \mathfrak{o}_r$, neboť $\mathfrak{a}\mathfrak{a}^{-1}\mathfrak{a} \subset \mathfrak{a}$.

Z dokázaného plyne, že $\mathfrak{a}^{-1}$ je levý $\mathfrak{o}_r$-ideál. Druhá část věty se dokáže obdobně.

Definice 13. *Ideál* $\mathfrak{a}^{-1}$ *se nazývá inversní k ideálu* $\mathfrak{a}$.

Definice 14. *Pořadatel* $\mathfrak{o}$ *se nazývá maximální, jestliže ze vztahu* $\mathfrak{o} \subset \mathfrak{o}'$, *kde* $\mathfrak{o}'$ *je pořadatel ekvivalentní k* $\mathfrak{o}$ *plyne* $\mathfrak{o} = \mathfrak{o}'$.

Následující tvrzení 5.3–5.9 platí za předpokladu, že $\mathfrak{o}$ *je maximální pořadatel okruhu* $\mathfrak{A}$.

5.3. *Je-li* $\mathfrak{a}$ *pravý* (*levý*) $\mathfrak{o}$-*ideál, pak* $\mathfrak{o} = \mathfrak{o}_r$ $(\mathfrak{o} = \mathfrak{o}_l)$.

Důkaz tvrzení plyne z 5.1, definice 14 a věty 10.

5.4. *Je-li* $\mathfrak{a}$ $\mathfrak{o}$-*ideál, potom také* $\mathfrak{a}^{-1}$ *je* $\mathfrak{o}$-*ideál.*

Důkaz plyne z 5.3 a věty 11.

5.5. *Je-li* $\mathfrak{a}$ *pravý* (*levý*) $\mathfrak{o}$-*ideál, potom inversní ideál* $\mathfrak{a}^{-1}$ *je množina všech prvků* $x \in \mathfrak{A}$, *pro které platí* $x\mathfrak{a} \subset \mathfrak{o}$ $(\mathfrak{a}x \subset \mathfrak{o})$.

Důkaz. Je-li $\mathfrak{a}x\mathfrak{a} \subset \mathfrak{a}$, platí $x\mathfrak{a} \subset \mathfrak{o}_r$ a podle 5.3 $x\mathfrak{a} \subset \mathfrak{o}$. Obráceně ze vztahu $x\mathfrak{a} \subset \mathfrak{o}$ plyne $\mathfrak{a}x\mathfrak{a} \subset \mathfrak{a}\mathfrak{o} \subset \mathfrak{a}$. Podobně se dokáže tvrzení v závorce.

5.6. *Je-li* $a \in \mathfrak{A}$ *regulární prvek, pak množina* $a\mathfrak{o}$ *je pravý* $\mathfrak{o}$-*ideál a množina* $\mathfrak{o}a$ *je levý* $\mathfrak{o}$-*ideál* (tzv. *hlavní ideály*). *Dále platí* $(a\mathfrak{o})^{-1} = \mathfrak{o}a^{-1}$, $(\mathfrak{o}a)^{-1} = a^{-1}\mathfrak{o}$.

Důkaz. První část tvrzení je zřejmá. Dále platí $\mathfrak{o}a^{-1}(a\mathfrak{o}) \subset \mathfrak{o}$ a tedy podle 5.5 $\mathfrak{o}a^{-1} \subset (a\mathfrak{o})^{-1}$. Obráceně ze vztahu $x \in (a\mathfrak{o})^{-1}$ plyne podle 5.5 $xa\mathfrak{o} \subset \mathfrak{o}$, odtud máme $xa \in \mathfrak{o}$ a tedy $x \in \mathfrak{o}a^{-1}$. Platí proto $(a\mathfrak{o})^{-1} = \mathfrak{o}a^{-1}$. Obdobně probíhá důkaz pro ideál $\mathfrak{o}a$.

