VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNÍHO INŽENÝRSTVÍ
ÚSTAV MATEMATIKY

FACULTY OF MECHANICAL ENGINEERING
INSTITUTE OF MATHEMATICS

DROZDOVY OKRUHY

DROZD RINGS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — JAN NYTRA
AUTHOR

VEDOUCÍ PRÁCE — doc. RNDr. MIROSLAV KUREŠ, Ph.D.
SUPERVISOR

BRNO 2013

Vysoké učení technické v Brně, Fakulta strojního inženýrství

Ústav matematiky
Akademický rok: 2012/2013

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

student(ka): Jan Nytra

který/která studuje v **bakalářském studijním programu**

obor: **Matematické inženýrství (3901R021)**

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma bakalářské práce:

Drozdovy okruhy

v anglickém jazyce:

Drozd rings

Stručná charakteristika problematiky úkolu:

Studium Drozdových okruhů a Drozdových algeber v diskrétním i spojitém případě.

Cíle bakalářské práce:

1. Klasifikace diskrétních Drozdových okruhů nad vybranými konečnými poli
2. Popis Weilových algeber, které jsou Drozdovými okruhy s důrazem na grupu automorfismů

Seznam odborné literatury:

L. Klingler, L. S. Levy, Representation Type Of Commutative Noetherian Rings (introduction), Proc. of the Intern. Conf. on alg., mod. and rings, University of Lisbon, Lisbon, Portugal, 2003, World Scientific, 113-151 (2006)
L. Klingler, L. S. Levy, Representation Type Of Commutative Noetherian Rings I, Local wildness, Pac. J. Math. 200, No.2, 345-386 (2001)
G. Bini, F. Flamini, Finite Commutative Rings and Their Appplications, Springer 2002
Wasserman, Robert H., Tensors and manifolds. With applications to physics. 2nd ed., Oxford University Press, 2004

Vedoucí bakalářské práce: doc. RNDr. Miroslav Kureš, Ph.D.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2012/2013.

V Brně, dne 21.11.2012

L.S.

prof. RNDr. Josef Šlapal, CSc. Ředitel ústavu	prof. RNDr. Miroslav Doupovec, CSc., dr. h. c. Děkan fakulty

Abstrakt
Tato práce se zabývá problematikou Drozdových okruhů. V úvodu jsou připomenuty vybrané partie z teorie algebry, potřebné pro jejich zavedení. Následující kapitola je věnována příkladu Dozdova okruhu. Dále následuje část, ve které se zabýváme Weilovými algebrami - ukazuje se, že Drozdovy algebry nad polem reálných čísel jsou specifickým příkladem Weilových algeber. Také zde konstruujeme grupy algebrových automorfismů těchto algeber. V poslední části se věnujeme Lieovým grupám, protože grupy algebrových automorfismů Weilových algeber jsou příklady Lieových grup.

Summary
This thesis focuses on Drozd rings. In the beginning, we mention important parts of algebraic theory for the definition of these rings. In the next chapter we describe an example of Drozd ring. In the following, we concentrate on Weil algebras - it shows up, that Drozd algebras over field of real numbers are specific examples of Weil algebras. We also construct groups of algebra automorphisms for these algebras. In the last part of the thesis, we mention Lie groups, because groups of algebra automorphisms of Weil algebras are examples of Lie groups.

Klíčová slova
okruh, ideál, homomorfismus, algebra, Lieova grupa

Keywords
ring, ideal, homomorphism, algebra, Lie group

NYTRA, J. *Drozdovy okruhy*. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2013. 30 s. Vedoucí doc. RNDr. Miroslav Kureš, Ph.D.

Prohlašuji, že jsem bakalářskou práci „Drozdovy okruhy“ zpracoval samostatně pod vedením své vedoucího doc. RNDr. Miroslava Kureše, Ph.D. za využití zdrojů uvedených v seznamu použité literatury.

Jan Nytra

Chtěl bych poděkovat zejména svému vedoucímu práce za jeho odbornou pomoc a vedení celé práce. Dále bych chtěl poděkovat Mgr. Jaromíru Kubenovi za jeho rady a připomínky a v neposlední řadě všem, kteří mi pomohli tuto práci upravit po stránce jazykové a vzhledové.

Jan Nytra

Obsah

1 Úvod **3**

2 Základní pojmy **4**
2.1 Základní algebraické struktury 4
2.2 Uspořádané množiny 6
2.3 Ideály 7
2.4 Okruhové a algebrové homomorfismy 9

3 Drozdovy okruhy **11**

4 Grupy $\mathbb{R}$-algebrových automorfismů Drozdových $\mathbb{R}$-algeber **16**
4.1 Weilovy algebry 16
4.2 Drozdovy $\mathbb{R}$-algebry 18

5 Lieovy grupy **21**
5.1 Úvod do Lieových grup 21
5.2 Grupy $\mathbb{R}$-algebrových automorfismů Weilových algeber 22

6 Závěr **24**

7 Seznam použitých zkratek a symbolů **26**

8 Přílohy **27**
8.1 Zobecnění Weilových algeber 27
8.2 Grupy $\mathbb{R}$-algebrových automorfismů Weilových algeber 28

1. Úvod

Náplní této bakalářské práce jsou Drozdovy okruhy. Jedná se o okruhy, které splňují jisté podmínky pro své ideály, zejména pak pro svůj maximální ideál. Pro tyto okruhy se ukazuje, že mají tzv. divokou reprezentaci (jiné okruhy mají zase na druhou stranu tzv. krotkou reprezentaci, např. Kleinovy okruhy, viz [3]). Své označení získaly po ukrajinském matematikovi Juriji Drozdovi díky jeho přínosu k této problematice.

V první kapitole připomeneme důležité pojmy z algebry. Nejprve zavedeme základní algebraické struktury a související pojmy s důrazem na okruhy a pole. Dále se budeme věnovat ideálům a uvedeme jejich základní typy a operace, které pro ně lze zavést. V poslední části této kapitoly se zaměříme na okruhové homomorfismy, pomocí kterých potom zavedeme pojem R-algebry nad polem či okruhem R. Toto pro nás bude později stěžejní, jelikož se budeme zabývat Weilovými algebrami, což jsou příklady $\mathbb{R}$-algeber.

V druhé kapitole uvedeme definici Drozdova okruhu. Také se zde zaměříme na jeden ukázkový případ, který důkladně probereme. Dokážeme všechny potřebné vlastnosti, které musí okruh splňovat, aby byl Drozdovým okruhem. Dále se ukazuje, že tento okruh není algebrou nad žádným polem, ať charakteristiky kladné, nebo nulové, což také důkladně rozebereme.

V následující kapitole se zaměříme na Drozdovy algebry - Drozdovy okruhy, které jsou zároveň algebrami. Začneme však pojmem Weilova algebra a uvedeme její základní charakteristiky, kterými jsou řád a šířka. Dále se zaměříme na v jistém smyslu speciální Weilovy algebry, kdy budeme uvažovat faktorizaci speciálními ideály. Dále se budeme věnovat Drozdovým $\mathbb{R}$-algebrám, které jsou speciálními případy Weilových algeber. Uvedeme zde dvě Drozdovy $\mathbb{R}$-algebry a také spočítáme jejich grupy $\mathbb{R}$-algebrových automorfismů. Na závěr kapitoly uvedeme větu, která uvádí nutné podmínky pro Weilovu algebru, aby se mohlo jednat o Drozdovu $\mathbb{R}$-algebru. Příklady Weilových algeber, u kterých se ukázalo, že nejsou Drozdovými $\mathbb{R}$-algebrami, uvádíme v příloze včetně jejich grup $\mathbb{R}$-algebrových automorfismů.

V poslední kapitole provedeme úvod do teorie Lieových grup v návaznosti na předchozí kapitolu - ukazuje se, že grupy $\mathbb{R}$-algebrových automorfismů Weilových algeber jsou příklady Lieových grup. Uvedeme zde také klasické maticové Lieovy grupy, které blíže popíšeme.

2. Základní pojmy

V této kapitole si připomeneme vybrané partie algebry, které budeme dále potřebovat.

2.1. Základní algebraické struktury

Začneme zavedením základních algebraických struktur, které budeme v rámci textu používat a připomeneme terminologii pro speciální prvky těchto struktur. Speciálně se zaměříme na okruhy a pole a některé jejich vlastnosti, které pro ně definujeme.

Definice 2.1.1. Množinu G s (binární) operací $*$ splňující:

(G1) $(x * y) * z = x * (y * z) \quad \forall x, y, z \in G$,

(G2) $\exists e \in G$ tak, že $x * e = e * x = x \quad \forall x \in G$,

(G3) $\forall x \in G$ existuje $x^{-1} \in G$ tak, že $x * x^{-1} = x^{-1} * x = e$

nazveme *grupa* (anglicky *group*). Tedy grupová operace je asociativní, existuje neutrální prvek (dá se ukazát, že právě jeden, viz [7]) a ke každému prvku existuje prvek inverzní (opět platí, že právě jeden). Pokud navíc platí

(G4) $x * y = y * x \quad \forall x, y \in G$,

mluvíme o *komutativní (abelovské) grupě*.

Dále budeme uvažovat grupy aditivní (s operací $+$), kdy neutrální prvek nazýváme *nulový prvek* a prvek inverzní *prvek opačný*, a grupy multiplikativní (s operací $\cdot$), kdy neutrální prvek nazýváme *jednotkový prvek* a inverzní prvek *multiplikativní inverze*.

Definice 2.1.2. Množinu R se dvěmi operacemi $+$ a $\cdot$ splňující:

(R1) R je komutativní grupa vůči operaci $+$,

(R2) $(x \cdot y) \cdot z = x \cdot (y \cdot z) \quad \forall x, y, z \in R$,

(R3) $\exists 1_R \in R$ tak, že $1_R \cdot x = x \cdot 1_R = x \quad \forall x \in R$,

(R4) $(x + y) \cdot z = x \cdot z + y \cdot z, \quad z \cdot (x + y) = z \cdot x + z \cdot y \quad \forall x, y, z \in R$

nazveme *okruh* (anglicky *ring*). Opět se dá ukázat, že jednotkový prvek je právě jeden. Značíme jej 1_R (nulový prvek značíme analogicky 0_R). Vlastnost (R4) ukazuje, jak jsou operace svázány distributivními zákony. Pokud navíc platí

(R5) $x \cdot y = y \cdot x \quad \forall x, y \in R$,

hovoříme o *komutativním okruhu*.

Poznámka. Dále budeme uvažovat okruhy komutativní, pokud nebude uvedeno jinak.

Poznámka. Okruh R, který má jediný prvek $0_R = 1_R$, nazýváme *nulový* nebo také *triviální okruh*.

Definice 2.1.3. Okruh R, ve kterém má každý prvek (kromě 0_R) multiplikativní inverzi, se nazývá *pole* (anglicky *field*). Je-li operace $\cdot$ komutativní, máme *komutativní pole*. Jinými slovy, množinu K s dvěmi operacemi $+$ a $\cdot$ splňující:

(F1) K je komutativní grupa vůči operaci $+$,

(F2) $K - \{0_K\}$ je grupa vůči operaci $\cdot$,

(F3) $(x+y)\cdot z = x\cdot z + y\cdot z, \quad z\cdot(x+y) = z\cdot x + z\cdot y \quad \forall x,y,z \in K$

nazveme *pole*. Pokud navíc platí

(F4) $x\cdot y = y\cdot x \quad \forall x,y \in K$,

dostáváme *komutativní pole*.

