UNIVERZA V LJUBLJANI,
FAKULTETA ZA MATEMATIKO IN FIZIKO

Jaka Cimprič

UREDITVE VIŠJEGA EKSPONENTA NA NEKOMUTATIVNIH KOLOBARJIH

Disertacija

Ljubljana, 1998

Zahvala

Zahvaljujem se svojemu mentorju Matjažu Omladiču in vsem drugim, ki so mi pomagali.

Jaka Cimprič.

Povzetek

Prvo in drugo poglavje obravnavata teorijo predureditev na polgrupah. V tretjem poglavju posplošimo Beckerjevo verzijo Kadison-Duboisove reprezentacije na asociativne kololobarje. V četrtem poglavju konstruiramo ureditve vseh sodih eksponentov na kolobarju kvantnih polinomov in na domeni Malceva. V petem poglavju dokažemo presečni izrek za ureditve eksponenta $n = 2^k$ na poljubnih domenah in presečni izrek za ureditve poljubnega eksponenta na Orejevih domenah. Obenem poenostavimo dokaz presečnega izreka za nekomutativne obsege. V šestem poglavju dokažemo, da abstraktni Positivstellensatz in Nullstellensatz za ureditve višjega eksponenta na asociativnih kolobarjih sledita iz presečnega izreka za domene. Odtod sledi, da izreka veljata za ureditve eksponenta $n = 2^k$ na poljubnih kolobarjih in za ureditve poljubnega eksponenta na Noetherskih kolobarjih. V sedmem poglavju ponovimo osnove teorije spektralnih prostorov in v osmem poglavju obravnavamo različne spektralne prostore, ki nastopajo v teoriji ureditev višjega eksponenta. Deveto poglavje obravnava abstraktno teorijo form višjega reda. Ponovimo dualnost med prostori signatur in reduciranimi prostori form in konstruiramo Postovo ovojnico prostora signatur.

MSC (1991) : 06Fxx, 14Pxx, 16Dxx, 16Wxx.

Summary

Chapters 1 and 2 are concerned with the theory of preorderings on semigroups. In chapter 3, we extend the Becker's version of the Kadison-Dubois representation theorem to asociative rings. In chapter 4, we construct orderings of all even exponents on the ring of quantum polinomials and on the Malcev domain. In chapter 5, we prove the intersection theorem for orderings of exponent $n = 2^k$ on arbitrary domains and the intersection theorem for orderings of arbitrary even exponents on Ore domains. At the same time we simplify the existing proof of the intersection theorem for skew fields. In chapter 6, we reduce the abstract Nullstellensatz and Positivstellensatz for orderings of higher exponent to the general intersection theorem for domains. Thus, we prove both theorems for orderings of exponent $n = 2^k$ on arbitrary rings and for orderings of arbitrary exponents on Noetherian rings. Chapter 7 recalls the basics of the thory of spectral speces and chapter 8 presents various constructions of the spectral spaces in the theory of orderings of higher eksponent. Chapter 9 deals with the abstract theory of higher level forms. We recall the duality between spaces of signatures and reduced form schemes and construct the Post hull of a space of signatures.

MSC (1991) : 06Fxx, 14Pxx, 16Dxx, 16Wxx

Predgovor

Eden od osnovnih rezultatov Artin-Schreierjeve teorije urejenih komutativnih obsegov [15] je t.i. presečni izrek: Vsaka predureditev je enaka preseku vseh ureditev, ki jo vsebujejo. Na tem rezultatu temelji Artinova rešitev sedemnajstega Hilbertovega problema in Prestelov dokaz realnega Nullstellensatza Duboisa in Rislerja (glej tretji razdelek tretjega poglavja v [27]). V tem dokazu nastopa Positivstellensatz kot pomožna lema. Za pospložitve Positivstellensatza in Nullstellensatza na komutativne kolobarje glej [28].

Presečni izrek za splošne (= ne nujno komutativne) obsege je dokazal T. Szele, glej [21], za celostne domene pa R. E. Johnson, glej [22]. Nullstellensatz in Positivstellensatz za nekomutativne kolobarje pa so dokazali šele lete 1997 K. H. Leung, M. Marshall in Y. Zhang, glej [32].

Teorija ureditev višjega eksponenta na komutativnih obsegih pripada E. Beckerju, glej [16] za primer, ko je eksponent potenca števila 2 in [17, 18, 19] za splošen primer. Dokaz presečnega izreka za ureditve višjega eksponenta sloni na Kadison-Duboisovi reprezentaciji arhimedskih delno urejenih kolobarjev, glej [12].

Beckerjeve rezultate so uporabili M. D. Choi, T. Y. Lam, A. Prestel in B. Reznick pri posplošitvi sedemnajstega Hilbertovega problema na $2n$-te potence, glej [26]. Nullstellensatz in Positivstellenzatz za ureditve višjega eksponenta na komutativnih kolobarjih sta najprej dokazala E. Becker in D. Gondard za primer, ko je eksponent potenca števila 2, glej [29]. Dokaz za splošen eksponent pripada R. Berru, glej [30] in [31]. V svoji habilitacijski nalogi je R. Berr uporabil teorijo ureditev višjega eksponenta na komutativnih kolobarjih pri klasifikaciji singularnosti realnih semialgebraičnih funkcij, glej [40].

Ureditve višjega eksponenta na splošnih obsegih sta študirala T. Craven v [23] in V. Powers v [24] in dokazala ustrezni presečni izrek. Ureditve višjega eksponenta na nekomutativnih kolobarjih je začela študirati V. Powers v [33]. Primera kolobarjev, ki dopuščata ureditve višjega reda sta Weylova algebra in kolobar kvantnih polinomov. Oba kolobarja sta Orejevi domeni in vsaka njuna ureditev višjega eksponenta se enolično razširi na obseg ulomkov.

Kazalo

1.

Predureditve na polgrupah

V tem razdelku bomo razvili Artin-Schreierjevo teorijo za polgrupe. Poudarek je na dokazu posledice 16, ki jo bomo uporabili pri dokazu presečnega izreka za obsege v petem poglavju.

1.1 Zaprtje in permutacijska lastnost

Naj bo S polgrupa in n poljubno naravno število. Naj bo S_n množica vseh produktov n-tih potenc elementov polgrupe S. Označimo s $\Pi_n(S)$ množico vseh elementov polgrupe S, ki se dajo izraziti kot produkt končnega zaporedja elementov iz S v katerem vsak element nastopa z večkratnostjo deljivo z n. Očitno je $S_n \subseteq \Pi_n(S)$. Če je naravno število m večkratnik števila n, potem velja $S_m \subseteq S_n$ in $\Pi_m(S) \subseteq \Pi_n(S)$. Velja tudi $S_1 = \Pi_1(S) = S$.

Podmnožica T polgrupe S je *predureditev*, če je $T \cdot T \subseteq T$ in obstaja tako naravno število n, da velja $\Pi_n(S) \subseteq T$. Število n se imenuje *eksponent* predureditve T in ni enolično določeno. Vsak večkratnik vsakega eksponenta je tudi eksponent. Najmanjši eksponent predureditve T imenujemo *strogi eksponent* predureditve T.

Za pomemben razred predureditev se bo izkazalo, da je vsak njihov eksponent večkratnik strogega eksponenta. Če multiplikativna množica T' vsebuje predureditev T, potem je tudi T' predureditev in vsak eksponent predureditve T je tudi eksponent predureditve T'. Očitno je množica $\Pi_n(S)$ predureditev z eksponentom n. Načeloma se lahko zgodi, da n ni njen strogi eksponent.

Lema 1 *Naj bo T poljubna predureditev na polgrupi S. Za poljuben element $s \in S$ velja $sT \cap T \neq \emptyset$ natanko tedaj, ko je $Ts \cap T \neq \emptyset$.*

Dokaz : Naj bo n poljuben eksponent predureditve T. Če velja $sT \cap T \neq \emptyset$, potem obstaja tak element $u \in T$, da velja $su \in T$. Če definiramo $v = (su)^{n-1}u$, potem velja $v \in T$ in $vs = (su)^{n-1}us \in \Pi_n(S) \subseteq T$. Torej je res $Ts \cap T \neq \emptyset$. Dokaz v drugo smer je simetričen. Q.E.D.

Vsaki predureditvi T na polgrupi S priredimo njeno *zaprtje*

$$\overline{T} := \{s \in S;\ sT \cap T \neq \emptyset\} = \{s \in S;\ Ts \cap T \neq \emptyset\}.$$

Očitno je vsaka predureditev vsebovana v svojem zaprtju. Predureditev T je *zaprta*, če velja $T = \overline{T}$.

Izrek 2 *Zaprtje poljubne predureditve je zaprta predureditev.*

Dokaz : Naj bo T poljubna predureditev na polgrupi S. Zadošča, če pokažemo, da je $\overline{T} \cdot \overline{T} \subset \overline{T}$ in $\overline{(\overline{T})} = \overline{T}$.

Naj bosta $x, y \in \overline{T}$ poljubna elementa. Potem obstajata taka elementa $u, v \in T$, da velja $ux \in T$ in $yv \in T$. Odtod sledi $u(xyv) = ux \cdot yv \in T$. Po lemi 1 obstaja tak element $v' \in T$, da velja $(xyv)v' \in T$. Ker je $vv' \in T$, velja $xy \in \overline{T}$.

Naj bo $x \in \overline{(\overline{T})}$ poljuben element. Potem obstaja tak element $u \in \overline{T}$, da velja $xu \in \overline{T}$. Vzemimo tak element $v \in T$, da velja $(xu)v \in T$. Po prejšnjem odstavku je $uv \in \overline{T} \cdot T \subseteq \overline{T}$, zato obstaja tak element $w \in T$, da velja $(uv)w \in T$. Ker velja tudi $x((uv)w) = ((xu)v)w \in T \cdot T \subseteq T$, velja $x \in \overline{T}$ po definiciji zaprtja. Q.E.D.

Pravimo, da ima podmnožica M polgrupe S *permutacijsko lastnost*, če za poljubno naravno število k, poljubne elemente $s_1, \ldots, s_k \in S$ in poljubno permutacijo π množice $\{1, \ldots, k\}$ velja

$$s_1 s_2 \cdots s_k \in M \iff s_{\pi(1)} s_{\pi(2)} \cdots s_{\pi(k)} \in M.$$

Očitno ima vsaka podmnožica vsake komutativne polgrupe permutacijsko lastnost. Zanimivo je, da lahko obstajajo množice s permutacijsko lastnostjo tudi na nekomutativnih polgrupah.

Izrek 3 *Vsaka zaprta predureditev ima permutacijsko lastnost.*

Dokaz : Naj bo T poljubna zaprta predureditev na polgrupi S in naj bo n njen poljuben eksponent. Naj bo k pojubno naravno število, $s_1, \ldots, s_k \in S$ poljubni elementi in π poljubna permutacija množice $\{1, \ldots, k\}$. Definirajmo $x = s_1 \cdots s_k$ in $y = s_{\pi(1)} \cdots s_{\pi(k)}$. Ker je T predureditev velja $y^{n-1}x \in \Pi_n(S) \subseteq T$. Če je $x \in T$, potem velja $y(y^{n-1}x) = y^n x \in \Pi_n(S) \cdot T \subseteq T$. Ker je predureditev T zaprta, sledi $y \in T$. Q.E.D.

Lema 4 *Naj bo T zaprta predureditev na polgrupi S. Naj bo n tako naravno število, da za vsak element $s \in S$ velja $s^n \in T$. Potem je n eksponent predureditve T.*

Dokaz : Ker predureditev T vsebuje množico S_n in ker ima po izreku 3 permutacijsko lastnost, vsebuje tudi $\Pi_n(S)$. Q.E.D.

1.2 Kongruenčna relacija zaprte predureditve

Pokazali bomo, da vsaka zaprta predureditev T na polgrupi S določa tako kongruenčno relacijo $\sim_T$ na polgrupi S, da je faktorska polgrupa $S/\sim_T$ kar Abelova grupa.

Lema 5 *Naj bo T zaprta predureditev na polgrupi S in naj bo n poljuben njen eksponent. Potem so naslednje trditve ekvivalentne:*

1. $xT \cap Ty \neq \emptyset$,
2. $Tx \cap yT \neq \emptyset$,
3. $TxT \cap TyT \neq \emptyset$,
4. $xy^{n-1} \in T$,
5. $yx^{n-1} \in T$.