5.7. *Je-li* $\mathfrak{a}$ $\mathfrak{o}$-*ideál, pak platí*:

1. $\mathfrak{a}$ *obsahuje regulární prvek* $a \in \mathfrak{o}$.
2. *Existuje regulární prvek* $b \in \mathfrak{o}$ *takový, že* $\mathfrak{a}b \subset \mathfrak{o}$, $b\mathfrak{a} \subset \mathfrak{o}$.

Důkaz. 1. Protože $\mathfrak{a}$ je pravý $\mathfrak{o}$-ideál, existuje v $\mathfrak{a}$ regulární prvek $c \in \mathfrak{A}$. Podle $O2$ platí $c = ab^{-1}$, kde $a, b \in \mathfrak{o}$ jsou zřejmě regulární prvky. Odtud plyne $a \in \mathfrak{a}b \subset \subset \mathfrak{a}\mathfrak{o} \subset \mathfrak{a}$.

2. Podle 5.4 je $\mathfrak{a}^{-1}$ oboustranný $\mathfrak{o}$-ideál, který podle 5.7–1 obsahuje regulární prvek $b \in \mathfrak{o}$. Odtud plyne podle 5.5 $\mathfrak{a}b \subset \mathfrak{o}$, $b\mathfrak{a} \subset \mathfrak{o}$.

5.8. *Jsou-li* $\mathfrak{a}, \mathfrak{b}$ $\mathfrak{o}$-*ideály, pak je* $\mathfrak{a} + \mathfrak{b}$ $\mathfrak{o}$-*ideál.*

Důkaz. Nechť $\mathfrak{a}, \mathfrak{b}$ jsou $\mathfrak{o}$-ideály. Předně platí

$$(\mathfrak{a} + \mathfrak{b})\,\mathfrak{o} = \mathfrak{a}\mathfrak{o} + \mathfrak{b}\mathfrak{o} \subset \mathfrak{a} + \mathfrak{b}\,, \quad \mathfrak{o}(\mathfrak{a} + \mathfrak{b}) = \mathfrak{o}\mathfrak{a} + \mathfrak{o}\mathfrak{b} \subset \mathfrak{a} + \mathfrak{b}\,.$$

Dále platí $\mathfrak{a} \subset \mathfrak{a} + \mathfrak{b}$ a tedy $\mathfrak{a} + \mathfrak{b}$ obsahuje regulární prvek. Podle 5.7–2 existují regulární prvky $a, b \in \mathfrak{o}$ takové, že platí $a\mathfrak{a} \subset \mathfrak{o}$, $b\mathfrak{b} \subset \mathfrak{o}$, odtud plyne $ab(\mathfrak{a} + \mathfrak{b}) = = ab\mathfrak{a} + ab\mathfrak{b} \subset a\mathfrak{a} + a\mathfrak{o} \subset \mathfrak{o}$, přitom ab je zřejmě regulární prvek. Podobně se ukáže, že $(\mathfrak{a} + \mathfrak{b})\,ab \subset \mathfrak{o}$.

5.9. *Jsou-li* $\mathfrak{a}, \mathfrak{b}$ $\mathfrak{o}$-*ideály, pak platí, že také* $\mathfrak{a}\mathfrak{b}$, $\mathfrak{a} \cap \mathfrak{b}$ *jsou* $\mathfrak{o}$-*ideály.*

Důkaz. Pro ideál $\mathfrak{a}\mathfrak{b}$ jsou vlastnosti $R1-3$, $L1-3$ zřejmé. Například $R3$ plyne takto: Existují prvky $a, b \in \mathfrak{A}$ takové, že $a\mathfrak{a} \subset \mathfrak{o}$, $b\mathfrak{b} \subset \mathfrak{o}$, odtud $ba\mathfrak{a}\mathfrak{b} \subset b\mathfrak{o}\mathfrak{b} \subset \subset b\mathfrak{b} \subset \mathfrak{o}$. Pro ideál $\mathfrak{a} \cap \mathfrak{b}$ jsou zřejmé vlastnosti 1, 3. Vlastnost 2: Podle 5.7–1 existují regulární prvky $a, b \in \mathfrak{o}$ takové, že $a \in \mathfrak{a}$, $b \in \mathfrak{b}$. Odtud plyne $ab \in a\mathfrak{o} \subset \mathfrak{a}$, $ab \in \in \mathfrak{o}b \subset \mathfrak{b}$, tedy $ab \in \mathfrak{a} \cap \mathfrak{b}$.