Poznámka. Značení operace násobení budeme standartně vynechávat, pokud bude jasné, ve které struktuře operaci provádíme. Pokud tedy budeme uvažovat dva okruhy nebo dvě pole, budeme operaci násobení označovat $\cdot_X$, kde X bude určovat strukturu, ve které operaci provádíme.

Definice 2.1.4. Nechť K je pole. Množinu V s operací $+$, přičemž $(V,+)$ tvoří grupu, a vnější operací $\cdot_s$ ($\cdot_s : K \times V \to V$) splňující:

(V1) $\mathbf{u} \in V, x \in K \Rightarrow x \cdot_s \mathbf{u} \in V \quad \forall x \in K, \forall \mathbf{u} \in V$,

(V2) $x \cdot_s (\mathbf{u}+\mathbf{v}) = x \cdot_s \mathbf{u} + x \cdot_s \mathbf{v} \quad \forall x \in K, \forall \mathbf{u},\mathbf{v} \in V$,

(V3) $(x+y) \cdot_s \mathbf{u} = x \cdot_s \mathbf{u} + y \cdot_s \mathbf{u} \quad \forall x,y \in K, \forall \mathbf{u} \in V$,

(V4) $x \cdot_s (y \cdot_s \mathbf{u}) = (xy) \cdot_s \mathbf{u} \quad \forall x,y \in K, \forall \mathbf{u} \in V$,

(V5) $1_K \cdot_s \mathbf{u} = \mathbf{u} \quad \forall \mathbf{u} \in V$

nazveme *vektorový prostor nad polem K* (anglicky *vector space over field K*). Pokud pole K nahradíme okruhem R, dostáváme *modul nad okruhem R*. Operaci $\cdot_s$ nazýváme *násobení skalárem z pole K.*.

Definice 2.1.5. Nechť R je okruh. Prvek $r \in R$, $r \neq 0_R$, nazveme *dělitel nuly*, jestliže $\exists s \in R, s \neq 0_R$, tak, že $rs = 0_R$.

Poznámka. Netriviální komutativní okruh bez dělitelů nuly se nazývá *obor integrity*.

Definice 2.1.6. Nechť R je okruh. Prvek $r \in R$, $r \neq 0_R$, se nazývá *nilpotentní*, jestliže $\exists n \in \mathbb{N}$ tak, že $r^n = 0_R$.

Poznámka. Jestliže je prvek nilpotentní, je také dělitel nuly (opak ale neplatí).

Definice 2.1.7. Nechť R je okruh. Prvek $r \in R$ nazveme *jednotka*, jestliže $\exists s \in R$ tak, že $rs = 1_R$.

Poznámka. Vidíme, že jednotka je takový prvek, ke kterému existuje multiplikativní inverze. Proto takový prvek někdy označujeme také jako *invertibilní prvek*.

Poznámka. Netriviální okruh je pole právě tehdy, když a je jednotka $\forall a \in R, a \neq 0_R$.

Tvrzení 2.1.8. *Množina jednotek tvoří (multiplikativní) grupu.*

Důkaz. Důkaz je zřejmý. Operace násobení je dle předchozího asociativní. Jednotkový prvek existuje, jelikož jednotkový prvek je jednotka a je sám sobě inverzí, a z definice jednotky plyne, že má svou multiplikativní inverzi. □

Definice 2.1.9. Nechť K je pole. Nejmenší $p \in \mathbb{N}$ takové, že $\underbrace{1 + \cdots + 1}_{p} = 0_K$, nazveme *charakteristika pole* K a značíme $\mathrm{char}(K)$. Pokud takové číslo p neexistuje, klademe pro uvažované pole $\mathrm{char}(K) = 0$.

Poznámka. Pro okruh zavádíme pojem *charakteristika okruhu* naprosto identicky jako u pole.

Poznámka. Pro konečné pole $\mathbb{F}_q$, kde $q = p^n$, p je prvočíslo a $n \in \mathbb{N}$, je $\mathrm{char}(\mathbb{F}_q) = p$.

Poznámka. Pro každé pole K takové, že $\mathbb{Q} \subseteq K$, je $\mathrm{char}(K) = 0$.

Definice 2.1.10. Nechť L je pole. Jestliže je K podpole pole L, nazýváme L *rozšíření pole* K.

Definice 2.1.11. Nechť L je rozšíření pole K. Potom prvek $a \in L$ nazýváme *algebraický nad polem* K, jestliže existuje nenulový polynom $f \in K[X]$ takový, že $f(a) = 0$, přičemž $K[X]$ značí okruh polynomů v neurčité X s koeficienty z K.

Definice 2.1.12. Nechť L je rozšíření pole K. Pak L nazýváme *algebraické rozšíření pole* K, jestliže každý prvek L je algebraický nad K.

Definice 2.1.13. Pole K nazveme *algebraicky uzavřené*, jestliže každý nekonstatní polynom $f \in K[X]$ má svůj kořen v K. *Algebraický uzávěr* je algebraické rozšíření pole K takové, že je algebraicky uzavřené. Značíme jej $\overline{K}$.

Poznámka. Konečná pole nejsou algebraicky uzavřená. Ale existuje nekonečné algebraicky uzavřené pole charakteristiky p, které značíme $\overline{\mathbb{F}_p}$ a které je algebraický uzávěr pro všechna pole $\mathbb{F}_{p^n}$.

$$\mathbb{F}_p \subset \mathbb{F}_{p^2} \subset \cdots \subset \overline{\mathbb{F}_p}$$

Další související pojmy k nalezení např. v [6]. Nám bude stačit pojem algebraického uzávěru.

2.2. Uspořádané množiny

V této pasáži si připomeneme vybrané pojmy týkající se uspořádaných množin neboli posetů.

Definice 2.2.1. Řekneme, že uspořádaná množina P splňuje *podmínku klesajících řetězců* (anglicky *descending chain condition*, stručně *DCC*), jestliže každá její klesající uspořádaná podmnožina je konečná, tj. má minimální prvek.
Analogicky, řekneme, že uspořádaná množina P splňuje *podmínku rostoucích řetězců* (anglicky *ascending chain condition*, stručně *ACC*), jestliže každá její rostoucí uspořádaná podmnožina je konečná, tj. má maximální prvek.

Definice 2.2.2. Nechť P je uspořádaná množina. Prvek $c \in P$ nazveme *horní závora prvků* a, b, jestliže platí

$$c \geq a \wedge c \geq b.$$

Analogicky, prvek $x \in P$ nazveme *dolní závora prvků* a, b, jestliže platí

$$x \leq a \wedge x \leq b.$$

Definice 2.2.3. Nechť P je uspořádaná množina. Nejmenší prvek z množiny všech horních závor prvků a, b nazýváme *suprémum prvků* a, b. Značíme jej $a \vee b$ nebo $\sup\{a, b\}$. Jinými slovy, prvek $c \in P$ se nazývá *suprémum prvků* a, b, jestliže platí:

(i) $c \geq a \wedge c \geq b$,

(ii) jestliže $\exists d \in P$, $d \geq a \wedge d \geq b$, potom $d \geq c$.

Analogicky největší prvek z množiny všech dolních závor prvků a, b nazýváme *infimum prvků* a, b. Značíme jej $a \wedge b$ nebo $\inf\{a, b\}$. Jinými slovy, prvek $x \in P$ se nazývá *infimum prvků* a, b, jestliže platí:

(i) $x \leq a \wedge x \leq b$,

(ii) jestliže $\exists y \in$P, $y \leq a \wedge y \leq b$, potom $y \leq x$.

Nyní již máme všechny potřebné pojmy k tomu, abychom mohli zavést speciální uspořádané množiny, svazy.

Definice 2.2.4. Uspořádanou množinu S nazveme *svaz* (anglicky *lattice*), jestliže každé její dva prvky mají své suprémum a infimum.

2.3. Ideály

V této kapitole se budeme věnovat speciálním podmnožinám okruhů, tzv. ideálům. Probereme si jejich základní typy a také operace, které pro ně lze zavést.

Definice 2.3.1. Nechť R je okruh. Množinu $\mathfrak{i} \subseteq R$, $\mathfrak{i} \neq \emptyset$, splňující:

(I1) $a, b \in \mathfrak{i} \Rightarrow a + b \in \mathfrak{i} \quad \forall a, b \in \mathfrak{i}$,

(I2) $a \in \mathfrak{i}, r \in R \Rightarrow ra \in \mathfrak{i} \quad \forall a \in \mathfrak{i}, r \in R$

nazveme *ideál* (anglicky *ideal*) okruhu R.

Poznámka. Vysvětlíme nyní, co znamená faktorizace okruhu jeho ideálem. Nechť R je okruh a $\mathfrak{i}$ jeho ideál. Uvažujme nyní nový okruh $R/\mathfrak{i}$, který sestrojíme tak, že všechny prvky ideálu $\mathfrak{i}$ budeme v okruhu R uvažovat jakožto nulové. Dostáváme tak okruh známý jako *faktorový okruh*, někdy také označovaný jako *okruh zbytkových tříd*. Formálně se faktorový okruh dá zavést tak, že se pro prvky okruhu R sestrojí relace ekvivalence (která je relací kongruence) a vzniklé třídy ekvivalence budou pak prvky faktorového okruhu, přičemž se ještě dodefinuje součet a součin tříd ekvivalence.

Definice 2.3.2. Nechť R je okruh a $\mathfrak{p}$ jeho ideál. Ideál $\mathfrak{p}$ nazveme *prvoideál*, jestliže $\mathfrak{p} \neq R$ a $xy \in \mathfrak{p} \Longrightarrow x \in \mathfrak{p} \vee y \in \mathfrak{p}$.

Poznámka. Platí, že ideál $\mathfrak{p}$ je *prvoideál* právě tehdy, když $R/\mathfrak{p}$ je obor integrity ($R/\mathfrak{p}$ značí faktorizaci okruhu R ideálem $\mathfrak{p}$).

Definice 2.3.3. Nechť R je okruh a $\mathfrak{m}$ jeho ideál. Ideál $\mathfrak{m}$ nazveme *maximální*, jestliže $\mathfrak{m} \neq R$ a pro každý ideál $\mathfrak{i}$, $R \supset \mathfrak{i} \supseteq \mathfrak{m}$, platí $\mathfrak{i} = \mathfrak{m}$.

Poznámka. Dá se ukázat (viz např. [1]), že ideál $\mathfrak{m}$ je *maximální* právě tehdy, když $R/\mathfrak{m}$ je pole.

Definice 2.3.4. Nechť R je okruh a zvolme prvek $x \in R$. Množinu $\mathfrak{i} = \{xa; a \in R\}$ nazveme *hlavní ideál* generovaný prvkem x. Značíme jej (x).

Poznámka. Prvek $x \in R$ je jednotka právě tehdy, když $(x) = R = (1)$.