Dokaz : Zadošča, če dokažemo ekvivalenčna kroga 1. $\Rightarrow$ 3. $\Rightarrow$ 4. $\Rightarrow$ 1. in 2. $\Rightarrow$ 3. $\Rightarrow$ 5. $\Rightarrow$ 2. Netrivialni del prvega kroga je 3. $\Rightarrow$ 4. in drugi krog sledi iz prvega zaradi simetrije.

Če je $TxT \cap TyT \neq \emptyset$, potem obstajajo taki elementi $s_1, t_1, s_2, t_2 \in T$, da velja $s_1 x t_1 = s_2 y t_2$. Sledi $(s_1 x t_1)(s_2 y t_2)^{n-1} = (s_2 y t_2)^n \in T$. Po izreku 3 sledi $s_1 t_1 s_2^{n-1} t_2^{n-1} x y^{n-1} \in T$. Ker je predureditev T zaprta in ker $s_1 t_1 s_2^{n-1} t_2^{n-1} \in T$, sledi $xy^{n-1} \in T$. Q.E.D.

Vsaki zaprti predureditvi T na polgrupi S priredimo relacijo $\sim_T$ s predpisom

$$x \sim_T y \iff TxT \cap TyT \neq \emptyset.$$

Izrek 6 *Naj bo T zaprta predureditev eksponenta n na polgrupi S.*

1. *Relacija $\sim_T$ je kongruenca. Množica T je kongruenčni razred.*
2. *Faktorska polgrupa $G_T := S/\sim_T$ je Abelova grupa. Njen nevtralni element je množica T, inverz pa je induciran s preslikavo $x \to x^{n-1}$.*

Dokaz : Refleksivnost in simetričnost relacije $\sim_T$ sta očitni. Dokazujemo tranzitivnost. Vzemimo poljubne elemente $x, y, z \in S$, ki zadoščajo $x \sim_T y$ in $y \sim_T z$. Po lemi 5 je $xy^{n-1} \in T$ in $yz^{n-1} \in T$. Ker je množica T predureditev, je $xy^n z^{n-1} \in T$. Izrek 3 nam da $(xz^{n-1})y^n \in T$. Ker je predureditev T zaprta, sledi $xz^{n-1} \in T$, torej $x \sim_T z$ po lemi 5.

Dokažimo, da je relacija $\sim_T$ kompatibilna z množenjem. Naj bodo $x, y, u, v \in S$ taki elementi, da velja $x \sim_T u$ in $y \sim_T v$. Po lemi 5 imamo $xu^{n-1} \in T$ in $yv^{n-1} \in T$. ker je $xu^{n-1}yv^{n-1} \in T$, sledi $xy(uv)^{n-1} \in T$ po izreku 3. Lema 5 nam da želeno relacijo $xy \sim_T uv$.

Dokažimo, da je množica T kongruenčni razred. Za poljubna elementa $s, t \in T$ velja $st^{n-1} \in T$, torej je $s \sim_T t$ po lemi 5. Če je $x \sim_T t$ za nek element $x \in S$ in element $t \in T$, potem je $xt^{n-1} \in T$ po lemi 5. Ker je predureditev T zaprta, sledi $x \in T$.

Za poljubna elementa $x, y \in S$ velja $xy(yx)^{n-1} \in \Pi_n(S) \subseteq T$. Po lemi 5 odtod sledi $xy \sim_T yx$. Torej je faktorska polgrupa komutativna. Očitno je množica T njen nevtralni element.

Definirajmo preslikavo $i(x) = x^{n-1}$. Ker je relacija $\sim_T$ kongruenčna, iz $x \sim_T y$ sledi $i(x) \sim_T i(y)$. Ker je predureditev T eksponenta n, ima preslikava, ki jo i porodi na G_T vse lastnosti inverza. Torej je polgrupa G_T grupa. Q.E.D.

1.3 Lastnosti predureditve T : lastnosti grupe G_T

Naj po T predureditev na polgrupi S in $s \in S$ poljuben element. Naravno število m, ki zadošča $s^m \in T$ imenujemo *red elementa s glede na predureditev T*. Najmanjši red elementa s glede na predureditev T označimo z $\mathrm{ord}_T(s)$ in ga imenujemo *strogi red elementa s glede na T*. Če je predureditev T zaprta, označimo s $\pi_T : S \to G_T$ kanonično projekcijo polgrupe S na njeno faktorsko polgrupo $G_T = S/\sim_T$.

Izrek 7 *Naj bo T zaprta predureditev na polgrupi S in $x \in S$ poljuben element.*

1. *Za poljubno naravno število k velja $x^k \in T$ tedaj in le tedaj, ko je $\pi_T(x)^k = T$.*

   Strogi eksponent $\mathrm{ord}_T(x)$ *se ujema z redom elementa $\pi_T(x)$ v polgrupi G_T.*

   Vsak red elementa x glede na T je večkratnik strogega reda $\mathrm{ord}_T(x)$.

2. *Predureditev T ima eksponent n natanko tedaj, ko je Abelova grupa G_T n-torzijska.*

   Strogi eksponent predureditve T se ujema z eksponentom Abelove grupe G_T.

   Vsak eksponent predureditve T je večkratnik strogega eksponenta.

Dokaz : Prva trditev je posledica lastnosti reda elementa v grupi. Druga trditev je posledica prve in leme 4. Q.E.D.

Lema 8 *Vsaka Abelova grupa končnega eksponenta m vsebuje ciklično podgrupo reda m.*

Dokaz : Naj bo G Abelova grupa s končnim eksponentom m. Naj bo $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ njegov praštevilski razcep. Po Prüfer-Baerovem izreku (glej [3], Corollary 10.37) je G izomorfna direktnemu produktu cikličnih grup. Ker je eksponent grupe G enak m, morajo v tem razcepu nastopati ciklične grupe redov $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_r^{\alpha_r}$. Njihov produkt je ciklična podgrupa reda m. Q.E.D.

Posledica 9 *Naj bo T zaprta predureditev na polgrupi S. Obstaja tak element $z \in S$, da se* $\mathrm{ord}_T(z)$ *ujema s strogim eksponentom predureditve T.*

Izrek 10 *Naj bo T dana zaprta predureditev na polgrupi S. Potem slika in praslika kanonične projekcije $\pi_T : S \to G_T = S/\!\sim_T$ podajata bijektivno korespondenco med podgrupami v G_T in zaprtimi predureditvami na polgrupi S, ki vsebujejo predureditev T.*

Dokaz : Če je množica P predureditev na polgrupi S, ki vsebuje predureditev T, potem je njena slika $\pi_T(P)$ multiplikativna podmnožica grupe G. Toda v podgrupi s končnim eksponentom je vsaka multiplikativna množica že kar podgrupa.

Če je H podgrupa grupe G, potem je množica $\pi_T^{-1}(H)$ multiplikativna in vsebuje predureditev T, torej je tudi sama predureditev. Pokažimo še, da se ujema s svojim zaprtjem. Če velja $xu = v$ za poljuben element $x \in S$ in poljubna elementa $u, v \in \pi_T^{-1}(H)$, potem je $\pi_T(x)\pi_T(u) = \pi_T(v)$ in $\pi_T(u), \pi_T(v) \in H$. Ker je H podgrupa, sledi $\pi_T(x) \in H$, torej $x \in \pi_T^{-1}(H)$.

Ker je preslikava π_T surjektivna, velja $\pi_T(\pi_T^{-1}(H)) = H$ za vsako podgrupo H grupe G_T. Očitno je za vsako predureditev P na polgrupi S množica $P' = \pi_T^{-1}(\pi_T(P))$ zaprta predureditev, ki vsebuje predureditev P. Za poljuben element $x \in P'$ velja $\pi_T(x) = \pi_T(p)$ za nek element $p \in P$. Odtod sledi, $\pi_T(xp^{n-1}) = \pi_T(p^n) = T$, torej je $xp^{n-1} \in T$. Ker je $p^{n-1} \in P$ in $T \subseteq P$, velja $x \in \overline{P}$. Torej je $P' = \overline{P}$. Dokazali smo celo več, kot trdi izrek. Q.E.D.

Izrek 11 *Naj bosta T in P zaprti predureditvi na polgrupi S in naj P vsebuje T. Potem identični endomorfizem polgrupe S inducira izomorfizem grup $G_T/\pi_T(P)$ in G_P.*

Dokaz : Ker predureditev P vsebuje predureditev T, je preslikava $\phi : G_T \to G_P$, kjer za vsak $x \in S$ postavimo $\phi(\pi_T(x)) = \pi_P(x)$, dobro definirana. Izračunajmo njeno jedro. Če je $\pi_P(x) = P$, potem $x \in P$, in zato $\pi_T(x) \in \pi_T(P)$. Trditev sledi iz prvega izreka o izomorfizmu. Q.E.D.

1.4 Ciklične predureditve

Naj bo μ_n grupa vseh kompleksnih n-tih korenov enice. Če je $\phi : S \to \mu_n$ homomorfizem polgrup, potem je množica $\phi^{-1}(1)$ očitno zaprta predureditev na polgrupi S z eksponentom n. Taki predureditvi pravimo *ciklična predureditev*.

Lema 12 *Zaprta predureditev T na polgrupi S je ciklična natanko tedaj, kadar je grupa G_T ciklična.*

Dokaz : Naj bo T ciklična predureditev na polgrupi S eksponenta n in naj bo $\phi : S \to \mu_n$ pripadajoči polgrupni homomorfizem. Ker je $\phi(T) = 1$, inducira ϕ surjektiven homomorfizem grup $\phi' : G_T \to \mu_n$. Ker je $\phi^{-1}(1) = T$, je ϕ' tudi injektiven.

Če je grupa G_T ciklična, potem obstajata naravno število n in izomorfizem $\phi' : G \to \mu_n$. Preslikava $\phi := \phi' \circ \pi_T : S \to \mu_n$ je homomorfizem polgrup z želeno lastnostjo $\phi^{-1}(1) = T$. Q.E.D.

Ciklična predureditev svojega polgrupnega homomorfizma ne določa enolično. Nekaj pa vseeno lahko povemo.

Izrek 13 *Naj bo S polgrupa, n naravno število in $\phi, \psi : S \to \mu_n$ polgrupna homomorfizma.*

Če velja $\phi^{-1}(1) = \psi^{-1}(1)$, potem obstaja tako število l tuje proti n, da velja $\psi = \phi^l$.

Dokaz : Označimo $T := \phi^{-1}(1) = \psi^{-1}(1)$. Očitno je T zaprta predureditev. Naj bosta $\overline{\phi}, \overline{\psi} : G_T \to \mu_n$ inducirana homomorfizma. Po lemi 12 sta $\overline{\phi}$ in $\overline{\psi}$ izomorfizma grup. Torej je preslikava $\overline{\psi} \circ \overline{\phi}^{-1}$ avtomorfizem grupe μ_n. Toda vsak avtomorfizem grupe μ_n je potenciranje s številom tujim proti n. Q.E.D.

Če je T zaprta predureditev na polgrupi S, potem preslikava $\phi \to \phi \circ \pi_T$ podaja bijektivno korespondenco med grupnimi homomorfizmi iz G_T v μ_n in polgrupnimi homomorfizmi iz S v μ_n, ki preslikajp množico T v 1.

Lema 14 *Naj bo G poljubna Abelova grupa končnega eksponenta in $x, y \in G$ poljubna neničelna elementa. Naj bo red elementa x enak r. Potem obstaja tak grupni homomorfizem $\chi : G \to \mathbb{C}^\times$, da velja $\chi(x) = e^{2\pi i/r}$ in $\chi(y) \neq 1$.*

Dokaz : Naj bo B podgrupa generirana z elementoma x in y. Grupa B je končna Abelova, zato jo lahko razcepimo na ciklične podgrupe. Odtod se hitro vidi, da obstaja tak homomorfizem grup $\phi : B \to \mathbb{C}^\times$, da velja $\phi(x) = e^{2\pi i/r}$ in $\phi(y) \neq 1$. Ker je grupa $\mathbb{C}^\times$ deljiva, lahko ϕ razširimo do homomorfizma $\chi : G \to \mathbb{C}^\times$ (glej [3], Theorem 10.23), ki ima želene lastnosti. Q.E.D.