Nyní jsme schopni dokázat základní větu, která dává interpretaci úvah předchozích odstavců v teorii $\mathfrak{o}$-ideálů.

Věta 12. *Nechť* $\mathfrak{o}$ *je maximální pořadatel okruhu* $\mathfrak{A}$. *Pak množina* **L** *všech* $\mathfrak{o}$-*ideálů okruhu* $\mathfrak{A}$ *je l-pologrupa splňující podmínky* (I), (II) z § 1.

Důkaz. Především podle 5.9 je množina **L** všech $\mathfrak{o}$-ideálů pologrupa s jednotkovým prvkem $\mathfrak{o}$. V částečném uspořádání této množiny podle inkluse existuje ke každým dvěma $\mathfrak{o}$-ideálům $\mathfrak{a}, \mathfrak{b}$ nejmenší horní závora $\mathfrak{a} + \mathfrak{b}$ a největší dolní závora $\mathfrak{a} \cap \mathfrak{b}$ (viz 5.8 a 5.9). Množina **L** je tedy svaz. V **L** zřejmě platí oba distributivní zákony pro násobení vzhledem ke svazové disjunkci. Podle 5.4 a z významu ideálu $\mathfrak{a}^{-1}$ vidíme, že je v **L** splněna podmínka (I). Konečně ze vztahu $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a}$ resp. $\mathfrak{b}\mathfrak{a} \subset \mathfrak{a}$ plyne $\mathfrak{b} \subset \mathfrak{o}_r$ resp. $\mathfrak{b} \subset \mathfrak{o}_l$ a podle 5.3 platí v obou případech $\mathfrak{b} \subset \mathfrak{o}$. V **L** je tedy splněna také podmínka (II).

V množině **L** lze nyní obvyklým způsobem zavést definici *prvoideálu* a *maximálního* $\mathfrak{o}$-*ideálu*; tyto ideály mají význam prvoelementu a maximálního elementu l-pologrupy **L**. Analogicky jako v definicích 4, 5 se zavádí pojem *kvazidělitelnosti* a *kvazirovnosti pro* $\mathfrak{o}$-*ideály* a pojem *kvazinerozložitelného* $\mathfrak{o}$-*ideálu*. Potom platí:

Věta 13. *Nechť* $\mathfrak{o}$ *je maximální pořadatel okruhu* $\mathfrak{A}$, *v němž je splněna maximální podmínka pro řetězce celých* $\mathfrak{o}$-*ideálů. Potom je každý* $\mathfrak{o}$-*ideál* $\mathfrak{a}$, *pro nějž* $\mathfrak{a}^{-1} \neq \mathfrak{o}$, *kvazirovný některému symbolickému součinu* $\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \dots \mathfrak{p}_m^{e_m}$, *kde* $e_i \gtrless 0$ $(i = 1, 2, \dots, m)$ *jsou celá čísla a* $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m$ *navzájem různé kvazinerozložitelné prvoideály; toto vyjádření je až na pořadí činitelů jednoznačné.*

Důkaz viz větu 8.

Definice 15. *Pořadatel $\mathfrak{o}$ okruhu $\mathfrak{A}$ se nazývá omezený, jestliže každý pravý resp. levý $\mathfrak{o}$-ideál obsahuje oboustranný $\mathfrak{o}$-ideál.*

Následující tvrzení platí za předpokladu, že $\mathfrak{o}$ *je maximální omezený pořadatel okruhu* $\mathfrak{A}$.