Ideál však nemusí být generovaný pouze jedním prvkem. Uvažujme okruh R a nechť $X = \{x_1, \ldots, x_n\} \subset R$. Potom ideál generovaný množinou X je ideál

$$\mathfrak{i} = \{r_1x_1 + \cdots + r_nx_n; r_i \in R, x_i \in X, i = 1, 2, \ldots, n\}.$$

Tento ideál označujeme $\mathfrak{i} = (x_1, \ldots, x_n)$. Tedy hlavní ideál je speciálním případem, kdy množina X je jednoprvková.

Dále uvedeme běžné operace s ideály:

a) Součet ideálů $\mathfrak{i}, \mathfrak{j}$, který značíme $\mathfrak{i} + \mathfrak{j}$, je ideál

$$\mathfrak{i} + \mathfrak{j} = \{x + y; x \in \mathfrak{i}, y \in \mathfrak{j}\}.$$

Jedná se o nejmenší ideál obsahující ideály $\mathfrak{i}$ a $\mathfrak{j}$. Součet konečného počtu (a dokonce spočetného počtu) ideálů je také ideál.

b) Průnik ideálů $\mathfrak{i}, \mathfrak{j}$ značíme $\mathfrak{i} \cap \mathfrak{j}$ a výsledkem je opět ideál.

c) Součin ideálů $\mathfrak{i}, \mathfrak{j}$, který značíme $\mathfrak{ij}$, je ideál generovaný prvky xy, $x \in \mathfrak{i}$ a $y \in \mathfrak{j}$. Neboli součin ideálů $\mathfrak{i}$, $\mathfrak{j}$ je ideál

$$\mathfrak{ij} = \left\{ \sum_{i=1}^{n} x_iy_i; x_i \in \mathfrak{i}, y_i \in \mathfrak{j}, i = 1, 2, \ldots, n, n \in \mathbb{N} \right\}.$$

Součin ideálů můžeme rozšířit na konečný počet ideálů. Zejména definujeme mocniny ideálu $\mathfrak{i}^n$ ($n > 0$). Tedy ideál $\mathfrak{i}^n$ je generovaný součiny $x_1x_2 \ldots x_n$, kde $x_i \in \mathfrak{i}$, $i = 1, 2, \ldots, n$. $\mathfrak{i}^0$ značí (1).

V [1] jsou dále rozebírány vlastnosti uvedených operací.

Definice 2.3.5. Nechť $\mathfrak{n}$ je ideál. Pokud existuje $n \in \mathbb{N}$ takové, že $\mathfrak{n}^n = \mathfrak{o}$, nazýváme ideál $\mathfrak{n}$ *nilpotentní* (také *nilradikál*), přičemž $\mathfrak{o}$ značí *nulový ideál* okruhu R obsahující pouze nulový prvek okruhu R.

2.4. Okruhové a algebrové homomorfismy

Nyní se zaměříme na speciální zobrazení mezi okruhy, tzv. okruhové homomorfismy, pomocí kterých zavedeme pojem R-algebry nad okruhem R. V jedné z dalších kapitol se potom zaměříme na speciální $\mathbb{R}$-algebry.

Definice 2.4.1. Nechť $(R, +_R, \cdot_R)$, $(S, +_S, \cdot_S)$ jsou okruhy. Zobrazení $\varphi : R \to S$ nazveme *okruhový homomorfismus*, jestliže platí:

(i) $\varphi(x +_R y) = \varphi(x) +_S \varphi(y) \quad \forall x, y \in R,$

(ii) $\varphi(x \cdot_R y) = \varphi(x) \cdot_S \varphi(y) \quad \forall x, y \in R,$

(iii) $\varphi(1_R) = 1_S.$

Poznámka. Vidíme, že okruhový homomorfismus zachovává operace (sčítání a násobení) a jednotkový prvek.

Definice 2.4.2. Nechť $(R, +_R, \cdot_R)$, $(S, +_S, \cdot_S)$ jsou okruhy a $\varphi : R \to S$ je okruhový homomorfismus. Pak zavádíme následující pojmy:

(i) $\mathrm{Ker}(\varphi) = \varphi^{-1}(0_S) = \{r \in R; \varphi(r) = 0_S\}$ - *jádro okruhového homomorfismu* φ,

(ii) $\mathrm{Im}(\varphi) = \varphi(R) = \{s \in S; \exists r \in R$ tak, že $\varphi(r) = s\}$ - *obraz okruhového homomorfismu* φ.

Tvrzení 2.4.3. *Nechť $(R, +_R, \cdot_R)$, $(S, +_S, \cdot_S)$ jsou okruhy a $\varphi : R \to S$ je okruhový homomorfismus. Pak platí:*

(i) $\mathrm{Ker}(\varphi)$ *je ideál okruhu* R,

(ii) $\mathrm{Im}(\varphi)$ *tvoří podokruh okruhu* S.

Důkaz. (i) Je potřeba dokázat dvě věci. Zaprvé že pro dva prvky $a, b \in \mathrm{Ker}(\varphi)$ máme také $a +_R b \in \mathrm{Ker}(\varphi)$. Jelikož okruhový homomorfismus zachovává operace, můžeme psát

$$\varphi(a +_R b) = \varphi(a) +_S \varphi(b) = 0_S +_S 0_S = 0_S \Rightarrow a +_R b \in \mathrm{Ker}(\varphi).$$

Dále je potřeba dokázat, že pro $a \in \mathrm{Ker}(\varphi)$ a $r \in R$ dostaneme $r \cdot_R a \in \mathrm{Ker}(\varphi)$. Z definice okruhového homomorfismu dostáváme

$$\varphi(r \cdot_R a) = \varphi(r) \cdot_S \varphi(a) = \varphi(r) \cdot_S 0_S = 0_S \Rightarrow r \cdot_R a \in \mathrm{Ker}(\varphi).$$

Celkově $\mathrm{Ker}(\varphi)$ je ideál okruhu R.

(ii) Uzavřenost $\mathrm{Im}(\varphi)$ vůči operacím $+_S$ a $\cdot_S$ je zřejmá a existence jednotkového prvku plyne z toho, že okruhový homomorfismus zachovává jednotkový prvek. □

Definice 2.4.4. Nechť $(R, +_R, \cdot_R)$ je okruh. Množinu

$$Z(R) = \{x; x \in R, x \cdot_R r = r \cdot_R x \quad \forall r \in R\}$$

nazveme *centrum okruhu* R.

Definice 2.4.5. Nechť $(R, +_R, \cdot_R)$, $(S, +_S, \cdot_S)$ jsou okruhy. Existuje-li okruhový homomorfismus $\varphi : R \to S$ tak, že $\mathrm{Dom}(\varphi) = R$ a $\mathrm{Im}(\varphi) \subseteq Z(S)$, řekneme, že S je *R-algebra*. Pak máme zavedenou operaci násobení $\cdot : R \times S \to S$ takto

$$r \cdot s = \varphi(r) \cdot_S s.$$

Poznámka. V případě, že R je okruh, je R-algebra modul nad okruhem R. Je-li R pole, je R-algebra vektorový prostor nad polem R.

Tvrzení 2.4.6. *Každý okruh je $\mathbb{Z}$-algebrou.*

Důkaz. Nechť R je okruh. Okruhový homomorfismus $\varphi : \mathbb{Z} \to R$ je určen tím, že

$$\varphi(1_{\mathbb{Z}}) = 1_R.$$

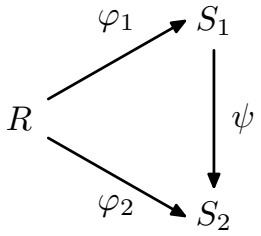
Nyní je potřeba rozmyslet, zda se jedná o okruh konečný, nebo nekonečný. V případě nekonečného okruhu položíme pro $z \in \mathbb{Z}$

$$\varphi(z) = \begin{cases} \underbrace{(1_R +_R \cdots +_R 1_R)}_{\mathrm{abs}(z)} & \text{pro } z > 0 \\ 0_R & \text{pro } z = 0 \\ -1_R \cdot_R \underbrace{(1_R +_R \cdots +_R 1_R)}_{\mathrm{abs}(z)} & \text{pro } z < 0 \end{cases},$$

kde -1_R je opačný prvek k prvku 1_R. V případě konečného okruhu určíme jeho charakteristiku p a homomorfimus předepíšeme obdobně pro zbytkové třídy $\bmod p$.
Zachování operace násobení je zřejmé. □

Definice 2.4.7. Řekneme, že S_1, S_2 jsou dvě R-algebry, pokud existuje okruhový homomorfismus $\psi : S_1 \to S_2$. Okruhový homomorfismus ψ nazveme R-algebrový homomorfismus, jestliže platí

$$\psi \circ \varphi_1 = \varphi_2.$$



Obrázek 2.1: R-algebrový homomorfismus

Poznámka. Množinu všech R-algebrových homomorfismů z S_1 do S_2 značíme $\mathrm{Hom}_R(S_1, S_2)$. Pokud ψ je okruhový izomorfismus a $S_1 = S_2 = S$, pak ψ je R-algebrový automorfismus. Analogicky, množinu všech R-algebrových automorfismů S budeme značit $\mathrm{Aut}_R S$.

Tvrzení 2.4.8. *Množina $\mathrm{Aut}_R S$ s operací skládání zobrazení je grupa.*

Důkaz. Důkaz je zřejmý. Skládání zobrazení je asociativní, neutrální prvek je identický R-algebrový automorfismus a inverzní prvek je inverzní R-algebrový automorfismus. □

3. Drozdovy okruhy

Nyní se budeme zabývat speciálními okruhy, tzv. Drozdovými okruhy. K jejich zavedení budeme potřebovat několik dalších vlastností okruhů, které teď vysvětlíme.

Definice 3.1.1. Okruh nazveme *lokální*, jestliže má jediný maximální ideál.

Definice 3.1.2. Okruh nazveme *noetherovský*, jestliže splňuje podmínku rostoucích řetězců pro své ideály.

Definice 3.1.3. Okruh nazveme *artinovský*, jestliže splňuje podmínku klesajících řetězců pro své ideály.

Nyní už máme všechny potřebné pojmy k tomu, abychom mohli uvést definici Drozdova okruhu.

Definice 3.1.4. Lokální noetherovský artinovský okruh R nazveme *Drozdův okruh*, jestliže $\mu(\mathfrak{m}) = 2$, $\mu(\mathfrak{m}^2) = 2$, $\mathfrak{m}^3 = \mathfrak{o}$ a $\exists z \in \mathfrak{m} - \mathfrak{m}^2$ tak, že $z^2 = 0_R$, kde $\mathfrak{m}$ je maximální ideál okruhu R, $\mathfrak{o}$ je nulový ideál okruhu R a $\mu(\mathfrak{m})$ značí minimální počet prvků potřebných k vygenerování $\mathfrak{m}$.[1]

Každý Drozdův okruh má následující vlastnost, díky které vypadá jako známá pětidimenzionální Drozdova algebra nad libovolným polem K, přičemž bázi této algebry tvoří prvky $1_K, x, x, xy$ a x^2 a všechny další monomy jsou rovny nule.

Lemma 3.1.5. *Uvažujme Drozdův okruh a $\mathfrak{m}$ jeho maximální ideál. Pak pro každý prvek $c \in \mathfrak{m}$ platí*

$$c = u_1 x + u_2 y + u_3 xy + u_4 x^2,$$

přičemž u_i, $i = 1, \ldots, 4$, jsou jednotky nebo rovny nule. Koeficienty u_i, $i = 1, \ldots, 4$, nejsou určeny jednoznačně.