Izrek 15 *Naj bo T zaprta predureditev na polgrupi S s strogim eksponentom n in naj bo $\epsilon \in S \setminus T$ poljuben element. Potem obstaja tak surjektiven polgrupni homomorfizem $\phi : S \to \mu_n$, da velja $\phi(T) = 1$ in $\chi(\epsilon) \neq 1$.*

Dokaz : Po posledici 9 obstaja tak element $z \in S$, da velja $\mathrm{ord}_T(z) = n$. Če uporabimo lemo 14 z $x = \pi_T(z)$ in $y = \pi_T(\epsilon)$, dobimo tak homomorfizem grup $\chi : S \to \mathbb{C}^\times$, da velja $\chi(x) = e^{2\pi i/n}$ in $\chi(y) \neq 1$. Iz prve zveze sledi, da je χ surjektiven. Ker je grupa G_T eksponenta n, je $\chi(G_T) \subseteq \mu_n$. Preslikava $\phi := \chi \circ \pi_T$ ima želene lastnosti. Q.E.D.

Posledico 16 bomo uporabili v razdelku 5.4. Tam bo S polgrupa neničelnih elementov nekomutativne domene in $\epsilon = -1$.

Posledica 16 *Naj bo T zaprta predureditev na polgrupi S s strogim eksponentom n in naj bo $\epsilon \in S \setminus T$ poljuben element. Potem je $T = \bigcap P$, kjer presek teče po vseh cikličnih predureditvah strogega eksponenta n, ki vsebujejo T in ne vsebujejo ϵ.*

Posledica 17 *Naj bo S poljubna polgrupa in $m \geq 2$ poljubno naravno število. Potem sta naslednji trditvi ekvivalentni:*

1. *Obstaja surjektiven polgrupni homomorfizem $\phi : S \to \mu_m$.*
2. *Velja $\overline{\Pi_m(S)} \neq \overline{\Pi_{m/p}(S)}$ za vsako praštevilo p, ki deli m.*

Dokaz : Očitno druga trditev sledi iz prve. Druga trditev je ekvivalentna s trditvijo, da je m strogi eksponent zaprte predureditve $\overline{\Pi_m(S)}$. Torej posledica sledi iz izreka 15. Q.E.D.

1.5 Mreža zaprtih predureditev

Lema 18 *Naj bo T zaprta predureditev na polgrupi S. Naj bosta T_1 in T_2 poljubni zaprti predureditvi, ki vsebujeta predureditev T. Potem je $\pi_T(T_1 \cap T_2) = \pi_T(T_1) \cap \pi_T(T_2)$.*

Dokaz : Očitno je $\pi_T(T_1 \cap T_2) \subseteq \pi_T(T_1) \cap \pi_T(T_2)$. Vzemimo sedaj poljuben element $z \in \pi_T(T_1) \cap \pi_T(T_2)$. Potem obstajata taka elementa $t_1 \in T_1$ in $t_2 \in T_2$, da velja $z = \pi_T(t_1)$ in $z = \pi_T(t_2)$. Ker je $\pi_T(t_1) = \pi_T(t_2)$, je po lemi 5 $t_1T \cap Tt_2 \neq \emptyset$. Torej obstajata taka elementa $u, v \in T$, da velja $t_1u = vt_2$. Ker je $T \subseteq T_1 \cap T_2$ velja $t_1u \in T_1 \cdot T \subseteq T_1$ in $vt_2 \in T \cdot T_2 \subseteq T_2$. Odtod sledi $t_1u \in T_1 \cap T_2$. Ker je $\pi_T(t_1u) = \pi_T(t_1) = z$, sledi, da $z \in \pi_T(T_1 \cap T_2)$. Q.E.D.

Izrek 19 *Presek končnega števila predureditev je predureditev. Presek končnega števila zaprtih predureditev je zaprta predureditev.*

Dokaz : Naj bo T_1 predureditev eksponenta n_1 in T_2 predureditev eksponenta n_2. Ker je $\Pi_{n_1n_2}(S) \subseteq \Pi_{n_1}(S) \cap \Pi_{n_2}(S) \subseteq T_1 \cap T_2$, je podpolgrupa $T_1 \cap T_2$ predureditev eksponenta n_1n_2.

Če sta predureditvi T_1 in T_2 zaprti, definirajmo zaprto predureditev $T = \overline{\Pi_{n_1n_2}(S)}$. Ker velja $T \subseteq \overline{\Pi_{n_1}(S)} \subseteq T_1$ in $T \subseteq \overline{\Pi_{n_2}(S)} \subseteq T_2$, sledi $T \subseteq T_1 \cap T_2$. Po izreku 10 je $\overline{T_1 \cap T_2} = \pi_T^{-1}(\pi_T(T_1 \cap T_2))$. Po izreku 18 je $\pi_T(T_1 \cap T_2) = \pi_T(T_1) \cap \pi_T(T_2)$. Odtod sledi $\overline{T_1 \cap T_2} = \pi_T^{-1}(\pi_T(T_1) \cap \pi_T(T_2)) = \pi_T^{-1}(\pi_T(T_1)) \cap \pi_T^{-1}(\pi_T(T_2)) = T_1 \cap T_2$. Torej je $T_1 \cap T_2$ zaprta predureditev.

Izrek sledi z indukcijo po številu predureditev. Q.E.D.

Izrek 20 *Naj bosta T_1 in T_2 poljubni zaprti predureditvi na polgrupi S. Najmanjša zaprta predureditev, ki vsebuje T_1 in T_2 obstaja in je enaka*

$$T_1 * T_2 = \{z \in S;\ (T_1 \cap T_2)z(T_1 \cap T_2) \cap (T_1 \cap T_2)T_1T_2(T_1 \cap T_2) \neq \emptyset\}.$$

Dokaz : Naj bo $T = T_1 \cap T_2$. Po izreku 19 je T zaprta predureditev. V grupi G_T ustreza najmanši zaprti predureditvi, ki vsebuje T_1 in T_2 najmanjša podgrupa, ki vsebuje podgrupi $\pi_T(T_1)$ in $\pi_T(T_2)$. Ta podgrupa je $\pi_T(T_1)\pi_T(T_2)$. Iskana predureditev je torej $\pi_T^{-1}(\pi_T(T_1)\pi_T(T_2))$. Element $z \in S$ leži v njej natanko takrat, ko je $\pi_T(z) = \pi_T(t_1)\pi_T(t_2)$ za neka elementa $t_1 \in T_1$ in $t_2 \in T_2$. Po lemi 5 velja to natanko takrat, ko velja $TzT \cap Tt_1t_2T \neq \emptyset$. Q.E.D.

Po izreku 20 je množica vseh zaprtih predureditev, ki vsebujejo zaprto predureditev T mreža za operaciji $\cap$ in $*$, ki je izomorfna mreži podgrup Abelove grupe G_T.

2.

Razširitveni izreki

Splošno znano je, da se da vsaka ureditev na komutativni domeni enolično razširiti na njen obseg ulomkov. Ta rezultat so posplošili v mnoge smeri. Hebisch [6] je našel potrebne in zadostne pogoje, ki zagotavljajo obstoj razširitve dane delne ureditve na polgrupi na dano polgrupo desnih ulomkov in pokazal, da je ta razširitev enolična. V tem poglavju bomo razvili podobno teorijo za predureditve na polgrupah. Poudarek je na dokazih izrekov 8 in 9, ki jih bomo v razdelku 5.1 uporabili za dokaz presečnega izreka za Orejeve domene.

2.1 Polgrupe desnih ulomkov

Namen tega razdelka je vpeljati pojem polgrupe desnih ulomkov in podati potrebne in zadostne pogoje za njen obstoj.

Naj bo S polgrupa, ki vsebuje podpolgrupo Σ. Množica Q se imenuje *polgrupa desnih ulomkov* polgrupe S glede na Σ, če velja

1. Q je monoid (polgrupa z enico).
2. Polgrupa S je podpolgrupa polgrupe Q.
3. Vsak element iz Σ je obrnljiv v Q.
4. Za vsak element $z \in Q$ obstajata tak element $a \in S$ in tak element $\alpha \in \Sigma$, da velja $z = a\alpha^{-1}$.

Dogovorimo se, da so grške črke rezervirane za elemente podpolgrupe Σ.

Podpolgrupa Σ polgrupe S se imenuje *množica desnih imenovalcev*, če velja

1. V polgrupi S lahko elemente iz Σ krajšamo z leve in z desne.

2. Velja *desni Ore-Asanov pogoj*: Za poljubna elementa $a \in S$ in $\alpha \in \Sigma$ obstajata taka elementa $x \in S$ in $\xi \in \Sigma$, da velja $a\xi = \alpha x$.

Izrek 1 *Naj bo Σ podpolgrupa polgrupe S. Polgrupa desnih ulomkov polgrupe S glede na Σ obstaja natanko tedaj, ko je Σ množica desnih imenovalcev.*

Če je Q polgrupa desnih ulomkov polgrupe S glede na Σ, potem za poljubna elementa $a\alpha^{-1} \in Q$ in $b\beta^{-1} \in Q$ velja

$$a\alpha^{-1} = b\beta^{-1} \Longleftrightarrow \exists x \in S\ \exists \xi \in \Sigma\ :\ \alpha\xi = \beta x \text{ in } a\xi = bx$$

$$\forall s \in S\ \forall \sigma \in \Sigma :\ b\sigma = \alpha s \Rightarrow a\alpha^{-1} \cdot b\beta^{-1} = as(\beta\sigma)^{-1}.$$

Če polgrupa Q obstaja, jo ti dve relaciji enolično določata.

Dokaz je v [5].

Izrek 2 *Naj bo Σ množica desnih imenovalcev v polgrupi Σ. Naj bo Q polgrupa desnih ulomkov polgrupe S po Σ in naj bo U poljuben monoid.*

Potem obstaja naravna bijektivna korespondenca med homomorfizmi iz monoida Q v monoid U in med homomorfizmi iz polgrupe S v monoid U, ki slikajo elemente množica Σ v obrnljive elemente monoida U.

Dokaz : Naj bo $\phi : S \to U$ tak homomorfizem polgrup, ki slika elemente množice Σ v obrnljive elemente monoida U. Za poljubne elemente $a, b \in S$ in $\alpha, \beta \in \Sigma$, ki zadoščajo $a\alpha^{-1} = b\beta^{-1}$ obstajata po izreku 1 taka elementa $x \in S$ in $\xi \in \Sigma$, da velja $\alpha\xi = \beta x$ in $a\xi = bx$. Odtod sledi $\phi(a)\phi(\alpha)^{-1} = \phi(a\xi)\phi(\alpha\xi)^{-1} = \phi(bx)\phi(\beta x) = \phi(b)\phi(\beta)^{-1}$. Odtod sledi, da je s predpisom $\phi'(a\alpha^{-1}) = \phi(a)\phi(\alpha)^{-1}$ dobro definirana preslikava $\phi' : Q \to U$.

Pokažimo sedaj, da je ϕ' homomorfizem polgrup. Naj bosta $a, b \in S$ in $\alpha, \beta \in \Sigma$ poljubna elementa. Zaradi Ore-Asanove lastnosti obstajata taka elementa $c \in S$ in $\gamma \in \Sigma$, da velja $b\gamma = \alpha c$. Torej velja

$$\phi'(a\alpha^{-1} \cdot b\beta^{-1}) = \phi'(ac(\beta\gamma)^{-1}) = \phi(ac)\phi(\beta\gamma)^{-1} =$$

$$= \phi(a)\phi(c)\phi(\gamma)^{-1}\phi(\beta)^{-1} = \phi(a)\phi(\alpha)^{-1}\phi(b)\phi(\beta)^{-1} = \phi'(a\alpha^{-1})\phi'(b\beta^{-1}).$$

Ostale trditve v izreku je preprosto preveriti. Q.E.D.

2.2 Enoličnost razširitve

Naj bo T poljubna predureditev na polgrupi S. Če je Σ poljubna podpolgrupa polgrupe S, potem je množica $T \cap \Sigma$ neprazna, saj vsebuje elemente ξ^n, kjer je $\xi \in \Sigma$ in je n eksponent predureditve T.

Pravimo, da je predureditev T Σ-*zaprta*, če za poljubne elemente $a \in S$ in $\xi, \eta \in \Sigma \cap T$ iz $\xi a \eta \in T$ sledi $a \in T$. To je ekvivalentno z zahtevama, da iz $\xi a \in T$ sledi $a \in T$ in iz $a\eta \in T$ sledi $a \in T$.