5.10. *Je-li a regulární prvek, potom množina $\mathfrak{o}a\mathfrak{o}$ je $\mathfrak{o}$-ideál.*

Důkaz. Vlastnosti $L1,2$ a $R1,2$ jsou zde zřejmě splněny. Dokážeme vlastnost $L3$. Nechť a je regulární prvek; pak podle 5.6 je $a^{-1}\mathfrak{o}$ pravý $\mathfrak{o}$-ideál, existuje tedy $\mathfrak{o}$-ideál $\mathfrak{a} \subset a^{-1}\mathfrak{o}$ a regulární prvek $b \in \mathfrak{a}$; platí tedy $\mathfrak{o}b \subset \mathfrak{a} \subset a^{-1}\mathfrak{o}$ a odtud plyne $(\mathfrak{o}a\mathfrak{o})\, b \subset$ $\subset \mathfrak{o}$. Podobně se ukáže, že existuje prvek b' takový, že $b'(\mathfrak{o}a\mathfrak{o}) \subset \mathfrak{o}$, tedy že platí $R3$. Tím je důkaz proveden.

Ve větě 2 § 2 jsme ukázali, že je-li $\mathbf{L}$ necelá l-pologrupa, potom kvazidělitelnost elementů definovaná na $\mathbf{L}$ je (ve zřejmém smyslu) netriviální relace. Následující věta zcela přirozeně navazuje na větu 2.

Věta 14. *Buď $\mathfrak{o}$ maximální pořadatel okruhu $\mathfrak{A}$. Postačující podmínkou pro to, aby l-pologrupa $\mathbf{L}$ oboustranných $\mathfrak{o}$-ideálů byla necelá je, aby pořadatel $\mathfrak{o}$ byl omezený a aby platilo $\mathfrak{o} \neq \mathfrak{A}$.*

Důkaz. Je-li splněna podmínka věty, pak existuje prvek $c \in \mathfrak{A}$ takový, že $c \notin \mathfrak{o}$. Podle $O2$ existují prvky $a, b \in \mathfrak{o}$ takové, že $c = ab^{-1}$. Kdyby platilo $b^{-1} \in \mathfrak{o}$, měli bychom $c \in \mathfrak{o}$, což je spor. Platí proto $b^{-1} \notin \mathfrak{o}$ a podle 5.10 je množina $\mathfrak{o}b^{-1}\mathfrak{o}$ necelý $\mathfrak{o}$-ideál.

Věta 15. *Je-li $\mathfrak{o}$ omezený maximální pořadatel, pak příslušná l-pologrupa $\mathbf{L}$ všech $\mathfrak{o}$-ideálů splňuje podmínku* (IV).

Důkaz. Buď $\mathfrak{a}$ libovolný $\mathfrak{o}$-ideál. Nechť $a \in \mathfrak{a}$ je regulární prvek; pak $a\mathfrak{o} \subset \mathfrak{a}$ a podle 5.6 je $a\mathfrak{o}$ pravý $\mathfrak{o}$-ideál. Poněvadž $\mathfrak{o}$ je omezený, existuje $\mathfrak{o}$-ideál $\mathfrak{b} \subset a\mathfrak{o}$. Snadno se vidí, že $(a\mathfrak{o})^{-1} \subset \mathfrak{b}^{-1}$ a $\mathfrak{b}^* \subset ((a\mathfrak{o})^{-1})^{-1}$. Podle 5.6 je ovšem $((a\mathfrak{o})^{-1})^{-1} =$ $= a\mathfrak{o}$. Platí tedy $\mathfrak{b}^* \subset a\mathfrak{o}$ a odtud $\mathfrak{b}^* \subset \mathfrak{a}$.