Důkaz. Viz [4], Lemma 4.2. □

Nyní uvedeme příklad Drozdova okruh, viz [3]. Jelikož autoři tento okruh pouze uvádějí, tak prověříme, zda se vážně jedná o Drozdův okruh.

Věta 3.1.6. *Okruh $A_p = \mathbb{Z}[X]/(X^2, p^3, p^2X)$, kde p je prvočíslo a X neurčitá, je Drozdův okruh.*

Důkaz. Nejprve popíšeme strukturu A_p. Prvky jsou tvaru

$$a + bx, a, b \in \mathbb{Z},$$

kde a, b budou specifikovány dále. Tedy prvky budou polynomy maximálně prvního stupně, protože $X^2 \in (X^2, p^3, p^2X)$. Každé $a \in \mathbb{Z}$ můžeme napsat ve tvaru

$$a = kp^3 + q, k \in \mathbb{Z}, q \in \{0, 1, \ldots, p^3 - 1\}.$$

[1] Jurij Drozd, profesor působící v rámci Matematického ústavu, Národní akademie věd, Kyjev, Ukrajina.

A protože $p^3 \in (X^2, p^3, p^2X)$, můžeme psát

$$a = q.$$

Obdobně pro každé $b \in \mathbb{Z}$ platí

$$b = lp^2 + r, l \in \mathbb{Z}, r \in \{0, 1, \ldots, p^2 - 1\} \Rightarrow b = r.$$

Celkově dostáváme

$$A_p = \{a + bx; a, b \in \mathbb{N}_0, a < p^3, b < p^2\}.$$

Tedy operace se počítají modulárně a to následovně - v absolutním členu $\bmod p^3$ a v lineárním členu $\bmod p^2$.

Aby okruh A_p byl Drozdův okruh, musí být noetherovský, artinovský a lokální. Dále musí platit

$$\mu(\mathfrak{m}) = \mu(\mathfrak{m}^2) = 2, \mathfrak{m}^3 = \mathfrak{o},$$

a musí existovat prvek z takový, že

$$z \in \mathfrak{m} - \mathfrak{m}^2, z^2 = 0_{A_p}.$$

Z těchto vlastností nejprve dokážeme, že

$$\mathfrak{m} = \mathfrak{i}_1 = \{a + bx; a = kp, k \in \mathbb{N}_0, k < p^2, b < p^2\}$$

je jediný maximální ideál. Z A_p nemůžeme vypustit žádný lineární člen, jinak by se nejednalo o ideál - násobením prvkem x bychom z absolutního členu dostali právě ten vypuštěný lineární. Neboli

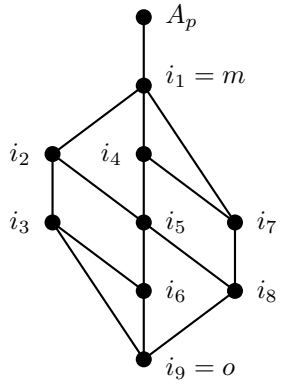
$$bx \notin \mathfrak{m} \Rightarrow b \notin \mathfrak{m}.$$

Takto dostaneme uzavřenost na násobení prvky z A_p. Omezení tak můžeme udělat pouze v členech absolutních. Nejvíce absolutních členů dostaneme tak, že za ně vezmeme pouze násobky p. Dostaneme tak uzavřenost $\mathfrak{m}$ na operaci sčítání.

Dále vypišme všechny možné ideály okruhu A_p:

$$\begin{aligned}
\mathfrak{i}_2 &= \{a + bx; a = kp, b = lp, k, l \in \mathbb{N}_0, k < p^2, l < p\},\\
\mathfrak{i}_3 &= \{a + bx; a = kp, k \in \mathbb{N}_0, k < p^2, b = 0\},\\
\mathfrak{i}_4 &= \{a + bx; a = kp^2, k \in \mathbb{N}_0, k < p, b < p^2\},\\
\mathfrak{i}_5 &= \{a + bx; a = kp^2, b = lp, k, l \in \mathbb{N}_0, k < p, l < p\},\\
\mathfrak{i}_6 &= \{a + bx; a = kp^2, k \in \mathbb{N}_0, k < p, b = 0\},\\
\mathfrak{i}_7 &= \{a + bx; a = 0, b < p^2\},\\
\mathfrak{i}_8 &= \{a + bx; a = 0, b = lp, l \in \mathbb{N}_0, l < p\},\\
\mathfrak{i}_9 &= \{a + bx; a = 0, b = 0\},
\end{aligned}$$

přičemž $\mathfrak{i}_9 = \mathfrak{o}$ je nulový ideál okruhu A_p. Platí, že také A_p je ideálem. Množinu ideálů okruhu A_p nyní zobrazme v Hasseově diagramu.



Obrázek 3.1: Hasseův diagram ideálů okruhu A_p

Je zřejmé, že ať vezmeme jakoukoli rostoucí posloupnost ideálů, tak je konečná a její minimální prvek je $\mathfrak{m} = \mathfrak{i}_1$, tj. maximální ideál. Tedy okruh A_p splňuje podmínku ACC neboli je noetherovský. Dále je ihned vidět, že okruh A_p splňuje také podmínku DCC neboli je artinovký.

Dále platí

$$(a + bx)^3 = a^3 + a^2bx.$$

Protože $a = kp$, je $a^3 = k^3p^3$, tj. $a^3 = 0_{A_p}$. Dále $a^2b = k^2p^2$, tj. $a^2b = 0_{A_p}$. Tedy platí podmínka

$$\mathfrak{m}^3 = \mathfrak{o}.$$

V dalším určíme generátory $\mathfrak{m}$ a $\mathfrak{m}^2$. Ze struktury $\mathfrak{m}$ je zřejmé, že jeho generátory budou prvky p a x, tudíž máme splněnu podmínku

$$\mu(\mathfrak{m}) = 2.$$

Dále máme

$$(a + bx)^2 = a^2 + abx, \text{ kde } a^2 = k^2p^2 \text{ a } ab = kp.$$

Je vidět, že generátory $\mathfrak{m}^2$ budou prvky p^2 a pX. Takže jsme ukázali, že platí

$$\mu(\mathfrak{m}^2) = 2.$$

Nakonec vezmeme prvek $z = x$, $z \in \mathfrak{m} - \mathfrak{m}^2$. Zároveň ale platí, že $z^2 = x^2 = 0_{A_p}$, protože $X^2 \in (X^2, p^3, p^2X)$. Celkově máme, že okruh A_p je Drozdův okruh. □

Poznámka. Je vidět, že množina ideálů okruhu A_p tvoří svaz (zřejmé z Hasseova diagramu pro ideály tohoto okruhu, obrázek 3.1). V tomto případě máme $\sup\{\mathfrak{i}_i, \mathfrak{i}_j\} = \mathfrak{i}_i \cup \mathfrak{i}_j$ a $\inf\{\mathfrak{i}_i, \mathfrak{i}_j\} = \mathfrak{i}_i \cap \mathfrak{i}_j$.

Tento okruh ale není algebrou, jak nyní ukážeme. Drozdovým okruhům, které jsou také algebrami, se budeme věnovat v další kapitole.

Věta 3.1.7. *Drozdův okruh A_p není algebrou nad polem.*

Důkaz. Nutno ukázat, že A_p není algebrou nad polem kladné charakteristiky (jsou možné případy: $\mathbb{F}_p$, $\mathbb{F}_{p^n}$, kde p je prvočíslo a $n \in \mathbb{N}$, $\mathbb{F}_q$, přičemž $p \neq q$, a $\overline{\mathbb{F}_p}$) ani nad polem charakteristiky nulové. Platí, že každé pole nulové charakteristiky obsahuje pole racionálních čísel $\mathbb{Q}$ - stačí tedy ukázat, že A_p není $\mathbb{Q}$-algebrou.

Vezměme nejprve případ pole $\mathbb{F}_p$. Připomeňme strukturu A_p

$$A_p = \{a + bx, a \in \{0, 1, \ldots, p^3 - 1\}, b \in \{0, 1, \ldots, p^2 - 1\}\}$$

a strukturu $\mathbb{F}_p$

$$\mathbb{F}_p = \{0, 1, \ldots, p - 1\}.$$

Předpokládejme, že existuje okruhový homomorfismus $\varphi : \mathbb{F}_p \to A_p$. Aby byla splněna podmínka zachování jednotkového prvku, předepíšeme

$$1 \mapsto 1 + 0x.$$

Dále

$$\varphi(0) = \varphi(\underbrace{1 + \cdots + 1}_{p}) = \underbrace{\varphi(1) + \cdots + \varphi(1)}_{p} = \underbrace{1 + \cdots + 1}_{p} = p, \quad \text{tedy } 0 \mapsto p.$$

Protože φ má zachovávat operace, musí platit

$$1 = \varphi(1) = \varphi(1 + 0) = \varphi(1) + \varphi(0) = 1 + p.$$

Dostáváme tak spor, tzn. A_p není $\mathbb{F}_p$-algebra.

Nyní vezmeme případ $\mathbb{F}_{p^n}$. Struktura tohoto pole je následující

$$\mathbb{F}_{p^n} = \{0, 1, \ldots, p - 1, x, \ldots, (p - 1)x^n + \cdots + (p - 2), (p - 1)x^n + \cdots + (p - 1)\}.$$

Z podmínky, že okruhový homomorfismus zachovává jednotkový prvek, dostáváme

$$1 \mapsto 1 + 0x.$$

Obdobně jako v předchozím případě

$$\varphi(0) = \varphi(\underbrace{1 + \cdots + 1}_{p}) = \underbrace{\varphi(1) + \cdots + \varphi(1)}_{p} = \underbrace{1 + \cdots + 1}_{p} = p, \quad \text{tedy } 0 \mapsto p.$$

A protože homorfismus má zachovat operace, máme

$$1 = \varphi(1) = \varphi(1 + 0) = \varphi(1) + \varphi(0) = 1 + p.$$

Stejně, jako v předešlém případě, jsme došli ke sporu, tzn. A_p není $\mathbb{F}_{p^n}$-algebra. Toto bychom také mohli dokázat úvahou, že pro $\mathbb{F}_p$ a $\mathbb{F}_{p^n}$ platí

$$\mathbb{F}_p \subset \mathbb{F}_{p^n}$$

pro $n > 1$. Tedy není-li A_p $\mathbb{F}_p$-algebrou, nebude ani $\mathbb{F}_{p^n}$-algebrou.

Stejnou úvahou odvodíme, že A_p není $\overline{\mathbb{F}_p}$-algebrou.

Nyní vezměme příklad pole $\mathbb{F}_q$, kde q je prvočíslo, $q \neq p$. Opět z podmínky, že okruhový homomorfimus má zachovat jednotkový prvek, položíme

$$1 \mapsto 1 + 0x.$$

Dále, stejně jako v předchozích případech, dostáváme

$$\varphi(0) = \varphi(\underbrace{1 + \cdots + 1}_{q}) = \underbrace{\varphi(1) + \cdots + \varphi(1)}_{q} = \underbrace{1 + \cdots + 1}_{q} = p, \quad \text{tedy } 0 \mapsto q.$$

Nyní položme

$$1 = \varphi(1) = \varphi(1 + 0) = \varphi(1) + \varphi(0) = 1 + q.$$

Aby poslední rovnost platila, musí platit

$$q = p^{3n}.$$

To je ale v rozporu s předpokladem, že q je prvočíslo, takže dostáváme spor, tzn. A_p není $\mathbb{F}_q$-algebrou.