Naslednji izrek pove, da je vsaka predureditev na S, ki se da razširiti do predureditve na $Q = Q_r(S, \Sigma)$ Σ-zaprta predureditev. Da nam tudi del eksistenčnega izreka.

Izrek 3 *Naj bo Q polgrupa desnih ulomkov polgrupe S glede na množico desnih imenovalcev Σ in naj bo T predureditev eksponenta n na polgrupi S. Potem sta naslednji trditvi ekvivalentni.*

1. *Predureditev T je Σ-zaprta.*

2. *Množica $T' = T(T \cap \Sigma)^{-1}$ je podpolgrupa polgrupe Q, ki zadošša $T' \cap S = T$ in $(T \cap \Sigma)^{-1} \subseteq T'$.*

3. *Obstaja taka podpolgrupa P polgrupe Q, da velja $P \cap S = T$ in $(T \cap \Sigma)^{-1} \subseteq P$.*

Vsaka predureditev P na polgrupi Q, ki zadošča $P \cap S = T$ ima avtomatično lastnost $(T \cap \Sigma)^{-1} \subseteq P$.

Dokaz : Recimo, da drži točka 3. Vzemimo poljubne elemente $a \in S$ and $\xi, \eta \in T \cap \Sigma$, ki zadoščajo $\xi a \eta \in T$. Ker je P podpolgrupa in ker je $\xi^{-1}, \eta^{-1} \in (T \cap \Sigma)^{-1} \subseteq P$, sledi $a \in \xi^{-1} T \eta^{-1} \subseteq P \cdot P \cdot P \subseteq P$. Ker je $P \cap S = T$, je $a \in T$. Torej drži točka 1.

Privzemimo sedaj, da drži točka 1. in definirajmo $T' = T(T \cap \Sigma)^{-1}$.

Pokažimo najprej, da je $(T \cap \Sigma)^{-1} T \subseteq T(T \cap \Sigma)^{-1}$. Vzemimo poljubna elementa $\xi \in T \cap \Sigma$ in $a \in T$. Po Ore-Asanovi lastnosti obstajata taka elementa $c \in S$ in $\tau \in \Sigma$, da velja $a\tau = \xi c$. Sledi $\xi c \tau^{n-1} = a\tau^n \in T$. Ker je predureditev T Σ-zaprta, sledi, da je $c\tau^{n-1} \in T$. Odtod sledi želena relacija $\xi^{-1} a = c\tau^{n-1}\tau^{-n} \in T(T \cap \Sigma)^{-1}$.

Zaradi prejšnjega odstavka velja račun $T' \cdot T' = T(T \cap \Sigma)^{-1} \cdot T(T \cap \Sigma)^{-1} = T \cdot ((T \cap \Sigma)^{-1} T) \cdot (T \cap \Sigma)^{-1} \subseteq T \cdot (T(T \cap \Sigma)^{-1}) \cdot (T \cap \Sigma)^{-1} \subseteq T(T \cap \Sigma)^{-1} = T'$. Torej je množica T' podpolgrupa polgrupe Q.

Dokažimo zdaj, da velja $T' \cap S = T$. Če je $t \in T$, potem je $t = (t\xi)\xi^{-1} \in T'$ za poljuben element $\xi \in T \cap \Sigma$. Torej je $T \subseteq T' \cap S$. Če je $s \in T' \cap S$, potem obstajata taka elementa $a \in T$ in $\alpha \in T \cap \Sigma$, da velja $s = a\alpha^{-1}$. Ker je predureditev T Σ-zaprta in ker je $s\alpha = a \in T$, sledi $s \in T$.

Ker polgrupa S nima nujno enice moramo dokazati tudi $(T \cap \Sigma)^{-1} \subseteq T'$. Za vsak element $\xi \in T \cap \Sigma$ je $\xi \in T$ in $\xi^2 \in T \cap \Sigma$, zato je $\xi^{-1} = \xi\xi^{-2} \in T'$.

Torej drži točka 2. Očitno iz 2. sledi 3. Preostane še dokaz zadnje trditve.

Naj bo P taka predureditev na Q, ki zadošča $P \cap S = T$ in naj bo $\xi \in (T \cap \Sigma)^{-1}$ poljuben element. Potem velja $\xi^{-1} = \xi^{m-1}(\xi^{-1})^m \in T \cdot \Pi_m(Q) \subseteq P \cdot P \subseteq P$ Q.E.D.

Naslednji izrek pove, da se da predureditev na kvečjemu en način razširiti na polgrupo desnih ulomkov.

Izrek 4 *Naj bo Q polgrupa desnih ulomkov polgrupe S glede na množico desnih imenovalcev Σ in naj bo T predureditev eksponenta n na polgrupi S.*

Naj bo P taka podpolgrupa grupe Q, da velja $P \cap S = T$ in $(T \cap \Sigma)^{-1} \subseteq P$. Potem je $P = T(T \cap \Sigma)^{-1} = \{a\xi^{-1} \in Q;\ a\xi^{n-1} \in T\}$.

Če obstaja predureditev P na polgrupi Q, ki razširja predureditev T, potem je $P = T(T \cap \Sigma)^{-1}$.

Dokaz : Zadošča, če dokažemo, da je $P = \{a\xi^{-1} \in Q;\ a\xi^{n-1} \in T\}$. To nam da enoličnost razširitve. Po izreku 3 odtod sledi, da je $P = T(T \cap \Sigma)^{-1}$.

Vzemimo poljubna elementa $a \in S$ in $\alpha \in \Sigma$, ki zadoščata $a\alpha^{-1} \in P$. Sledi $a\alpha^{n-1} = (a\alpha^{-1})\alpha^n \in P \cdot T \subseteq P$, ker je $T \subseteq P$ in ker je P podpolgrupa. Iz $P \cap S = T$ sledi, da $a\alpha^{n-1} \in T$.

Če $a\alpha^{n-1} \in T$ za nek $a \in S$ in $\alpha \in \Sigma$, potem je $a\alpha^{-1} = (a\alpha^{n-1})\alpha^{-n} \in T(T \cap \Sigma)^{-1} \subseteq P \cdot P \subseteq P$ po izbiri P.

Vsaka predureditev P na polgrupi Q, ki razširja predureditev T ima po izreku 3 lastnost $(T \cap \Sigma)^{-1} \subseteq P$. Torej po prvem delu izreka sledi, da je $P = T(T \cap \Sigma)^{-1}$. Q.E.D.

2.3 Eksistenca razširitve

Naj bo Q polgrupa desnih ulomkov polgrupe S glede na množico desnih imenovalcev Σ. Naj bo T Σ-zaprta predureditev na polgrupi S in naj bo $T' = T(T \cap \Sigma)^{-1}$. Rezultati iz

prejšnjega razdelka napeljujejo na naslednje vprašanje. Ali je množica $T' = T(T \cap \Sigma)^{-1}$ predureditev na polgrupi S? Ali je predureditev eksponenta n?

Če je množica Σ vsebovana v centru polgrupe S, potem je odgovor na obe vprašanji pozitiven. To sledi iz $\Pi_n(Q) \subseteq \Pi_n(S)(\Pi_n(\Sigma))^{-1}$, $\Pi_n(S) \subseteq T$ in $\Pi_n(\Sigma) \subseteq T \cap \Sigma$. V nadaljevanju bomo našli bolj splošen pogoj, ki bo zagotavljal, da je odgovor na obe vprašanji pozitiven.

Trditev 5 *Naj bodo Q, S, Σ kot zgoraj. Naj bo T Σ-zaprta predureditev eksponenta n na polgrupi S in naj bo $T' = T(T \cap \Sigma)^{-1}$.*

Naslednje trditve so ekvivalentne.

1. *Za poljubne elemente $a, c \in S$ in $\xi \in T \cap \Sigma$ iz $a\xi c \in T$ sledi $ac \in T$.*
2. *Za poljubne elemente $a, b \in S$ in $\xi \in T \cap \Sigma$ iz $ab \in T$ sledi $a\xi^{-1}b \in T'$.*
3. *Za poljubne elemente $a_1, \ldots, a_k \in S$ in $\xi_1, \ldots, \xi_k \in T \cap \Sigma$ iz $a_1 \cdots a_k \in T$ sledi $a_1\xi_1^{-1} \cdots a_k\xi_k^{-1} \in T'$.*
4. *Za poljubne elemente $a_1, \ldots, a_k \in S$ in $\alpha_1, \ldots, \alpha_k \in \Sigma$ iz $a_1\alpha_1^{n-1} \cdots a_k\alpha_k^{n-1} \in T$ sledi $a_1\alpha_1^{-1} \cdots a_k\alpha_k^{-1} \in T'$.*

Tudi naslednje trditve so ekvivalentne.

5. *Za poljubne elemente $a, c \in S$ in $\xi \in T \cap \Sigma$ iz $ac \in T$ sledi $a\xi c \in T$.*
6. *Za poljubne elemente $a, b \in S$ in $\xi \in T \cap \Sigma$ iz $a\xi^{-1}b \in T'$ sledi $ab \in T$.*
7. *Za poljubne elemente $a_1, \ldots, a_k \in S$ in $\xi_1, \ldots, \xi_k \in T \cap \Sigma$ iz $a_1\xi_1^{-1} \cdots a_k\xi_k^{-1} \in T'$ sledi $a_1 \cdots a_k \in T$.*
8. *Za poljubne elemente $a_1, \ldots, a_k \in S$ in $\alpha_1, \ldots, \alpha_k \in \Sigma$ iz $a_1\alpha_1^{-1} \cdots a_k\alpha_k^{-1} \in T'$ sledi $a_1\alpha_1^{n-1} \cdots a_k\alpha_k^{n-1} \in T$.*

Dokaz : Dokažimo, da velja 1. $\Leftrightarrow$ 2. $\Leftrightarrow$ 3. $\Leftrightarrow$ 4. Če v sledečem dokazu obrnemo puščice, dobimo 5. $\Leftrightarrow$ 6. $\Leftrightarrow$ 7. $\Leftrightarrow$ 8.

Privzemimo, da drži trditev 1. Vzemimo poljubna elementa $a, b \in S$, ki zadoščata $ab \in T$ in poljuben element $\xi \in T \cap \Sigma$. Po Ore-Asanovi lastnosti obstajajo taki elementi $c \in S$ in $\tau \in \Sigma$, da velja $b\tau = \xi c$. Ker je $ab \in T$, sledi $a\xi(c\tau^{n-1}) = ab\tau^n \in T$. Če

uporabimo trditev 1. dobimo $ac\tau^{n-1} \in T$. Sledi $a\xi^{-1}b = a\xi^{-1}b\tau^n\tau^{-n} = (ac\tau^{n-1})\tau^{-n} \in T(T \cap \Sigma)^{-1} = T'$. Torej drži trditev 2.

Če drži trditev 2., vzemimo poljubne elemente $a, c \in S$ in $\xi \in T \cap \Sigma$, ki zadoščajo $(a\xi)c \in T$. Sledi $ac = (a\xi)\xi^{-1}c \in T$. Torej drži trditev 1.

Če vstavimo $k = 2$ v trditev 3., dobimo 2.

Privzemimo, da drži trditev 2. Če $k-1$ krat uporabimo dejstvo, da iz predpostavke $ab\tau^{-1} \in T'$ sledi $a\xi^{-1}b\tau^{-1} \in T'$ za poljubne $a, b \in S$ in $\xi, \tau \in T \cap \Sigma$., potem dobimo naslednje zaporedje sklepov $a_1 \cdots a_{k-1}a_k\xi_k^{-1} \in T' \Rightarrow a_1 \cdots a_{k-1}\xi_{k-1}^{-1}a_k\xi_k^{-1} \in T' \Rightarrow \ldots \Rightarrow a_1\xi_1^{-1} \cdots a_{k-1}\xi_{k-1}^{-1}a_k\xi_k^{-1} \in T'$. Torej drži trditev 3.

Ekvivalenca med 3. in 4. sledi iz $a_1\alpha_1^{-1} \cdots a_k\alpha_k^{-1} = (a_1\alpha_1^{n-1})\alpha_1^{-n} \cdots (a_k\alpha_k^{n-1})\alpha_k^{-n}$ in iz dejstva, da $\alpha_1^n, \ldots, \alpha_k^n \in T \cap \Sigma$ za poljubne $a_1, \ldots, a_k \in S$ in $\alpha_1, \ldots, \alpha_k \in \Sigma$. Q.E.D.