Z věty 9 pak ihned plyne základní věta o jednoznačné faktorisaci.:

Věta 16. *Nechť $\mathfrak{o}$ je pořadatel okruhu $\mathfrak{A}$, který splňuje následující podmínky:*

1) *$\mathfrak{o}$ je maximální.*
2) *$\mathfrak{o}$ je omezený.*
3) *Platí maximální podmínka pro řetězce celých $\mathfrak{o}$-ideálů.*
4) *Každý prvoideál okruhu $\mathfrak{o}$ je maximální.*

Potom platí:

1. *Množina $\mathbf{L}$ všech $\mathfrak{o}$-ideálů je komutativní grupa.*
2. *Každý celý $\mathfrak{o}$-ideál lze vyjádřit jako součin konečného počtu prvoideálů a to až na pořadí činitelů jednoznačně.*

Každý $\mathfrak{o}$-ideál $\mathfrak{a} \neq \mathfrak{o}$ je roven jistému symbolickému součinu $\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_m^{e_m}$, kde $e_i \gtrless 0$ $(i = 1, 2, \ldots, m)$ jsou celá čísla a $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_m$ jsou navzájem různé prvoideály; toto vyjádření je až na pořadí činitelů jednoznačné.

Literatura

[1] *Г. Биркгоф*: Теория структур. ИЛ, Москва 1952.
[2] *В. Ходж* и *Д. Пидо*: Методы алгебраической геометрии, том 3., ИЛ, Москва 1955.
[3] *N. Jacobson*: The theory of rings. Amer. math. soc. 1943.
[4] *Е. Г. Шулгейфер*: Разложение на простые множители в структурах с умножением. Украинский математический журнал, том II, Киев (1950), стр. 100—114.
[5] *B. L. van der Waerden*: Moderne Algebra, II. Teil, Berlin 1931.

Резюме

К ТЕОРИИ $\mathfrak{o}$-ИДЕАЛОВ В НЕКОММУТАТИВНЫХ КОЛЬЦАХ

ОЛДРЖИХ КОВАЛЬСКИ (Oldřich Kowalski), Брно

Е. Нетер установила необходимые и достаточные условия для того, чтобы все дробные идеалы, соответствующие данной коммутативной области целостности, можно было точно одним способом разложить в произведение степеней простых идеалов.

Ван дер Варден показал, что при более слабых предположениях, чем условия Нетер, можно установить между этими дробными идеалами отношение квазиравенства так, чтобы всякий идеал однозначно представлялся как произведение степеней простых идеалов с точностью до квазиравенства.

Результаты Нетер были обобщенны с другой точки зрения в теории $\mathfrak{o}$-идеалов, основы которой положил К. Асано:

Пусть $\mathfrak{o}$ — некоммутативное кольцо. Тогда всякий дробный $\mathfrak{o}$-идеал однозначно представляется в виде произведения степеней простых $\mathfrak{o}$-идеалов в том и только в том случае, когда $\mathfrak{o}$ подчиненно следующим условиям:

1. $\mathfrak{o}$ максимально в своем кольце частных. 2. $\mathfrak{o}$ ограничено. 3. Выполнено условие максимальности для цепей целых $\mathfrak{o}$-идеалов. 4. Все простые $\mathfrak{o}$-идеалы максимальны.

В настоящей статье применяются идеи Вардена к теории $\mathfrak{o}$-идеалов и таким образом дальше обобщаются классические результаты. В начале нашей работы введено понятие l-полугруппы (т. е. структурно упорядоченной полугруппы) и определены отношения квазиравенства и квазиделительности в нецелой l-полугруппе. Далее установлены достаточные условия, при которых имеет место однозначное представление элементов некоторой l-полугруппы в виде произведений степеней простых множителей — или буквально, или с точностью до квазиравенства.

В последнем параграфе применяются выведенные результаты к теории $\mathfrak{o}$-идеалов. Здесь доказывается:

а) *Если в кольце* $\mathfrak{o}$ *выполняется условие* 1, *то совокупность всех дробных* $\mathfrak{o}$*-идеалов образует l-полугруппу.*

б) *Если в кольце* $\mathfrak{o}$ *имеют место условия* 1 *и* 3, *на множестве всех дробных* $\mathfrak{o}$*-идеалов можно установить отношение квазиравенства так, чтобы всякий* $\mathfrak{o}$*-идеал однозначно представлялся как произведение степеней простых* $\mathfrak{o}$*-идеалов с точностью до квазиравенства.*