Tímto jsme vyloučili případy polí kladné charakteristiky, nyní je potřeba vyloučit možnost, že A_p je algebrou nad nějakým polem nulové charakteristiky. Jak již bylo řečeno, každé takové pole obsahuje pole racionálních čísel $\mathbb{Q}$, tedy stačí ukázat, že A_p není $\mathbb{Q}$-algebrou. Protože okruhový homomorfismus musí zachovat jednotkový prvek, předepíšeme

$$1 \mapsto 1 + 0x.$$

Potom z podmínky, že okruhový homomorfismus má zachovat operace, dostáváme

$$1 = \varphi(1) = \varphi\left(\frac{1}{2} + \frac{1}{2}\right) = \varphi\left(\frac{1}{2}\right) + \varphi\left(\frac{1}{2}\right).$$

Pro čísla $q \notin \mathbb{Z}$ tedy okruhový homomorfismus neexistuje, čímž dostáváme spor, protože musí platit

$$\mathrm{Dom}\varphi = \mathbb{Q}.$$

Ukázali jsme, že A_p není $\mathbb{Q}$-algebra, čímž jsme vyloučili všechna možná pole nulové charakteristiky.

Dokázali jsme tak tvrzení, že Drozdův okruh $A_p = \mathbb{Z}[X]/(p^3, p^2X, X^2)$ není algebrou nad žádným polem. □

4. Grupy $\mathbb{R}$-algebrových automorfismů Drozdových $\mathbb{R}$-algeber

V této kapitole se budeme zabývat Drozdovými algebrami (Drozdovy okruhy, které jsou zároveň algebrami). Konkrétně se zaměříme na Drozdovy $\mathbb{R}$-algebry a zejména pak na jejich grupy $\mathbb{R}$-algebrových automorfismů, které pro ně lze zkonstruovat. Zajímavostí je to, že tyto grupy jsou příklady Lieových grup, o kterých bude pojednávat další kapitola. Začneme tím, že zavedeme Weilovou algebru a později se dostaneme k Drozdovým $\mathbb{R}$-algebrám.

4.1. Weilovy algebry

Zaveďme označení

$$\mathbb{D}_n^r = \mathbb{R}[X_1, \ldots, X_n]/(X_1, \ldots, X_n)^{r+1},$$

přičemž $\mathfrak{m} = (X_1, \ldots, X_n)$ je maximální ideál $\mathbb{R}[X_1, \ldots, X_n]$. Takto dostáváme okruh polynomů stupně maximálně r nad $\mathbb{R}$, který je zároveň $\mathbb{R}$-algebrou. Maximální ideál $\mathbb{D}_n^r$ budeme značit $\mathfrak{n}$, protože se jedná o nilpotentní ideál. Skutečně, z definice $\mathbb{D}_n^r$ je zřejmé, že existuje $n \in \mathbb{N}$ tak, že $\mathfrak{n}^n = \mathfrak{o}$. Prvky toho ideálu jsou polynomy stupně jedna až r v neurčitých $x_1, \ldots, x_n$ takové, že neobsahují absolutní člen, tedy $\mathfrak{n} = (x_1, \ldots, x_n)$.

Definice 4.1.1. Uvažujme $\mathbb{R}$-algebru $\mathbb{D}_n^r$ a její ideál $\mathfrak{i}$. Potom libovolnou $\mathbb{R}$-algebru typu

$$A = \mathbb{D}_n^r/\mathfrak{i},$$

nazýváme *Weilova algebra.*

Grupu $\mathbb{R}$-algebrových automorfismů Weilovy algebry A budeme značit $\mathrm{Aut}_{\mathbb{R}}A$. Pro Weilovy algebry dále zavádíme dva pojmy - jejich řád a šířku. Nilpotentní ideál Weilovy algebry A budeme označovat $\mathfrak{n}_A$. Tohoto využijeme k definici řádu a šířky Weilovy algebry.

Definice 4.1.2. Řád Weilovy algebry A je takové $r \in \mathbb{N}$, že

$$\mathfrak{n}_A^r \neq \mathfrak{o} \quad \text{a} \quad \mathfrak{n}_A^{r+1} = \mathfrak{o}.$$

Značíme jej $\mathrm{ord}(A)$. Dále šířku Weilovy algebry A definujeme následovně

$$\mathrm{w}(A) = \dim(\mathfrak{n}_A/\mathfrak{n}_A^2).$$

Tvrzení 4.1.3. *Uvažujme $\mathbb{R}$-algebru $\mathbb{D}_n^r$. Potom platí*

$$\mathrm{ord}(\mathbb{D}_n^r) = r, \quad \mathrm{w}(\mathbb{D}_n^r) = n.$$

Důkaz. $\mathbb{D}_n^r$ je speciálním případem Weilovy algebry, kdy ideál $\mathfrak{i}$ je nulový ideál. Z definice $\mathbb{D}_n^r$ plyne, že její nilpotentní ideál $\mathfrak{n}$ je množina polynomů stupně jedna až r, které neobsahují absolutní člen. Dále pro tento ideál platí

$$X_i^k X_j^l = 0 \Longleftrightarrow k + l > r \quad i, j \in 1, \ldots, n.$$

Tedy je zřejmé, že platí $\mathfrak{n}^r \neq \mathfrak{o}$, protože $\mathfrak{n}^r$ bude obsahovat polynomy stupně r a to takové, že budou obsahovat pouze monomy stupně r. Ihned vidíme, že $\mathfrak{n}^{r+1} = \mathfrak{o}$. Dle definice řádu Weilovy algebry dostáváme $\mathrm{ord}(\mathbb{D}_n^r) = r$.

Dále si uvědomme, že $\mathfrak{n}^2$ obsahuje polynomy stupně dva až r, které neobsahují absolutní ani lineární členy. Tedy pokud provedeme faktorizaci $\mathfrak{n}/\mathfrak{n}^2$, dostaneme množinu polynomů stupně jedna v n neurčitých $X_1, \ldots, X_n$, které neobsahují absolutní člen. Odtud plyne tvrzení, protože $\mathrm{w}(\mathbb{D}_n^r) = \dim(\mathfrak{n}/\mathfrak{n}^2) = n$. □

Tvrzení 4.1.4. *Uvažujme Weilovu algebru $A = \mathbb{D}_n^r/\mathfrak{i}$, přičemž $\mathfrak{i} \subset \mathfrak{n}^2$. Pak platí*

$$\mathrm{w}(A) = n.$$

Důkaz. Uvedeme pouze ideu důkazu. Podmínka, kterou klademe na ideál $\mathfrak{i}$, znamená, že $\mathfrak{i}$ obsahuje pouze polynomy stupně dva až r, přičemž tyto polynomy neobsahují absolutní ani lineární členy. Tedy pokud provedeme faktorizaci $A = \mathbb{D}_n^r/\mathfrak{i}$, nevynulujeme žádné polynomy stupně jedna. Nilpotentní ideál $\mathfrak{n}_A$ Weilovy algebry A tak bude obsahovat všechny polynomy stupně jedna stejně jako nilpotentní ideál $\mathfrak{n}$ Weilovy algebry $\mathbb{D}_n^r$. Potom už analogickým postupem jako v důkazu tvrzení 4.1.3 dostaneme, že $\mathrm{w}(A) = \dim(\mathfrak{n}_A/\mathfrak{n}_A^2) = n$. □

Poznámka. Budeme dále uvažovat Weilovy algebry $\mathbb{D}_n^r/\mathfrak{i}$ takové, že $\mathfrak{i} \subset \mathfrak{n}^2$. Takovéto ideály $\mathfrak{i}$ budeme nazývat vhodné a dle předchozího tvrzení vidíme, že nezmenšují šířku Weilovy algebry. Neformálně můžeme říct, že při faktorizaci Weilovy algebry $\mathbb{D}_n^r$ ideálem $\mathfrak{i}$ se nám nesníží počet neurčitých, v nichž jsou polynomy z A. Toto přiblížíme na následujícím příkladu.

Příklad 4.1.5. Uvažujme Weilovu algebru $A = \mathbb{D}_3^r/(Z)$, kde neurčité označme $X_1 = X$, $X_2 = Y$ a $X_3 = Z$. Ale protože jsme vzali $\mathfrak{i} = (Z)$, dostáváme Weilovu algebru $B = \mathbb{D}_2^r$, kde neurčité jsou $X_1 = X$ a $X_2 = Y$. Tedy zápisem by se zdálo, že se jedná o dvě různé Weilovy algebry, ale při bližším zoumání je ihned vidět, že Weilovy algebry A a B jsou totožné (toto zde nebudeme rozepisovat, protože je zřejmé, že volbou $\mathfrak{i} = (Z)$ jsme položili všechny monomy obsahující neurčitou Z rovny nule a ve Weilově algebře A tak zůstaly pouze polynomy v neurčitých X a Y). Tedy máme nejednoznačné označení Weilovy algebry a to právě proto, že jsme zvolili nevhodný ideál $\mathfrak{i}$. Proto budeme nadále požadovat podmínku na ideál $\mathfrak{i}$ uvedenou v tvrzení 4.1.4

Poznámka. Když v $\mathbb{D}_n^r$ položíme $n = 1$ a $r = 1$, dostáváme strukturu

$$\mathbb{D} = \mathbb{D}_1^1 = \mathbb{R}[X]/(X)^2 = \{a + bx; a, b \in \mathbb{R}, x^2 = 0\},$$

známou jako duální čísla.

Poznámka. Pojem Weilovy algebry můžeme zobecnit tím, že místo pole $\mathbb{R}$ budeme uvažovat jiné pole, např. pole konečné. U těchto algeber lze opět sestrojit grupy jejich algebrových automorfismů. Nejedná se v tomto případě o Lieovy grupy, nýbrž *grupy Lieova typu.* Např. pro

$$\left(\mathbb{D}_{\mathbb{F}_p}\right)_2^1 = \mathbb{F}_p[X, Y]/(X, Y)^2$$

máme grupu automorfismů, kterou označujeme $\mathrm{GL}(2, \mathbb{F}_p)$. Více k těmto algebrám v příloze.

4.2. Drozdovy $\mathbb{R}$-algebry

Vraťme se k Weilovým algebrám nad $\mathbb{R}$. V kapitole 3 jsme uvedli Drozdův okruh, pro který se ukázalo, že není algebrou nad žádným polem. Pokud však budeme uvažovat Weilovu algebru $\mathbb{D}_n^r/\mathfrak{i}$ a položíme $n = 2$, $r = 2$ a $\mathfrak{i} = (X^2)$, dostaneme známou Drozdovu $\mathbb{R}$-algebru

$$D_1 = \mathbb{D}_2^2/(X^2) = \{a + bx + cy + dxy + ey^2; a, b, c, d, e \in \mathbb{R}, x^2 = y^2x = y^3 = 0\}.$$

Nejprve ukažme, že se jedná o Drozdovu $\mathbb{R}$-algebru. Zřejmě

- $\mu(\mathfrak{n}_{D_1}) = 2$ - prvky x a y,
- $\mu(\mathfrak{n}_{D_1}^2) = 2$ - prvky xy a y^2,
- $\mathfrak{n}_{D_1}^3 = \mathfrak{o}$,
- $z = x \in \mathfrak{n}_{D_1} - \mathfrak{n}_{D_1}^2$ a platí $z^2 = x^2 = 0$.