Izrek 6 *Naj bodo Q, S, Σ kot zgoraj. Naj bo T Σ-zaprta predureditev eksponenta n na polgrupi S in naj bo $T' = T(T \cap \Sigma)^{-1}$.*

Če ima T lastnost 1. iz trditve 5, potem je T' predureditev eksponenta n.

Dokaz : Naj bo T taka Σ-zaprta predureditev eksponenta n, da iz predpostavke $a\xi c \in T$ sledi $ac \in T$ za poljubne elemente $a, c \in S$ in $\xi \in T \cap \Sigma$.

Za poljuben $z \in \Pi_n(Q)$ obstaja tako končno zaporedje $(a_1, \alpha_1), \ldots, (a_k, \alpha_k)$ v množici $S \times \Sigma$, da vsak element nastopa z večkratnostjo, deljivo z n in da velja $z = a_1\alpha_1^{-1} \cdots a_k\alpha_k^{-1}$. Ker je $a_1\alpha_1^{n-1} \cdots a_k\alpha_k^{n-1} \in \Pi_n(S) \subseteq T$, sledi po točki 4. trditve 5, da velja $z \in T'$ Q.E.D.

2.4 Lastnosti, ki se ohranjajo pri razširitvah

Izrek 7 *Naj bodo Q, S, Σ kot zgoraj. Množica T je Σ-zaprta predureditev na S eksponenta n s permutacijsko lastnostjo natanko tedaj, ko je množica $T' = T(T \cap \Sigma)^{-1}$ predureditev eksponenta n na polgrupi Q s permutacijsko lastnostjo.*

Dokaz : Naj bo T Σ-zaprta predureditev eksponenta n s permutacijsko lastnostjo. Potem ima T lastnosti 1. in 5. iz trditve 5. Privzemimo, da velja $a_1\alpha_1^{-1} \cdots a_k\alpha_k^{-1} \in T'$. Po lastnosti 8. iz trditve 5 sledi $a_1\alpha_1^{n-1} \cdots a_k\alpha_k^{n-1} \in T$. Ker ima T permutacijsko lastnost, sledi $a_{\pi(1)}\alpha_{\pi(1)}^{n-1} \cdots a_{\pi(k)}\alpha_{\pi(k)}^{n-1} \in T$ za poljubno permutacijo π množice $\{1, \ldots, k\}$. Po lastnosti 4. iz trditve 5 sledi $a_{\pi(1)}\alpha_{\pi(1)}^{-1} \cdots a_{\pi(k)}\alpha_{\pi(k)}^{-1} \in T'$. Torej ima množica T' permutacijsko lastnost. Odtod sledi po izreku 6, da je T' predureditev eksponenta n. Q.E.D.

Izrek 8 *Naj bodo Q, S, Σ kot zgoraj. Množica T je zaprta predureditev na S eksponenta n natanko tedaj, ko je množica $T' = T(T \cap \Sigma)^{-1}$ zaprta predureditev na Q eksponenta n.*

Dokaz : Če je T zaprta predureditev, ima tudi permutacijsko lastnost. Po izreku 7 je množica T' predureditev eksponenta n.Dokazujemo, da je tudi predureditev T' zaprta.

Naj bodo $a \in S$, $\xi \in \Sigma$, $a \in T$ in $\tau \in T \cap \Sigma$ taki elementi, da velja $a\xi^{-1}b\tau^{-1} \in T'$. Odtod sledi $(a\xi^{n-1})\xi^{-n}b = (a\xi^{-1}b\tau^{-1})\tau \in T'$. Ker je $\xi^n \in \Sigma \cap T$, dobimo odtod po lastnosti 6. iz trditve 5 da velja $a\xi^{n-1}b \in T$. Ker je predureditev T zaprta, sledi $a\xi^{n-1} \in T$. Torej res velja $a\xi^{-1} = a\xi^{n-1}\xi^{-n} \in T(T \cap \Sigma)^{-1} = T'$, kar smo želeli dokazati. Q.E.D.

Izrek 9 *Naj bodo Q, S, Σ kot zgoraj. Množica T je ciklična predureditev eksponenta n na polgrupi S natanko tedaj, ko je množica $T' = T(T \cap \Sigma)^{-1}$ ciklična predureditev eksponenta n na polgrupi Q.*

Dokaz : Naj bo T ciklična predureditev in naj bo $\phi : S \to \mu_n$ tak polgrupni homomorfizem, da velja $T = \phi^{-1}(1)$. Po izreku 2 lahko ϕ razširimo do homomorfizma $\phi' : Q \to \mu_n$. Naj bo $P = (\phi')^{-1}(1)$. Očitno je P ciklična predureditev eksponenta n. Če dokažemo $P \cap S = T$, bo iz enoličnosti razširitve sledilo $P = T'$. Naj bo $x \in P \cap S$ poljuben element. Torej je $\phi(x) = \phi'(x) = 1$ in zato $x \in T$. Obratna smer je očitna. Q.E.D.

3.

Kadison-Duboisova reprezentacija

Kadison-Duboisova reprezentacija (glej [8],[10] in [11]) velja za kolobarje, ki niso nujno asociativni ali komutativni. Njen dokaz uporablja tehnike iz funkcionalne analize (Banach-Alaoglujev in Krein-Milmanov izrek). Becker in Schwarz [12] sta za komutativne kolobarje našla konkreten opis reprezentacijskega prostora in zelo poenostavila dokaz. V tem poglavju njun opis reprezentacijskega prostora razširimo na asociativne kolobarje.

3.1 Predstožci in moduli

Naj bo R poljuben kolobar z enico (ne zahtevamo niti komutativnosti niti asociativnosti). Množica $H \subset R$ se imenuje *predstožec*, če zadošča naslednjim lastnostim:

1. $H + H \subseteq H$,
2. $H \cdot H \subseteq H$.
3. $0, 1 \in H$,
4. $-1 \notin H$,

Množici, ki zadošča samo prvim trem lastnostim pravimo *podpolkolobar* v R. Če je H poljuben podpolkolobar v R potem velja $-1 \notin H$ natanko tedaj, ko H ni podkolobar. Predstožci so torej ravno tisti podpolkolobarji, ki niso podkolobarji.

Primeri predstožcev:

1. Naj bo R poljuben kolobar z enico in naj bo $N = \{n \cdot 1;\ n = 0, 1, 2, \ldots\}$. Množica N je vsebovana v vsakem predstožcu na kolobarju R. Torej so ekvivalentne trditve:

(a) Kolobar R ima karakteristiko 0.

(b) Množica N je predstožec na R.

(c) Na R obstaja vsaj en predstožec.

2. Obstaja naravna bijektivna korespondenca med predstožci H na kolobarju R, za katere velja $H \cap -H = \{0\}$ in med delnimi ureditvami $<$ na R, za katere velja $0 < 1$.

3. Predureditve na kolobarjih (glej razdelek 6.1).

Naj bo H predstožec na kolobarju R. Množica $H - H$ je podkolobar kolobarja R. Pravimo, da je predstožec H *usmerjen*, če velja $H - H = R$. V nadaljevanju bomo spoznali dva primera usmerjenih predstožcev: arhimedske predstožce in izolirane predureditve.

Za vsak predstožec H vpeljimo naslednje oznake: $H^0 = H \cap -H$, $H^+ = H \setminus -H$ in $H^- = -H \setminus H$. Množici H^0 pravimo *nosilec* predstožca H. Očitno je H^0 pravi dvostranski ideal v podkolobarju $H - H$. Če je predstožec usmerjen, je njegov nosilec dvostranski ideal v kolobarju R.

Podmnožica $M \subseteq R$ je *modul* nad predstožcem H, Če zadošča naslednjim štirim lastnostim:

1. $M + M \subseteq M$,

2. $HM \subseteq M$,

3. $MH \subseteq M$,

4. $1 \in M$,

Modul M nad H je *pravi*, če velja $-1 \notin M$. Najenostavnejši primer pravega modula nad H je kar množica H. Očitno je unija naraščajoče družine pravih modulov nad H spet pravi modul nad H. Za vsak predstožec H torej obstaja maksimalen pravi modul nad H.

Naj bo H usmerjen predstožec in M modul nad H. Potem je M pravi modul natanko tedaj, ko je prava podmnožica kolobarja R. V tem primeru je množica $M \cap -M$ pravi dvostranski ideal v kolobarju R.

Za poljubno množico S označimo $S^e = \{r \in R; \exists k \in \mathbb{N} : kr \in S\}$. Pravimo, da je množica S *izolirana*, če velja $S = S^e$. Očitno velja $(S^e)^e = S^e$, torej je množica S^e vedno izolirana množica.

Če je H predstožec, potem je množica H^e tudi predstožec. Če je M modul nad H, potem je tudi M^e modul nad H (pa tudi nad H^e). Če je modul M pravi, je tudi modul M^e pravi.

3.2 Arhimedski predstožci

Naj bo R poljuben asociativen kolobar z enico in naj bo P poljuben predstožec na R. Pravimo, da je predstožec P *arhimedski*, če za vsak element $r \in R$ obstaja tako naravno število k, da velja $k - r \in P$. Očitno je vsak arhimedski predstožec usmerjen.

Za vsak modul M označimo $\mathrm{Arch}(M) = \{r \in R;\ \forall n \in \mathbb{N} :\ 1 + nx \in M^e\}$. Pravimo, da je modul M *arhimedsko poln*, če velja $\mathrm{Arch}(M) = M$.

Trditev 1 *Naj bo M pravi modul nad arhimedskim predstožcem P. Potem je množica* $\mathrm{Arch}(M)$ *arhimedsko poln pravi modul nad P in $M \subseteq \mathrm{Arch}(M)$.*

Dokaz : Očitno je $M \subseteq \mathrm{Arch}(M)$. Vzemimo poljubna elementa $a, b \in \mathrm{Arch}(M)$ in poljubno naravno število n. Potem velja $2(1 + n(a + b)) = (1 + 2na) + (1 + 2nb) \in M^e + M^e \subseteq M^e$. Torej je $a + b \in \mathrm{Arch}(M^e) = \mathrm{Arch}(M)$. S tem smo dokazali zaprtost za seštevanje.

Dokažimo še zaprtost za množenje z elementi iz P. Naj bodo $a \in \mathrm{Arch}(M)$, $p \in P$ in $n \in \mathbb{N}$ poljubni. Ker je predstožec P arhimedski, obstaja tako naravno število k, da velja $k - p \in P$. Potem velja $k(1 + npa) = (k - p) + p(1 + kna) \in P + P \cdot M^e \subseteq M^e$ in $k(1 + nap) = (k - p) + (1 + kna)p \in M^e$. Torej $pa \in \mathrm{Arch}(M)$ in $ap \in \mathrm{Arch}(M)$.

Dokažimo sedaj, da je modul $\mathrm{Arch}(M)$ pravi. Če $-1 \in \mathrm{Arch}(M)$, potem je $1+2(-1) \in M^e$, kar je v nasprotju s predpostavko, da je modul M pravi.

Preostane še dokaz, da je modul $\mathrm{Arch}(M)$ arhimedsko poln. Vzemimo poljuben element $a \in \mathrm{Arch}(\mathrm{Arch}(M))$ in poljubno naravno število n. Potem velja $1 + (n + 1)a \in \mathrm{Arch}(M)$ in $(n + 1)(1 + na) = 1 + n(1 + (n + 1)a) \in M^e$. Torej je $1 + na \in M^e$ za vsako naravno število n, kar po definiciji pomeni, da $a \in \mathrm{Arch}(M)$. Q.E.D.

Trditev 2 *Naj bo M pravi modul nad arhimedskim predstožcem P. Naj bo $a \in R$ tak element, da $-1 \in M - \Sigma(PaP)$. Potem $a \in \mathrm{Arch}(M)$.*

Dokaz : Ker $-1 \in M - \Sigma(PaP)$, obstaja tako naravno število l in taki elementi $p_1, q_1, \ldots, p_l, q_l \in P$ in $m \in M$, da velja $-1 = m - p_1aq_1 - \ldots - p_laq_l$. Ker je predstožec P arhimedski, obstaja tako naravno število $n > 1$, da velja $n - p_i \in P$ in $n - q_i \in P$ za vsak $i = 1, \ldots, l$.