в) *Если в кольце* $\mathfrak{o}$, *сверх того, выполнено условие* 2, *и если оно не совпадает со своим кольцом частных, то надлежащее отношение квазиравенства заведомо нетривиально.*

г) *Если присоединим к условиям* $1-3$ *еще условие* 4, *то мы получим снова основное предложение теории* $\mathfrak{o}$*-идеалов.*

Zusammenfassung

BEITRAG ZUR THEORIE DER $\mathfrak{o}$-IDEALE DER NICHTKOMMUTATIVEN RINGE

OLDŘICH KOWALSKI, Brno

E. NOETHER hatte die notwendigen und hinreichenden Bedingungen dafür gegeben, daß sich alle einem gegebenen kommutativen Integritätsbereiche zuständigen gebrochenen Ideale eindeutig als Produkte von Primidealpotenzen darstellen lassen.

VAN DER WAERDEN hatte gezeigt, daß unter den schwächeren Voraussetzungen, als die von E. Noether sind, zwischen diesen Idealen eine ,,Quasigleichheitrelation" so definiert werden kann, daß sich jedes gebrochene Ideal eindeutig bis auf die Quasigleichheit als Produkt von Primidealpotenzen darstellen läßt.

Die Ergebnisse von E. Noether wurden anderseits in der von K. ASANO begründeten Theorie der $\mathfrak{o}$-Ideale verallgemeinert:

Ist $\mathfrak{o}$ ein nichtkommutativer Ring, so ist jedes gebrochene $\mathfrak{o}$-Ideal genau dann eindeutig als Produkt von $\mathfrak{o}$-Primidealpotenzen darstellbar, wenn der Ring $\mathfrak{o}$ folgende Bedingungen erfüllt:

1. $\mathfrak{o}$ ist maximal in seinem Quotientenring $\mathfrak{A}$.
2. $\mathfrak{o}$ ist beschränkt.
3. Es gilt der Teilerkettensatz für ganze $\mathfrak{o}$-Ideale.
4. Alle $\mathfrak{o}$-Primideale sind teilerlos.

In der vorliegenden Arbeit werden die Gedanken von Waerden auf die Theorie der $\mathfrak{o}$-Ideale angewendet, so dass die klassischen Ergebnisse noch weiter verallgemeinert werden. Am Anfang ist der Begriff einer l-Halbgruppe (d. h. einer Verbandshalbgruppe) eingeführt und dann werden die Quasigleichheit- und Quasiteilbarkeitrelationen auf einer nichtganzen l-Halbgruppe definiert. Weiter werden die Bedingungen festgelegt, unter welchen die eindeutige Primfaktorzerlegung der Elemente einer l-Halbgruppe pünktlich bzw. bis auf die Quasigleichheit möglich ist.

Im letzten Absatze interpretiert man schließlich diese Ergebnisse in der Theorie der $\mathfrak{o}$-Ideale.

Hier wird bewiesen, daß:

a) *Wenn der Ring $\mathfrak{o}$ die Bedingung* 1 *erfüllt, dann bildet die Gesamtheit aller gebrochenen $\mathfrak{o}$-Ideale eine l-Halbgruppe.*

b) *Wenn der Ring $\mathfrak{o}$ die beiden Bedingungen* 1 *und* 3 *erfüllt, dann ist es möglich auf der Menge aller $\mathfrak{o}$-Ideale die Quasigleichheitrelation derart definieren, daß jedes gebrochene $\mathfrak{o}$-Ideal eindeutig bis auf die Quasigleichheit als Produkt von $\mathfrak{o}$-Primidealpotenzen darstellbar ist.*

c) *Erfüllt der Ring überdies die Bedingung* 2 *und ist von seinem Quotientenring verschieden, dann ist die zuständige Quasigleichheitrelation sicherlich nicht-trivial.*

d) *Fügen wir zu den Bedingungen* 1—3 *noch die letzte* 4. *hinzu, bekommen wir wieder den Hauptsatz der Theorie der $\mathfrak{o}$-Ideale.*