$\mathbb{R}$-algebrové automorfismy popíšeme následovně

$$\begin{aligned} 1 &\mapsto 1, \\ x &\mapsto Ax + By + Cxy + Dy^2, \\ y &\mapsto Ex + Fy + Gxy + Hy^2, \ A, B, C, D, E, F, G, H \in \mathbb{R}. \end{aligned}$$

Z podmínky $x^2 = 0$ dostáváme

$$0 = x^2 = (Ax + By + Cxy + Dy^2)^2 = 2ABxy + B^2y^2 \Rightarrow B = 0.$$

Dále musí platit (z podmínky invertibility)

$$AF - BE \neq 0 \Rightarrow AF \neq 0, \text{ protože } B = 0.$$

Tedy pro předpis $\mathbb{R}$-algebrových automorfismů celkově máme

$$\begin{aligned} 1 &\mapsto 1, \\ x &\mapsto Ax + Cxy + Dy^2, \\ y &\mapsto Ex + Fy + Gxy + Hy^2, \ A, C, D, E, F, G, H \in \mathbb{R}, AF \neq 0. \end{aligned}$$

Dále můžeme předpis Weilovy algebry změnit v tom smyslu, že položíme $\mathfrak{i} = (Y^2)$ a dostaneme tak

$$D_2 = \mathbb{D}_2^2/(Y^2) = \{a + bx + cy + dx^2 + exy; a, b, c, d, e \in \mathbb{R}, y^2 = x^3 = x^2y = 0\}.$$

Opět se jedná o Drozdovu $\mathbb{R}$-algebru. $\mathbb{R}$-algebrové automorfismy popíšeme jako v předchozím případě a z podmínky $y^2 = 0$ dostáváme

$$0 = y^2 = (Ex + Fy + Gxy + Hy^2)^2 = E^2x^2 + 2EFxy \Rightarrow E = 0.$$

Stejně jako v přechozím případě obdržíme

$$AF \neq 0.$$

Tedy pro předpis $\mathbb{R}$-algebrových automorfismů celkově máme

$$\begin{aligned} 1 &\mapsto 1, \\ x &\mapsto Ax + By + Cxy + Dy^2, \\ y &\mapsto Fy + Gxy + Hy^2, \ A, B, C, D, F, G, H \in \mathbb{R}, AF \neq 0. \end{aligned}$$

Tvrzení 4.2.1. *Drozdovy $\mathbb{R}$-algebry D_1 a D_2 jsou izomorfní.*

Důkaz. Izomorfismus $\varphi : D_1 \to D_2$ zavedeme následovně

$$\varphi(x) = y,$$
$$\varphi(y) = x.$$

□

Tvrzení 4.2.2. *Grupy automorfismů* $\mathrm{Aut}_{\mathbb{R}} D_1$ *a* $\mathrm{Aut}_{\mathbb{R}} D_2$ *jsou izomorfní.*

Důkaz. Plyne z izomorfismu příslušných $\mathbb{R}$-algeber D_1 a D_2. □

Dále bychom mohli zkoumat Weilovu algebru

$$A = \mathbb{D}_2^2/(XY) = \{a + bx + cy + dx^2 + ey^2; a, b, c, d, e \in \mathbb{R}, xy = x^3 = y^3 = 0\}.$$

V tomto případě se nejedná o Drozdovu $\mathbb{R}$-algebru, jelikož není splněna podmínka Drozdova okruhu

$$\exists z \in \mathfrak{n}_A - \mathfrak{n}_A^2 : z^2 = 0.$$

Obecný prvek $z \in \mathfrak{n}_A - \mathfrak{n}_A^2$ je tvaru

$$z = ax + by$$

a jeho mocnina

$$z^2 = (ax + by)^2 = a^2x^2 + 2abxy + b^2y^2 = a^2x^2 + b^2y^2.$$

Aby $z^2 = 0$, muselo by být

$$a = b = 0,$$

čímž ale dostáváme spor, protože

$$z = 0x + 0y \notin \mathfrak{n}_A - \mathfrak{n}_A^2.$$

Další Weilovy algebry, pro které byly napočítány jejich grupy $\mathbb{R}$-algebrových automorfismů, zde neuvádíme, protože se ukázalo, že nejsou Drozdovými $\mathbb{R}$-algebrami. Jsou však k nahlédnutí v příloze.

Věta 4.2.3. *Uvažujme Weilovu algebru* $\mathbb{D}_n^r = \mathbb{R}[X_1, \ldots, X_n]/(X_1, \ldots, X_n)^{r+1}$ *a* $\mathfrak{n}$ *její nilpotentní ideál. Potom Weilova algebra* $\mathbb{D}_n^r/\mathfrak{i}$, *kde* $\mathfrak{i}$ *je ideál* $\mathbb{D}_n^r$ *takový, že* $\mathfrak{i} \subset \mathfrak{n}^2$, *může být Drozdovou* $\mathbb{R}$*-algebrou právě tehdy, když* $r = n = 2$.

Důkaz. Připomeňme si, co znamená podmínka $\mathfrak{i} \subset \mathfrak{n}^2$. Jedná se o ideál, jehož prvky jsou polynomy alespoň druhého stupně v neurčitých $X_1, \ldots, X_n$, přičemž tyto polynomy neobsahují absolutní ani lineární členy. Tedy tato podmínka nám nedovolí pomocí ideálu $\mathfrak{i}$ „odeliminovat“ jednu či více neurčitých (viz příklad 4.1.5).

Omezení pro n dokažme sporem, tedy nechť $n \neq 2$. Nejprve vyšetřeme případ $n = 1$. Potom nilpotentní ideál $\mathfrak{n}_1$ Weilovy algebry $\mathbb{D}_1^r$ má strukturu

$$\mathfrak{n}_1 = a_1x + a_2x^2 + \cdots + a_rx^r, \quad \text{kde } a_1, a_2, \ldots, a_r \in \mathbb{R}.$$

Tedy vidíme, že pro libovolnou Weilovu algebru $A = \mathbb{D}_1^r/\mathfrak{i}$ bude $\mu(\mathfrak{n}_A) = 1$, což je spor s definicí Drozdova okruhu, protože neplatí $\mu(\mathfrak{n}_A) = 2$. Obdobně pro $n \geq 3$ bude $\mu(\mathfrak{n}_A) \geq 3$.

Dále dokažme omezující podmínku pro r, tj. maximální stupeň polynomů v uvažované Weilově algebře. Při $r = 1$ bychom obdrželi Weilovu algebru, ve které by byly pouze lineární polynomy, a tedy bychom dostali spor s podmínkou Drozdova okruhu, protože by neplatilo $\mu(\mathfrak{n}_A^2) = 2$. Dále pro $r \geq 3$ bychom dostali opět dostali spor, jelikož by nebylo splněno $\mathfrak{n}_A^3 = \mathfrak{o}$. □

Tedy Weilova algebra $\mathbb{D}_n^r/\mathfrak{i}$ může být Drozdovou $\mathbb{R}$-algebrou pouze pro $r = n = 2$, přičemž $\mathfrak{i} \subseteq (X, Y)^2$. Toto odpovídá dvěma výše uvedeným Drozdovým $\mathbb{R}$-algebrám D_1, resp. D_2, které jsme získali faktorizací Weilovy algebry $\mathbb{D}_n^r$ ideálem $\mathfrak{i} = (X^2)$, resp. $\mathfrak{i} = (Y^2)$.

5. Lieovy grupy

5.1. Úvod do Lieových grup

V této kapitole si uvedeme základy teorie Lieových grup a ukážeme si jejich základní příklady. Začneme obecnějším pojmem, pomocí kterého potom budeme Lieovu grupu definovat.

Definice 5.1.1. Množinu G, která je topologickým prostorem a na které je definovaná operace $*$, která splňuje grupové axiomy, nazveme *topologická grupa*. Operace

$$* : G \times G \to G, \quad {}^{-1} : G \to G$$

jsou zde spojitá zobrazení.

Definice 5.1.2. Topologický prostor G nazveme *obloukově souvislý*, jestliže pro každé dva body $A, B \in G$ existuje oblouk takový, že

$$s(\langle 0, 1\rangle) \subset G, \text{ přičemž } s(0) = A \text{ a } s(1) = B.$$

Pak topologickou grupu nazveme *souvislá*, pokud je obloukově souvislá jako topologický prostor.

Pojem topologické grupy můžeme zesílit. Nespokojíme se se strukturou topologického prostoru, ale budeme požadovat strukturu hladké variety (struktura třídy C^∞, která je zobecněním pojmu křivka/plocha v libovolné dimenzi). Přesná definice např. v [8].

Definice 5.1.3. Nechť G je topologická grupa. Pokud je G zároveň hladkou varietou, pak je G *Lieova grupa* (někdy také označovaná jako *spojitá grupa*).

O Lieových grupách mluvíme jako o spojitých transformačních grupách. Tyto grupy mají využití například při řešení diferenciálních rovnic. Aplikace nalézají také v teorii řízení a robotice, jelikož se pomocí Lieových grup dá popisovat kinematika těles (viz např. [2]).

Maticové Lieovy grupu označujeme jako klasické, z nichž jmenujme například:

- $\mathrm{GL}(n, \mathbb{R})$ - obecná lineární grupa, grupa regulárních matic řádu n,
- $\mathrm{SL}(n, \mathbb{R})$ - speciální lineární grupa, grupa matic řádu n s $\det A = 1$,
- $\mathrm{O}(n, \mathbb{R})$ - grupa ortogonálních matic řádu n,
- $\mathrm{SO}(n, \mathbb{R})$ - grupa ortogonálních matic řádu n s $\det A = 1$.

Další příklady Lieových grup např. v [5], [8].

Poznámka. Ortogonální matice je taková matice, pro kterou platí

$$QQ^T = I = Q^T Q,$$

kde I je jednotková matice příslušného řádu. Tedy ortogonální matice je taková matice, že její transpozice je zároveň maticí inverzní. Přepišme matici Q do tvaru $Q = [\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_n]$, kde $\mathbf{q}_i$, $i = 1, \ldots, n$, jsou její sloupce. Potom z rovnosti $Q^T Q = I$ vidíme, že platí

$$\mathbf{q}_j^T \cdot \mathbf{q}_k = \begin{cases} 1 & \text{pro } j = k \\ 0 & \text{pro } j \neq k, \end{cases}$$

kde $\mathbf{q}_j^T \cdot \mathbf{q}_k$ je skalární součin vektorů $\mathbf{q}_j$ a $\mathbf{q}_k$. Tedy sloupce ortogonální matice Q jsou navzájem ortonormální. Z rovnosti $QQ^T = I$ se dá podobně ukázat, že i řádky ortogonální matice Q jsou navzájem ortonormální. Proto se někdy ortogonální matice označuje jako ortonormální.

Ortogonální matice mají determinant roven 1 nebo -1. V případě matic třetího řádu s determinantem rovným 1 se jedná o klasické matice rotace.