Definirajmo množico $A = \{\frac{r}{s};\ r, s \in \mathbb{N}, r + sa \in M^e\}$. Ker je predstožec P arhimedski, je množica A neprazna. Trdimo, da je $\inf(A) = 0$. Vzemimo poljubni naravni števili r, s, za katere velja $r + sa \in M^e$. Naj bo $k := ln^2$. Potem velja $kr - s + ksa = ln^2(r + sa) - s = \sum_{i=1}^{l}(n - p_i + p_i)(r + sa)(n - q_1 + q_i) - s = \sum_{i=1}^{l}(n - p_i)(r + sa)(n - q_1) + \sum_{i=1}^{l} p_i(r + sa)(n - q_1) + \sum_{i=1}^{l}(n - p_i)(r + sa)q_i + r\sum_{i=1}^{l} p_iq_i + sm \in M^e$.

Ločimo dve možnosti. Če je $\frac{r}{s} > \frac{1}{k}$, potem sta $kr - s$ in ks naravni števili, zato iz $kr - s + ksa \in M^e$ sledi, da $\frac{r}{s} - \frac{1}{k} = \frac{kr-s}{ks} \in A$. Če je $\frac{r}{s} < \frac{1}{k}$, potem je $s - kr > 0$. Odtod sledi, da $r + ksa = (kr - s + ksa) + (s - kr) + r \in M^e$. Torej je $\frac{r}{ks} \in A$. Ker je število k fiksno, odtod sledi, da je $\inf(A) = 0$.

Vzemimo poljubno naravno število n. Po pravkar dokazanem obstajata taki naravni števili r in s, da velja $\frac{r}{s} \in A$ in $\frac{r}{s} < \frac{1}{n}$. Odtod sledi $s(1 + na) = n(r + sa) + (s - nr) \in M^e$, torej je res $a \in \mathrm{Arch}(M)$. Q.E.D.

Izrek 3 *Naj bo M pravi modul nad arhimedskim predstožcem P. Potem je* $\mathrm{Arch}(M) = \bigcap S$*, kjer presek teče po vseh maksimalnih pravih modulih nad P, ki vsebujejo modul M.*

Dokaz : Ker je S maksimalen modul nad P, sledi po trditvi 1, da je $\mathrm{Arch}(S) = S$. Očitno je $\mathrm{Arch}(M) \subseteq \mathrm{Arch}(S)$. Torej je leva stran res vsebovana v desni.

Dokažimo sedaj, da je desna stran vsebovana v levi. Vzemimo poljuben element $a \in \bigcap S$ in poljubno naravno število n. Če $1 + na \notin \mathrm{Arch}(M)$, potem je po trditvi 2 modul $M' = M - \Sigma(P(1 + na)P)$ pravi. Po Zornovi lemi obstaja tak maksimalen pravi modul S nad P ki vsebuje modul M'. Iz $-1 - na \in S$ in $a \in S$ sledi protislovje $-1 \in S$. Torej $1 + na \in \mathrm{Arch}(M)$ za vsako naravno število n. Ker je po trditvi 1 modul $\mathrm{Arch}(M)$ arhimedsko poln, sledi $a \in \mathrm{Arch}(M)$. Q.E.D.

Izrek 4 *Naj bo S maksimalen pravi modul nad arhimedskim predstožcem. Potem velja $S \cup -S = R$.*

Dokaz : Vzemimo poljuben element $a \notin S$. Množica $S + \Sigma(PaP)$ je modul nad P, ki strogo vsebuje modul S. Ker je S maksimalen pravi modul, odtod sledi $-1 \in S + \Sigma(PaP)$.

Po trditvi 2 odtod sledi, da $-a \in \mathrm{Arch}(S) = S$. Q.E.D.

3.3 Reprezentacijski prostor

Naj bo R asociativen kolobar z enico, P predstožec na R in M pravi modul nad P. Če velja $M \cup -M = R$, pravimo, da je modul M *polureditev* nad P. Po izreku 4 je vsak maksimalen pravi modul nad arhimedskim predstožcem P tudi polureditev nad P.

Izrek 5 *Naj bo P arhimedski predstožec na kolobarju R in naj bo M polureditev nad P. Potem obstaja natanko en unitalen homomorfizem ϕ_S iz kolobarja R v kolobar realnih števil, ki zadošča $\phi_S(S) \geq 0$.*

Dokaz : Vzemimo poljuben element $a \in R$ in definirajmo $M_S(a) = \{\frac{r}{s};\ (r,s) \in \mathbb{Z} \times \mathbb{N}\ \&\ r - sa \in S\}$. Ker je predstožec P arhimedski, obstajata taki naravni števil k in l, da velja $k - a \in P$ in $l + a \in P$. Iz prve relacije sledi, da je množica $M_S(a)$ neprazna. Iz druge relacije dobimo, da je množica $M_S(a)$ navzdol omejena. Za vsak element $\frac{r}{s} \in M_S(a)$ namreč velja $r + sl = (r - sa) + s(l + a) \in S$. Ker je modul S pravi, odtod sledi $r + sl \geq 0$, torej je $\frac{r}{s} \geq -l$.

Definirajmo $\phi_S(a) = \inf M_S(a)$ za vsak element $a \in R$.

Dokažimo najprej, da je $\phi_S(1) = 1$. Ker je modul S pravi, velja $r - s \in S$ natanko tedaj, ko je $r - s \geq 0$. Torej je $\frac{r}{s} \in M_S(1)$ natanko tedaj, ko je $\frac{r}{s} \geq 1$. To pomeni, da je $\inf M_S(1) = 1$.

Dokažimo sedaj, da je $\phi_S(-a) = -\phi_S(a)$ za vsak $a \in R$. Vzemimo poljubna elementa $\frac{r}{s} \in M_S(a)$ in $\frac{u}{v} \in M_S(-a)$. Odtod sledi $vr + su = v(r - sa) + s(u + va) \in S$. Ker je modul S pravi, je $vr + su =\geq 0$. Iz $\frac{r}{s} + \frac{u}{v} \geq 0$ sledi $\phi_S(-a) \geq -\phi_S(a)$. Če je $\phi_S(-a) \neq -\phi_S(a)$, potem obstaja tako racionalno število $\frac{m}{n}$, da je $\phi_S(-a) > \frac{m}{n} > -\phi_S(a)$. Odtod sledi $\frac{m}{n} \notin M_S(-a)$ in $-\frac{m}{n} \notin M_S(a)$. Torej je $m + na \notin S$ in $-m - na \notin S$, kar je v nasprotju s predpostavko, da je S polureditev.

Naj bosta $a, b \in R$ poljubna elementa. Trdimo, da je $\phi_S(a + b) = \phi_S(a) + \phi_S(b)$. Vzemimo poljubna $\frac{r}{s} \in M_S(a)$ in $\frac{u}{v} \in M_S(b)$. Potem je $(vr + su) - vs(a + b) = v(r - sa) + s(u - vb) \in S$, torej je $\frac{r}{s} + \frac{u}{v} = \frac{vr+su}{vs} \in M_S(a + b)$. Odtod sledi $\phi_S(a + b) \leq \phi_S(a) + \phi_S(b)$. Nasprotno oceno dobimo, če zamenjamo a in b z $-a$ in $-b$ in upoštevamo prejšnji odstavek.

Naj bosta $a, b \in R$ poljubna elementa. Trdimo, da je $\phi_S(ab) = \phi_S(a)\phi_S(b)$. Ker je $P - P = R$ in ϕ_S aditivna, lahko privzamemo, da je $b \in P$. Vzemimo poljubna $\frac{r}{s} \in M_S(a)$

in $\frac{u}{v} \in M_S(b)$. Ker je S modul nad P, velja $ru - svab = (r - sa)vb + r(u - vb)$, torej je $\frac{ru}{sv} \in M_S(ab)$. Odtod sledi ocena $\phi_S(ab) \leq \phi_S(a)\phi_S(b)$. Nasprotno oceno dobimo, če zamenjamo a z $-a$.

Dokažimo še enoličnost. Naj bo $\phi : R \to \mathbb{R}$ tak unitalen homomorfizem kolobarjev, da velja $\phi(S) \geq 0$. Naj bo $a \in R$ poljuben element. Če je $\phi_S(a) < \frac{r}{s}$, potem je $r - sa \in S$. Odtod sledi $r - s\phi(a) = \phi(r - sa) \geq 0$, torej je $\phi(a) \leq \frac{r}{s}$. To pomeni, da je $\phi(a) \leq \phi_S(a)$. Nasprotno oceno dobimo, če zamenjamo a z $-a$. Q.E.D.

Trditev 6 *Za vsako polureditev S velja $\phi_S^{-1}(\mathbb{R}^+) = \mathrm{Arch}(S)$.*

Dokaz : Naj bo $a \in R$ tak element, da je $\phi_S(a) \geq 0$. Naj bo n poljubno naravno število. Če $1 + na \notin S$, potem $1 + na \in -S$. Odtod sledi, da je $1 + n\phi_S(a) \leq 0$, torej $\phi_S(a) \leq -\frac{1}{n}$, kar je v nasprotju z izbiro elementa a. Torej je $1 + na \in S$ za vsako naravno število n, se pravi $a \in \mathrm{Arch}(S)$.

Obratno, če je $a \in \mathrm{Arch}(S)$, potem je $1 + na \in S$ za vsak naraven n, torej je $1 + n\phi_S(a) \geq 0$ za vsak naraven n. Odtod sledi, da je $\phi_S(a) \geq 0$. Q.E.D.

Naj bo M pravi modul nad arhimedskim predstožcem P. Množici $X_P(M) = \{\phi \in Hom(R, \mathbb{R});\ \phi(M) \geq 0\}$ pravimo *reprezentacijski prostor* modula M.

Izrek 7 *Naj bo P arhimedski stožec na kolobarju R in M modul nad P. Preslikavi $F : \phi \to \phi^{-1}(\mathbb{R}^+)$ in $G : S \to \phi_S$ podajata bijektivno korespondenco med elementi reprezentacijskega prostora modula M in maksimalnimi moduli nad P, ki vsebujejo modul M.*

Dokaz : Vzemimo poljuben element $\phi \in X_P(M)$. Trdimo, da je množica $\phi^{-1}(\mathbb{R}^+)$ maksimalen modul nad P, ki vsebuje M. Očitno je ta množica polureditev nad P, ki vsebuje modul M. Naj bo S maksimalen pravi modul nad P, ki vsebuje množico $\phi^{-1}(\mathbb{R}^+)$ in naj bo ϕ_S pripadajoči homomorfizem kolobarjev. Ker je $\phi_S(\phi^{-1}(\mathbb{R}^+)) \subseteq \mathbb{R}^+$ in $\phi(\phi^{-1}(\mathbb{R}^+)) \subseteq \mathbb{R}^+$, velja $\phi = \phi_S$. Odtod sledi $S \subseteq \phi_S^{-1}(\mathbb{R}^+) = \phi^{-1}(\mathbb{R}^+) \subseteq S$. Torej je množica $\phi^{-1}(\mathbb{R}^+) = S$ res maksimalen modul nad P. Odtod sledi tudi, da je $\phi_{\phi^{-1}(\mathbb{R}^+)} = \phi$, kar je ravno $G(F(\phi)) = \phi$. Za poljuben maksimalen pravi modul S' nad P velja po trditvi 6 $F(G(S')) = \phi_{S'}^{-1}(\mathbb{R}^+) = \mathrm{Arch}(S') = S'$. Q.E.D.

Izrek 8 *Naj bo M pravi modul nad arhimedskim predstožcem P. Najšibkejša topologija na reprezentacijskem prostoru $X_P(M)$, za katero so vse evaluacije $\widehat{a} : \phi \to \phi(a)$ zvezne, je kompaktna.*

Dokaz : Za vsak element $a \in R$ izberimo tako naravno število k_a, da velja $k_a \pm a \in P$. Označimo $X = X_P(M)$, $Y = \{\psi;\ \psi$ funkcija iz R v $\mathbb{R}$ in $-k_a < \psi(a) < k_a$ za vsak $a \in R\}$. $Z = \{f;\ f$ funkcija iz R v $\mathbb{R}\}$. Očitno velja $X \subseteq Y \subseteq Z$. Na Z vsamemo najšibkejšo topologijo v kateri so vse evaluacije zvezne. (To je ravno topologija konvergence po točkah.) Prostor Y (z relativno topologijo) je homeomorfen prostoru $\prod_{a\in R}[-k_a, k_a]$ (s produktno topologijo), zato je kompakten po izreku Tihonova. Dokažimo, da je podprostor X zaprt v prostoru Y in zato kompakten. Naj bo ψ poljuben element iz zaprtja X v Y. Vzemimo poljubna $a, b \in R$ in $\epsilon > 0$. Potem obstaja tak element $\phi \in X_P(M)$, da velja $|\phi(a) - \psi(a)| < \frac{\epsilon}{3k_a}$, $|\phi(b) - \psi(b)| < \frac{\epsilon}{3k_b}$ in $|\phi(ab) - \psi(ab)| < \frac{\epsilon}{3}$. Potem je $|\psi(ab) - \psi(a)\psi(b)| \leq |\psi(ab) - \phi(ab)| + |\phi(a)||\phi(b) - \psi(b)| + |\psi(b)||\phi(a) - \psi(a)| \leq \epsilon$. Odtod sledi, da je $\psi(ab) = \psi(a)\psi(b)$. Podobno dokažemo še $\psi(a + b) = \psi(a) + \psi(b)$, $\psi(1) = 1$ in $\psi(M) \geq 0$, torej res $\psi \in X_P(M)$. Q.E.D.

3.4 Kadison-Duboisova reprezentacija

Naj bo M pravi modul nad arhimedskim predstožcem P. Po definiciji topologije na reprezentacijskem prostoru $X_P(M)$ velja $\widehat{a} \in C(X_P(M), \mathbb{R})$ za vsak element $a \in R$. Po trditvi 5 je reprezentacijski prostor neprazen in po izreku 8 je kompakten. Preslikavi

$$\Phi : R \to C(X_P(M), \mathbb{R}),\ \Phi(a) = \widehat{a}$$

pravimo *Kadison-Duboisova reprezentacija* (kolobarja R glede na modul M.) Očitno je Φ unitalen homomorfizem kolobarjev, ki zadošča $\Phi(M) \subseteq C^+(X_P(M), \mathbb{R})$, kjer je $C^+(X_P(M), \mathbb{R})$ množica nenegativnim zveznih funkcij. Lahko dokažemo celo več.

Izrek 9 *Pri gornjih predpostavkah velja*

1. $\Phi^{-1}(C^+(X_P(M), \mathbb{R})) = \mathrm{Arch}(M)$.
2. $\Phi^{-1}(0) = \mathrm{Arch}(M) \cap -\mathrm{Arch}(M)$.
3. *Množica* $\mathbb{Q}\cdot\Phi(R)$ *je gosta v* $C(X_P(M), \mathbb{R})$, *glede na topologijo konvergence po točkah.*

Dokaz : Velja $\Phi^{-1}(C^+(X_P(M), \mathbb{R})) = \{a \in R;\ \widehat{a} \in C^+(X_P(M), \mathbb{R})\} = \{a \in R;\ \phi(a) \in \mathbb{R}^+ \text{ za vsak } \phi \in X_P(M)\} = \bigcap_{\phi \in X_P(M)} \phi^{-1}(\mathbb{R}^+)$ Po izreku 7 je ta množica enaka množici $\bigcap S$ kjer S teče po maksimalnih pravih modulih nad P, ki vsebujejo modul M. Po izreku 3 je ta množica enaka $\mathrm{Arch}(M)$.

Druga trditev sledi iz prve. Tretja trditev sledi iz Stone-Weierstrassovega izreka. Množica $\mathbb{R} \cdot \Phi(R)$ namreč loči točke in vsebuje konstante. Q.E.D.

Posledica 10 *Naj bo P arhimedski predstožec na kolobarju R.*

1. *Množica $\mathrm{Arch}(P) \cap -\mathrm{Arch}(P)$ je reduciran ideal, ki vsebuje vse elemente oblike $xy - yx$, kjer $x, y \in R$.*

2. *Za vsak pravi modul M nad P je množica $\mathrm{Arch}(M)$ zaprta za množenje. Posebej je vsak maksimalen pravi modul S nad P zaprt za množenje.*

Skicirajmo še klasičen pristop k Kadison-Duboisovi reprezentaciji. Naj bo P arhimeadski predstožec na R. Množica $P' = P/P^0$ je arhimedski stožec na faktorskem kolobarju $R' = R/P^0$. Nato stožec P' razširimo do arhimedskega stožca P_N na racionalni algebri $R_N = R \otimes \mathbb{Q}$. Preslikava $t(x) := \inf\{r;\ r \pm x \in \mathrm{Arch}(P_N)\}$ je norma na algebri R_N. Ko napolnimo R_N v tej normi dobimo Banachovo algebro R^* in $\mathrm{Arch}(P_N)$ se razširi do stožca P^* na R^*. Urejena algebra (R^*, P^*) je izomorfna urejeni algebri $(C(X), C^+(X))$, kjer je X množica pozitivnih karakterjev na algebri (R^*, P^*). Za dokaz nepraznosti in kompaktnosti množice X potrebujemo Krein-Milmanov in Banach Alaoglujev izrek. Za podrobnosti glej originalne članke. Prednosti Beckerjevega pristopa so:

1. je rahlo splošnejši (M namesto P),

2. dobimo konkreten opis reprezentacijskega prostora z maksimalnimi polureditvami,

3. ne potrebujemo sredstev iz funkcionalne analize.

Problem pri uporabi Kadison-Duboisove reprezentacije je v tem, da za nas zanimivi predstožci ponavadi niso arhimedski. Ta problem se delno reši tako, da se reprezentacija uporabi na določenem podkolobarju kolobarja R.

Naj bo P poljuben predstožec na kolobarju R. Definirajmo množico $\mathrm{A}(P) = \{a \in R;\ \exists k \in \mathbb{N} : k \pm a \in P^e\}$.

Izrek 11 *Naj bo P poljuben predstožec na kolobarju R. Potem je množica $\mathrm{A}(P)$ unitalen podkolobar v R in množica $P^e \cap \mathrm{A}(P)$ je arhimedski predstožec na R.*

Dokaz : Naj bosta $a, b \in \mathrm{A}(P)$ poljubna elementa in naj bosta k, l taki naravni števili, da velja $k \pm a \in P^e$ in $l \pm b \in P^e$. Potem velja $2(kl - ab) = (k-a)(l+b) + (k+a)(l-b) \in P^e$ in $2(kl + ab) = (k+a)(l+b) + (k-a)(l-b) \in P^e$. Odtod sledi, da $kl \pm ab \in P^e$, torej $ab \in \mathrm{A}(P)$. Ostale trditve je enostavno preveriti. Q.E.D.

Naslednji izrek je neposredna posledica izrekov 9 in 11.

Izrek 12 *Naj bo P poljuben izoliran predstožec na kolobarju R.*

1. *Za vsak element $a \in \mathrm{A}(P)$ je $a^2 \in \mathrm{Arch}(P)$.*
2. *Če $a^n \in \mathrm{Arch}(P)$ za nek $a \in \mathrm{A}(P)$ in nek lih n, potem je $a \in \mathrm{Arch}(P)$.*
3. *$\mathrm{I}(P) := \mathrm{Arch}(P) \cap -\mathrm{Arch}(P)$ je reduciran ideal v $\mathrm{A}(P)$.*

4.

Ciklični stožci na domenah

V prvem razdelku konstruiramo primer cikličnega stožca na kolobarju kvantnih polinomov. Preostanek poglavja je posvečen vprašanju: Ali obstaja taka domena, ki se ne da vložiti v obseg in na kateri obstajajo ciklični stožci vseh sodih eksponentov.

Domeno, ki se ne da vložiti v obseg je konstruiral Malcev [13], Vinogradov [14] pa je pokazal, da je ta domena linarno urejena.

4.1 Definicije

Domena je asociativen kolobar z enico, ki nima deliteljev niča.

Lema 1 *Za poljubno podmnožico P domene D so ekvivalentne trditve:*

1. *P je pozitivni stožec kake delne ureditve na D,*
2. *$P + P \subseteq P$, $P \cdot P \subseteq P$ in $P \cap -P = \{0\}$,*
3. *$P^\times + P^\times \subseteq P^\times$, $P^\times \cdot P^\times \subseteq P^\times$ in $0 \in P$.*

Tu smo označili $P^\times = P \setminus \{0\}$.

Množici, ki zadošča eni od ekvivalentnih lastnosti v lemi 1 pravimo *pozitivni stožec.*

Število n se imenuje *eksponent* pozitivnega stožca P, če velja $\Pi_n(D) \subseteq P$. Pozitiven stožec P ima eksponent n natanko tedaj, ko je množica $P^\times$ predureditev eksponenta n na polgrupi $D^\times = D \setminus \{0\}$.

Pozitivnim stožcem, ki imajo kak eksponent pravimo *stožci*. Vsak stožec vsebuje 1 in zato ne vsebuje -1. Torej je vsak stožec tudi predstožec. Poljuben eksponent poljubnega stožca je sodo število. V petem poglavju bomo potrebovali tole karakterizacijo stožcev.

Lema 2 *Za poljubno podmnožico P domene D sta ekvivalentni trditvi:*

1. *P je stožec,*

2. *$0 \in P$ in množica $P^\times$ je aditivna predureditev na polgrupi $D^\times$.*

Naj bo μ grupa vseh kompleksnih števil z absolutno vrednostjo 1. Homomorfizem grup $\phi : \ D^\times \to \mu$ je *signatura*, če je množica $\phi^{-1}(1)$ zaprta za seštevanje. Pravimo, da je signatura ϕ *eksponenta* n, če velja $\phi(D^\times) \subseteq \mu_n$. Za poljubno signaturo ϕ je množica $\phi^{-1}(1) \cup \{0\}$ pozitiven stožec. Vsakemu pozitivnemu stožcu take oblike pravimo *cikličen pozitiven stožec.*

Lema 3 *Za poljubno podmnožico P domene D so ekvivalentne trditve:*

1. *P je cikličen stožec.*

2. *$0 \in P$ in množica $P^\times$ je aditivna ciklična predureditev na polgrupi $D^\times$.*

3. *Obstaja taka signatura ϕ na $D^\times$ končnega eksponenta, da velja $P = \sigma^{-1}(1) \cup \{0\}$.*

Odnose med pojmi, ki smo jih uvedli v tem razdelku ponazarja naslednji diagram:

$$\begin{array}{ccccc}
\text{predureditve na} & & \text{stožci na} & & \text{pozitivni stožci} \\
\text{polgrupi } D^\times & \leftarrow & \text{domeni } D & \rightarrow & \text{na domeni } D \\
\uparrow & & \uparrow & & \uparrow \\
\text{ciklične predureditve} & \leftarrow & \text{ciklični stožci} & \rightarrow & \text{ciklični pozitivni} \\
\text{na polgrupi } D^\times & & \text{na domeni } D & & \text{stožci na domeni } D
\end{array}$$

Primer : Naj bo a tako realno število, da je $a > 0$ in $a \neq 1$. Naj bo S polgrupa vseh besed na množici $\{x, y\}$ in naj bo $\mathbb{R}[S]$ pripadajoči polgrupni kolobar nad obsegom realnih števil. Naj bo I dvostranski ideal v kolobarju $\mathbb{R}[S]$ generiran z elementom $yx - axy$ in naj bo $D = R[S]/I$. Kolobar D je Orejeva domena. Pravimo mu kolobar realnih kvantnih polinomov v dveh spremenljivkah.

Vsak element $p \in R$ se da enolično izraziti kot $p = a_0(x)y^k + \ldots + a_{k-1}(x)y + a_k(x)$, kjer $a_0(x), \ldots, a_k(x) \in \mathbb{R}[x]$. Vzemimo poljubno sodo naravno število n Za vsak $p \neq 0$ definirajmo $\sigma(p) = \mathrm{sgn}(a_0(x))e^{2\pi ik/n}$. Tu je $\mathrm{sgn}(a_0(x))$ predznak vodilnega koeficienta polinoma a_0. Trdimo, da je σ signatura eksponenta n na domeni D.

Dokažimo, da je preslikava σ polgrupni homomorfizem. Vzemimo še en element $q = b_0(x)y^l + \ldots + b_{l-1}(x)y + b_l(x)$ kolobarja R. Potem je $pq = c_0(x)y^m + \ldots + c_{m-1}(x)y + c_m(x)$, kjer je $m = k+l$ in vodilni keeficient polinoma $c_0(x)$ je ravno produkt vodilnih koeficientov polinomov $a_0(x)$ in $b_0(x)$ pomnožen z ustrezno potenco števila a. Odtod sledi, da je $\sigma(p)\sigma(q) = \mathrm{sgn}(a_0(x))\mathrm{sgn}(b_0(x))e^{2\pi i(k+l)/n} = \mathrm{sgn}(c_0(x))e^{2\pi im/n} = \sigma(pq)$.