Zaměřme se nyní blíže na výše uvedené Lieovy grupy. Nejprve vezměme případ $\mathrm{GL}(n, \mathbb{R})$. Jedná se o nesouvislou grupu, jelikož máme omezení, že determinant matic této grupy nesmí být nulový neboli matice mají být regulární. Konkrétně má tato grupa dvě souvislé komponenty, a to množinu matic s kladným determinantem a množinu matic se záporným determinantem. Dále dimenze této grupy je n^2.

Grupa $\mathrm{SL}(n, \mathbb{R})$ je podgrupou grupy $\mathrm{GL}(n, \mathbb{R})$. Tentokrát se jedná o grupu souvislou, která má dimenzi $n^2 - 1$.

Dále vezměme poslední dvě grupy z výše uvedených. Grupa $\mathrm{O}(n, \mathbb{R})$ má dimenzi $\frac{n(n-1)}{2}$ a jedná se o grupu nesouvislou. Grupa $\mathrm{SO}(n, \mathbb{R})$ je její podgrupou stejné dimenze, avšak jedná se o souvislou grupu. Pro $n = 3$ je $\mathrm{SO}(n, \mathbb{R})$ grupa klasických matic rotace.

5.2. Grupy $\mathbb{R}$-algebrových automorfismů Weilových algeber

Podívejme se nyní, v návaznosti na minulou kapitolu, detailněji na grupu $\mathrm{GL}(n, \mathbb{R})$, když zvolíme konkrétní n. Grupa $\mathrm{GL}(1, \mathbb{R})$ má strukturu

$$\{c, c \in \mathbb{R}, c \neq 0\}.$$

Uvažujme Weilovu algebru

$$A = \mathbb{D}_1^1 = \{a + bx, a, b \in \mathbb{R}, x^2 = 0\}$$

a zkonstruujme pro ni grupu $\mathbb{R}$-algebrových automorfismů. Získáme následující předpis pro $\mathbb{R}$-algebrové automorfismy

$$\begin{aligned} 1 &\mapsto 1 \\ x &\mapsto cx, \ c \in \mathbb{R}, c \neq 0. \end{aligned}$$

Tedy vidíme, že $\mathrm{Aut}_{\mathbb{R}}(A)$ je izomorfní s obecnou lineární grupou $\mathrm{GL}(1, \mathbb{R})$. Dostáváme reálnou osu, ze které je vyjmuta nula.

Podívejme se nyní detailněji na grupu $\mathrm{GL}(n, \mathbb{R})$, když položíme $n = 2$. Ta má strukturu

$$\left\{ \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}, c_i \in \mathbb{R}, i = 1, \ldots, 4, \ c_1 c_4 - c_2 c_3 \neq 0 \right\}.$$

Vezměme Weilovu algebru

$$B = \mathbb{D}_2^1 = \{a + bx + cy, a, b, c \in \mathbb{R}, x^2 = xy = y^2 = 0\}$$

a opět pro ni zkonstruujme grupu $\mathbb{R}$-algebrových automorfismů. Dostaneme následující předpis automorfismů

$$\begin{aligned} 1 &\mapsto 1 \\ x &\mapsto c_1 x + c_2 y \\ y &\mapsto c_3 x + c_4 y \ c_1, c_2, c_3, c_4 \in \mathbb{R}, c_1 c_4 - c_2 c_3 \neq 0. \end{aligned}$$

Je vidět, že stejně jako u grupy $\mathrm{GL}(2, \mathbb{R})$ máme čtveřice reálných čísel, na které je kladena stejná podmínka. Neboli grupa $\mathrm{GL}(2, \mathbb{R})$ a grupa $\mathrm{Aut}_{\mathbb{R}}(B)$ jsou izomorfní. Máme tedy čtyřrozměrný prostor, ze kterého vyjímáme trojrozměrnou kvadratickou varietu.

Připomeňme Drozdovu $\mathbb{R}$-algebru

$$D_1 = \mathbb{D}_2^2/(X^2) = \{a + bx + cy + dxy + ey^2; a, b, c, d, e \in \mathbb{R}, x^2 = y^2 x = y^3 = 0\},$$

kterou jsme uvedli v oddílu 4.2 a její grupu $\mathbb{R}$-algebrových automorfismů. $\mathbb{R}$-algebrové automorfismy jsme navrhli takto

$$\begin{aligned} 1 &\mapsto 1, \\ x &\mapsto Ax + By + Cxy + Dy^2, \\ y &\mapsto Ex + Fy + Gxy + Hy^2, \ A, B, C, D, E, F, G, H \in \mathbb{R}. \end{aligned}$$

Odvodili jsme, že $B = 0$, a celkově tak máme

$$\begin{aligned} 1 &\mapsto 1, \\ x &\mapsto Ax + Cxy + Dy^2, \\ y &\mapsto Ex + Fy + Gxy + Hy^2, \ A, C, D, E, F, G, H \in \mathbb{R}, AF \neq 0. \end{aligned}$$

Je vidět, že se zde pohybujeme v sedmirozměrném prostoru. Dále pak omezením pro koeficienty A a F vyjímáme z tohoto prostoru $AF = 0$, tj. šestirozměrnou kvadratickou varietu. Díky podmínky $AF \neq 0$ máme pak $AF > 0$, nebo $AF < 0$. Je zřejmé, že takto se nám grupa rozpadne na dvě komponenty - vezmeme-li kombinaci koeficientů tak, že $AF > 0$, a druhou kombinaci tak, že $AF < 0$, a spojíme tyto dva body obloukem, zákonitě tento oblouk protne vyjmutou varietu $AF = 0$.

6. Závěr

V této práci jsme přiblížili problematiku Drozdových okruhů. Postupovali jsme od základů algebry a postupně jsme vybudovali teoretický základ pro jejich zavedení a další studování. Poté jsme uvedli příklad Drozdova okruhu, pro který jsme provedli důkladný důkaz, že se skutečně jedná o Drozdův okruh. Dále jsme zkoumali, zda je tento okruh algebrou nad nějakým polem, a dokázali jsme, že se nejedná o algebru nad žádným polem. Nicméně jedná se o $\mathbb{Z}$-algebru, jelikož lze vždy zavést okruhový homorfismus ze $\mathbb{Z}$ do libovolného okruhu.

V druhé části jsme se věnovali Weilovým algebrám, což jsou okruhy polynomů v n neurčitých stupně maximálně r. Tyto $\mathbb{R}$-algebry nalézají své uplatnění v diferenciální geometrii. Uvedli jsme některé základní pojmy a tvrzení týkající se těchto $\mathbb{R}$-algeber a dále jsme se zaměřili na speciální Weilovy algebry. Dvěma vhodnými zvoleními parametrů Weilovy algebry jsme dostali dvě Drozdovy $\mathbb{R}$-algebry, pro které jsme ukázali, že jsou izomorfní, přičemž to stejné platí pro jejich grupy $\mathbb{R}$-algebrových automorfismů, které jsme pro ně spočítali. Dále jsme se pokusili najít další příklady Weilových algeber, které by byly Drozdovými $\mathbb{R}$-algebrami, což se ale nepodařilo. V příloze tedy alespoň uvádíme jejich grupy $\mathbb{R}$-algebrových automorfismů, které jsme pro ně spočítali. Zformulovali jsme tak alespoň větu, která uvádí podmínky pro Weilovu algebru, aby se mohlo jednat o Drozdovu $\mathbb{R}$-algebru. Po tomto zevrubném rozboru se zdá, že existuje pouze jediná Drozdova $\mathbb{R}$-algebra (až na izomorfismus). Je to ale pouze domněnka, neměli jsme dostatečný aparát pro to, abychom toto dokázali.

Grupy $\mathbb{R}$-algebrových automorfismů Weilových algeber jsou příklady Lieových grup a proto v poslední kapitole uvádíme základy teorie Lieových grup. Ukazuje se, že námi spočítané grupy $\mathbb{R}$-algebrových automorfismů Weilových algeber jsou nesouvislé Lieovy grupy. Pro speciální Weilovy algebry (např. duální čísla, která jsou v textu uvedena) se ukázalo, že jejich grupy $\mathbb{R}$-algebrových automorfismů jsou izomorfní s obecnou lineární grupou.

Jako možné pokračování této práce bych uvedl podrobnější studium Drozdových okruhů nad konečnými poli. Dále je pro Lieovy grupy možno zkonstruovat jejich příslušné Lieovy algebry, což bylo nad rámec této práce (zavedení Lieovy algebry Lieovy grupy viz např. [5]). Jako poslední směr dalšího pozorování bych označil další zkoumání Drozdových algeber nad jinými poli nulové charakteristiky - zejména potom prozkoumat např. pole komplexních čísel $\mathbb{C}$, zda uvedené závěry pro $\mathbb{R}$ platí i pro tento případ.

Literatura

[1] ATIYAH, Michael F. a Ian G. MACDONALD. *Introduction to Commutative Algebra.* 1. vyd. Reading, Mass: Addison-Wesley Pub. Co, 1969, 128 s. ISBN 0813345448.

[2] KARGER, Adolf a Josef NOVÁK. *Prostorová kinematika a Lieovy grupy.* 1. vyd. Praha: SNTL, 1978, 333 s.

[3] KLINGLER, Lee a Lawrence S. LEVY. Representation Type of Commutative Noetherian Rings (Introduction). Proc. of the Intern. Conf. on alg., mod. and rings, University of Lisbon, Lisbon, Portugal, 2003, *World Scientific*, s 113–151 (2006).

[4] KLINGLER, Lee a Lawrence S. LEVY. Representation Type of Commutative Noetherian Rings I: Local wildness. *Pac. J. Math.* 2001, Vol. 200, No.2, s 345–386.

[5] KUREŠ, Miroslav. *Automorfismy Weilových algeber z pohledu teorie Lieových grup.* Seminář z algebry a geometrie, VUT, Brno, Česká republika, 2012, v rukopise.

[6] PERZYNOVÁ, Kateřina. *Hypereliptické křivky a jejich aplikace v kryptografii.* [Diplomová práce] Brno: VUT, FSI, 2010, 67 s.

[7] SKULA, Ladislav. *Obecná algebra.* (přednášky) Brno: VUT, FSI, zimní semestr akademického roku 2010/2011.

[8] *Wolfram MathWorld* [online]. [cit. 2013-05-15]. Dostupné z: http://mathworld.wolfram.com/

7. Seznam použitých zkratek a symbolů

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$	přirozená, celá, racionální a reálná čísla
G, H	grupy
R, S	okruhy
K, L	pole
$R[X_1, \ldots, X_n]$	okruh polynomů v neurčitých $X_1, \ldots, X_n$ s koeficienty z R
ACC	podmínka rostoucích řetězců
DCC	podmínka klesajících řetězců
$\mathfrak{i}, \mathfrak{j}$	ideály
$\mathfrak{m}$	maximální ideál
$\mu(\mathfrak{m})$	minimální počet prvků potřebných k vygenerování $\mathfrak{m}$
$\varphi : R \to S$	okruhový homomorfismus z okruhu R do okruhu S
$\mathrm{Ker}(\varphi)$	jádro okruhového homomorfismu φ
$\mathrm{Im}(\varphi)$	obraz okruhového homomorfismu φ
$Z(R)$	centrum okruhu R
$\mathbb{D}_n^r$	okruh polynomů v neurčitých $X_1, \ldots, X_n$ maximálního stupně r s koeficienty z $\mathbb{R}$
$\mathfrak{n}$	nilpotentní ideál $\mathbb{R}$-algebry $\mathbb{D}_n^r$
$\mathrm{Aut}_{\mathbb{R}} A$	grupa $\mathbb{R}$-algebrových automorfismů Weilovy algebry A
$\mathfrak{n}_A$	nilpotentní ideál Weilovy algebry A

8. Přílohy

8.1. Zobecnění Weilových algeber

V části 4.1 jsme zavedli Weilovy algebry a naznačili jsme jejich zobecnění, kdy je uvažujeme nad jinými poli než $\mathbb{R}$, např. nad poli konečnými $\mathbb{F}_{q^m}$, kde q je prvočíslo a $m \in \mathbb{N}$.

Příklad 8.1.1. Zvolíme nyní $r = 1$, $n = 1$, $q = 2$ a $m = 1$ a dostaneme tak $\mathbb{F}_2$-algebru

$$(\mathbb{D}_{\mathbb{F}_2})_1^1 = \mathbb{F}_2[X]/(X)^2 = \{a + bx, a, b \in \mathbb{F}_2, x^2 = 0\},$$

jejíž prvky jsou

$$0, 1, x \text{ a } 1 + x.$$

Nyní uvedeme pro tuto $\mathbb{F}_2$-algebru tabulky pro operace sčítání a násobení.

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	x
$1+x$	0	$1+x$	x	1

$\mathbb{F}_2$-algebrové automorfismy popíšeme následovně

$$\begin{aligned} 1 &\mapsto 1, \\ x &\mapsto Ax, \ A \in \mathbb{F}_2. \end{aligned}$$

Z podmínky invertibility dostaneme $A \neq 0 \Rightarrow A = 1$. Tedy grupa $\mathbb{F}_2$-algebrových automorfismů této $\mathbb{F}_2$-algebry má jediný prvek a to identický automorfismus.

Příklad 8.1.2. Obměňme náš příklad nyní v tom smyslu, že položíme $n = 2$. Dostaneme tak $\mathbb{F}_2$-algebru

$$(\mathbb{D}_{\mathbb{F}_2})_2^1 = \mathbb{F}_2[X, Y]/(X, Y)^2 = \{a + bx + cx, a, b, c \in \mathbb{F}_2, x^2 = xy = y^2 = 0\},$$

jejíž prvky jsou

$$0, 1, x, y, 1 + x, 1 + y, x + y \text{ a } 1 + x + y.$$

$\mathbb{F}_2$-algebrové automorfismy popíšeme následovně

$$\begin{aligned} 1 &\mapsto 1, \\ x &\mapsto Ax + By, \\ y &\mapsto Cx + Dy, \ A, B, C, D \in \mathbb{F}_2. \end{aligned}$$

Z podmínky invertibility dostáváme omezení

$$AD - BC \neq 0.$$

Obdržíme tak následující možnosti kombinace koeficientů A až D:

$$\begin{aligned}
&A = D = 0, B = C = 1;\\
&A = 1, D = 0, B = C = 1;\\
&A = 0, D = 1, B = C = 1;\\
&A = D = 1, B = C = 0;\\
&A = D = 1, B = 1, C = 0;\\
&A = D = 1, B = 0, C = 1.
\end{aligned}$$

Tedy vidíme, že grupa $\mathbb{F}_2$-algebrových automorfismů $\mathbb{F}_2$-algebry $(\mathbb{D}_{\mathbb{F}_2})_2^1$ má šest prvků.

8.2. Grupy $\mathbb{R}$-algebrových automorfismů Weilových algeber

V oddílu 4.2 jsme počítali grupy $\mathbb{R}$-algebrových automorfismů vybraných Weilových algeber, které byly zároveň Drozdovy $\mathbb{R}$-algebry. Zde uvedeme grupy $\mathbb{R}$-algebrových automorfismů těch Weilových algeber, u kterých se ukázalo, že Drozdovými algebrami nejsou. Začneme příkladem, který jsme uvedli v kapitole 4 a to Weilovou algebrou pro $n = r = 2$ a $\mathfrak{i} = (XY)$.

Příklad 8.2.1.

$$W_1 = \mathbb{D}_2^2/(XY) = \{a + bx + cy + dx^2 + ey^2; a, b, c, d, e \in \mathbb{R}, xy = x^3 = y^3 = 0\}.$$

$\mathbb{R}$-algebrové automorfismy popíšeme následovně

$$\begin{aligned}
1 &\mapsto 1,\\
x &\mapsto Ax + By + Cx^2 + Dy^2,\\
y &\mapsto Ex + Fy + Gx^2 + Hy^2,\ A, B, C, D, E, F, G, H \in \mathbb{R}.
\end{aligned}$$

Z podmínky $xy = 0$ dostáváme

$$0 = xy = (Ax+By+Cx^2+Dy^2)(Ex+Fy+Gx^2+Hy^2) = AEx^2+BFy^2 \Rightarrow AE = BF = 0.$$

Grupa musí obsahovat svůj neutrální prvek, tj. identický $\mathbb{R}$-algebrový automorfismus ($A = 1$, $F = 1$ a všechny ostatní koeficienty rovny nule) - nicméně může obsahovat komponentu, která tento neutrální prvek neobsahuje. Ke splnění podmínky

$$AE = BF = 0$$

máme dvě možnosti - nejprve položíme $A = F = 0$ a dostaneme tak

$$\begin{aligned}
1 &\mapsto 1,\\
x &\mapsto By + Cx^2 + Dy^2,\\
y &\mapsto Ex + Gx^2 + Hy^2,\ A, C, D, F, G, H \in \mathbb{R}, BE \neq 0.
\end{aligned}$$

Dále nám zbývá možnost $B = E = 0$, díky které obdržíme další komponenty grupy $\mathbb{R}$-algebrových automorfismů Weilovy algebry W_1:

$$\begin{aligned} 1 &\mapsto 1, \\ x &\mapsto Ax + Cx^2 + Dy^2, \\ y &\mapsto Fy + Gx^2 + Hy^2,\ A, C, D, F, G, H \in \mathbb{R}, AF \neq 0. \end{aligned}$$

Vidíme, že se jedná o nesouvislou grupu.

Příklad 8.2.2. Uvažujme nyní Weilovu algebru

$$W_2 = \mathbb{D}_2^2/(X^2 + Y^2) = \{a + bx + cy + dx^2 + exy; a, b, c, d, e \in \mathbb{R}, x^2 + y^2 = 0\}.$$

$\mathbb{R}$-algebrové automorfismy popíšeme následovně

$$\begin{aligned} 1 &\mapsto 1, \\ x &\mapsto Ax + By + Cx^2 + Dxy, \\ y &\mapsto Ex + Fy + Gx^2 + Hxy,\ A, B, C, D, E, F, G, H \in \mathbb{R}. \end{aligned}$$

Dále spočítáme

$$\begin{aligned} x^2 &= A^2x^2 + 2ABxy + By^2 = (A^2 - B^2)x^2 + 2ABxy, \\ y^2 &= E^2x^2 + 2EFxy + Fy^2 = (E^2 - F^2)x^2 + 2EFxy \end{aligned}$$

a z podmínky $x^2 = -y^2$ dostaneme

$$(A^2 - B^2)x^2 + 2ABxy = -(E^2 - F^2)x^2 - 2EFxy.$$

Tedy dostáváme rovnice

$$\begin{aligned} A^2 - B^2 &= -E^2 + F^2, \\ AB &= -EF, \end{aligned}$$

přičemž stějně jako minule musíme respektovat, že grupa musí obsahovat svůj neutrální prvek. Dostáváme tak následující podmínku pro koeficienty A, B, E a F

$$|A| = |F| \text{ a pro splnění druhé rovnice položíme } E = -B\frac{A}{F}.$$

Tedy vidíme, že popis obrazů generátorů se rozpadá na dvě možnosti. Začneme alternativou $F = A$, čímž dojdeme k následujícímu předpisu

$$\begin{aligned} 1 &\mapsto 1, \\ x &\mapsto Ax + By + Cx^2 + Dxy, \\ y &\mapsto -Bx + Ay + Gx^2 + Hxy,\ A, B, C, D, G, H \in \mathbb{R}, A \neq 0. \end{aligned}$$

Nyní vezmeme druhou možnost, $F = -A$, a obdržíme tak

$$\begin{aligned} 1 &\mapsto 1, \\ x &\mapsto Ax + By + Cx^2 + Dxy, \\ y &\mapsto Bx - Ay + Gx^2 + Hxy,\ A, B, C, D, G, H \in \mathbb{R}, \end{aligned}$$

přičemž nesmí nastat

$$A = B = 0.$$

Vidíme, že už se jedná o složitější grupu, o které můžeme říct, že je nesouvislá.

Příklad 8.2.3. Vezměme nyní případ Weilovy algebry

$$W_3 = \mathbb{D}_2^2/(X^2 + XY) = \{a + bx + cy + dx^2 + ey^2; a, b, c, d, e \in \mathbb{R}, x^2 + xy = 0\}.$$

$\mathbb{R}$-algebrové automorfismy popíšeme stejně jako u předchozích případů a spočítáme

$$\begin{aligned} x^2 &= A^2x^2 + 2ABxy + By^2 = (A^2 - 2AB)x^2 + B^2y^2, \\ xy &= AEx^2 + (AF + BE)xy + BFy^2 = (AE - AF - BE)x^2 + BFy^2 \end{aligned}$$

a z podmínky $x^2 = -xy$ dostaneme

$$(A^2 - 2AB)x^2 + B^2y^2 = -(AE - AF - BE)x^2 - BFy^2.$$

Máme tedy následující rovnice

$$\begin{aligned} A^2 - 2AB &= -AE + AF + BE, \\ B^2 &= -BF. \end{aligned}$$

Máme teď dvě možnosti, jak pokračovat:

1) Vezměme nejprve možnost $B = -F$. Takto dostaneme rovnici

$$A^2 + 2AF = -AE + AF - EF.$$

Po úpravě máme

$$A(A + F) = -E(A + F) \Rightarrow E = -A,$$

čímž dostaneme spor, protože

$$AF - BE = AF - (-F)(-A) = AF - FA = 0,$$

což je rozpor s podmínkou invertibility zobrazení (musí platit $AF - BE \neq 0$).

2) Vezměme tedy případ $B = 0$. Tímto dostaneme rovnici

$$A^2 = -AE + AF$$

a protože $A \neq 0$, můžeme psát

$$A = -E + F \Rightarrow E = F - A.$$

Celkově tak pro předpis $\mathbb{R}$-algebrových automorfismů Weilovy algebry W_3 platí

$$\begin{aligned} 1 &\mapsto 1, \\ x &\mapsto Ax + Cx^2 + Dy^2, \\ y &\mapsto (F - A)x + Fy + Gx^2 + Hy^2,\ A, C, D, F, G, H \in \mathbb{R}, AF \neq 0. \end{aligned}$$

Jedná se o sedmirozměrný prostor. Omezením na koeficienty A a F vyjímáme z tohoto prostoru kvadratickou varietu $AF = 0$, tedy jedná se o grupu nesouvislou.