Dokažimo še, da je množica $\sigma^{-1}(1)$ zaprta za seštevanje. Naj bosta $p = a_0(x)y^k + \ldots + a_k(x)$ in $q = b_0(x)y^l + \ldots + b_l(x)$ poljubna elementa množice $\sigma^{-1}(1)$. Ločimo tri možnosti. Če $k < l$, potem imata polinoma $p+q$ in q isti vodilni člen, zato velja $\sigma(p+q) = \sigma(q) = 1$. Če $k > l$, potem imata polinoma $p+q$ in p isti vodilni člen, zato velja $\sigma(p+q) = \sigma(p) = 1$. Če je $k = l$, potem imata polinoma $a_0(x)$ in $b_0(y)$ vodilni koeficient istega predznaka, ki se očitno ujema s predznakom vodilnega koeficienta polinoma $a_0(x) + b_0(x)$. Torej je tudi v tem primeru $\sigma(p + q) = \sigma(q) = 1$.

Zelo podobno bi lahko konstruirali signaturo eksponenta n na Weylovi algebri poljubnega reda. Tudi Weylova algebra je zelo pomembna v kvantni mehaniki.

4.2 Polgrupa Malceva

Pravimo, da polgrupa S zadošča pogoju Z, če za poljubne elemente $a, b, c, d, x, y, u, v \in S$, ki zadoščajo $ax = by$, $cx = dy$ in $au = bv$, velja $cu = dv$.

Lema 4 *Vsaka polgrupa, ki se da vložiti v grupo zadošča pogoju Z.*

Dokaz : Naj bo S podpolgrupa grupe G in naj bodo $a, b, c, d, x, y, u, v \in S$ poljubni elementi, ki zadoščajo $ax = by$, $cx = dy$ in $au = bv$. V grupi G velja $b^{-1}a = yx^{-1}$, $d^{-1}c = yx^{-1}$ in $b^{-1}a = vu^{-1}$. Odtod sledi $d^{-1}c = vu^{-1}$, torej je res $cu = dv$. Q.E.D.

Naj bo S prosta polgrupa nad množico $\{a, b, c, d, x, y, u, v\}$. Elementom polgrupe S pravimo *besede*. število črk v besedi je enolično določeno, pravimo mu *dolžina besede*.

Na polgrupi S definirajmo relacijo $>_t$ s predpisom: $\alpha >_t \beta$ natanko tedaj, ko obstajata taki besedi $\gamma \in S$ in $\delta \in S$, da velja bodisi $\alpha = \gamma ax\delta$ in $\beta = \gamma by\delta$ bodisi $\alpha = \gamma cx\delta$ in

$\beta = \gamma dy\delta$ bodisi $\alpha = \gamma au\delta$ in $\beta = \gamma bv\delta$.

Naj bosta α in β poljubni besedi. Če velja $\alpha >_t \beta$, potem pravimo, da je beseda β *elementarna transformiranka* besede α. Če sta besedi α in β primerljivi glede na relacijo $>_t$, potem pravimo, da sta *elementarno ekvivalentni*. V tem primeru sta α in β iste dolžine.

Beseda β je *transformiranka* besede α, če obstaja končno zaporedje besed, ki se začne z α, konča z β in v katerem je vsaka beseda elementarna transformiranka tiste besede, ki stoji neposredno pred njo. Očitno je relacija "biti transformiranka od" tranzitivna. Če vzamemo v definicijo enoelementno zaporedje, potem vidimo, da je tudi refleksivna.

Besedi α in β sta *ekvivalentni*, če obstaja končno zaporedje besed, ki se začne z α, konča z β in v katerem je vsaka beseda elementarno ekvivalentna s tisto besedo, ki stoji neposredno pred njo.

Relacijo ekvivalence besed označimo z $\sim$. Relacija $\sim$ je kongruenčna relacija, ki ima lastnost levega in desnega krajšanja. Faktorska polgrupa $S/\sim$ je torej polgrupa s krajšanjem. Pravimo ji *polgrupa Malceva*.

Izrek 5 *Polgrupa Malceva se na da vložiti v nobeno grupo.*

Dokaz : Naj bodo A, B, C, D, X, Y, U, V ekvivalenčni razredi besed a, b, c, d, x, y, u, v. Ker velja $AX = BY$, $CX = DY$ in $AU = BV$ in ker ne velja $CU = DV$, polgrupa Malceva nima lastnosti Z. Po lemi 1 se torej polgrupa Malceva ne da vložiti v grupo. Q.E.D.

Spomnimo se, da imata ekvivalentni besedi na polgrupi S glede na relacijo $\sim$ isto dolžino. Torej je za vsak element polgrupe Malceva (= ekvivalenčni razred po relaciji ekvivalence besed) dobro definirana njegova dolžina. Vsak ekvivalenčni razred je končen in v njem obstaja natanko ena beseda, ki ni tranformiranka nobene druge besede. Tej besedi rečemo najstarejša beseda danega ekvivalenčnega razreda. Beseda, ki je najstarejša beseda kakega razreda, ne vsebuje podnizov by, dy in dv.

Naj bo $>_l$ leksikografska urejenost na polgrupi S porojena z $y >_l v >_l x >_l u >_l a >_l b >_l c >_l d$. Natančneje, če je dolžina besede α strogo večja od dolžine besede β, potem je $\alpha >_l \beta$. če pa sta njuni dolžini enaki, potem velja $\alpha >_l \beta$ natanko takrat, ko obstajajo take besede γ, δ, ϵ in taki črki m, n, da velja $\alpha = \gamma m\delta$, $\beta = \gamma n\epsilon$ in $m >_l n$.

Naj bosta A in B poljubna ekvivalenčna razreda po relaciji $\sim$ in naj bosta α oziroma β njuni najstarejši besedi. Definirajmo relacijo $>$ s predpisom $A \geq B \iff \alpha >_l \beta$. Očitno vedno velja bodisi $A > B$ bodisi $B > A$ bodisi $A = B$.

Naslednji izrek pripada Vinogradovu, [14].

Izrek 6 *Vse leve in vse desne translacije na polgrupi Malceva so monotone glede na relacijo* $>$.

Dokaz : Naj bosta A in B poljubna elementa polgrupe Malceva. Naj bo α najstarejša beseda razreda A in naj bo β najstarejša beseda razreda B. Spomnimo se, da besedi α in β ne vsebujeta podnizov by, dy ali bv. Naj bo γ najstarejša beseda razreda AB. Če produkt besed α in β ne vsebuje podniza by, dy ali bv, potem je $\gamma = \alpha\beta$. V nasprotnem primeru je produkt $\alpha\beta$ elementarna transformiranka besede γ.

Naj bodo A, B, C, D taki elementi polgrupe Malceva, da velja $A > B$. Radi bi dokazali, da velja tudi $CA > CB$ in $AD > BD$. Če se dolžini razredov A in B razlikujeta, je trditev očitna. Če sta dolžini enaki, potem se po prejšnjem odstavku lahko omejimo na primer, ko so razredi A, B, C, D dolžine 1. Toraj moramo samo še preveriti, da so vrstice in stolpci v naslednji tabeli padajoči glede na relacijo $>$. (besede by, dy oziroma bv so nadomeščne z besedami ax, cx oziroma au. Mesta, kjer je bila elementarna transformacija izvršena so označena s klicajem.)

	y	v	x	u	a	b	c	d
y	yy	yv	yx	yu	ya	yb	yc	yd
v	vy	vv	vx	vu	va	vb	vc	vd
x	xy	xv	xx	xu	xa	xb	xc	xd
u	uy	uv	ux	uu	ua	ub	uc	ud
a	ay	av	ax	au	aa	ab	ac	ad
b	ax!	au!	bx	bu	ba	bb	bc	bd
c	cy	cv	cx	cu	ca	cb	cc	cd
d	cx!	dv	dx	du	da	db	dc	dd

Q.E.D.

4.3 Domena Malceva

Naj bo $U = S/\sim$ polgrupa Malceva. Namen tega razdelka je pokazati, da je celoštevilski polgrupni kolobar $\mathbb{Z}[U]$ domena. Pravimo ji *domena Malceva*.

V nadaljevanju bomo večkrat uporabili naslednjo lastnost polgrupe Malceva. Naj bo γ poljubna beseda, ki dopušča elementarno transformacijo na mestu $(i, i+1)$. Potem elementarna transformiranka besede γ ne dopušča elementarne transformacije na mestih $(i-1, i)$, $(i, i+1)$ ali $(i+1, i+2)$.

Lema 7 *Naj bodo $\alpha_1, \alpha_2, \beta_1, \beta_2$ take besede, da sta β_1 in β_2 iste dolžine in velja $\alpha_1\beta_1 \sim \alpha_2\beta_2$. Razcepimo $\alpha_1 = \alpha' p_1$ in $\beta_1 = q_1\beta'$, kjer sta α', β' besedi in $p_1.q_1$ črki. Potem obstajata taki črki p_2, q_2, da velja $\alpha_2 \sim \alpha' p_2$, $\beta_2 \sim q_2\beta'$ in $p_1q_1 \sim p_2q_2$.*

Če $p_1q_1 \neq p_2q_2$, potem $p_1q_1, p_2q_2 \in \{ax, by, cx, dy, au, bv\}$.

Dokaz : Naj bo $\alpha_2 = \alpha'' p_1'$, $\beta_2 = q_1'\beta''$. Ker je $\alpha_1\beta_1 \sim \alpha_2\beta_2$, sledi $\alpha' p_1 q_1 \beta' \sim \alpha'' p_1' q_1' \beta''$. Potem je bodisi $\alpha_1 \sim \alpha_2$ in $\beta_1 \sim \beta_2$ bodisi $\alpha' \sim \alpha''$ in $\beta' \sim \beta''$ in $p_1q_1 \sim p_1'q_1'$. V prvem primeru vzamemo $p_2 = p_1$ in $q_2 = q_1$, v drugem pa $p_2 = p_1'$ in $q_2 = q_1'$. Q.E.D.

Trditev 8 *Naj bodo $X_1, X_2, X_3, Y_1, Y_2, Y_3 \in U$ taki element, da velja $X_1Y_1 = X_2Y_2$ in $X_1Y_2 = X_3Y_3$. Če imajo elementi X_1, X_2, X_3 isto dolžino, potem velja bodisi $Y_1 = Y_2$ bodisi $Y_1 = Y_3$.*

Dokaz : Recimo, da obstajajo taki elementi $X_1, X_2, X_3, Y_1, Y_2, Y_3 \in U$, da so elementi X_1, X_2, X_3 iste dolžine in velja $X_1Y_1 = X_2Y_2$, $X_1Y_2 = X_3Y_3$, $Y_1 \neq Y_2$ ter $Y_1 \neq Y_3$.

Naj bodo $\gamma_1, \gamma_2, \gamma_3$ poljubne besede iz razredov X_1, X_2, X_3 in $\delta_1, \delta_2, \delta_3$ poljubne besede iz razredov Y_1, Y_2, Y_3. Naj bo $\gamma_1 = \gamma' m$ in $\delta_1 = n\delta'$, kjer sta γ' in δ' besedi in m, n črki.

Če uporabimo lemo 7 z $\gamma_1, \gamma', m, \gamma_2, m'$ namesto $\alpha_1, \alpha', p_1, \alpha_2, p_2$ in z $\delta_1, \delta', n, \delta_2, n'$ namesto $\beta_1, \beta', q_1, \beta_2, q_2$, potem iz relacije $X_1Y_1 = X_2Y_2$ sledi, da obstajata taki črki m' in n', da velja $\gamma_2 \sim \gamma' m'$, $\delta_2 \sim n'\delta'$ in $mn \sim m'n'$.

Če uporabimo lemo 7 z $\gamma_1, \gamma', m, \gamma_3, p$ namesto $\alpha_1, \alpha', p_1, \alpha_2, p_2$ in z $n'\delta', \delta', n', \delta_3, q$ namesto $\beta_1, \beta', q_1, \beta_2, q_2$, potem iz relacije $X_1Y_2 = X_3Y_3$ in iz $\delta_2 \sim n'\delta'$ sledi, da obstajata taki črki p in q, da velja $\gamma_3 \sim \gamma' p$, $\delta_3 \sim q\delta'$.in $mn' \sim pq$.

Ker je $(n)(\delta') = (\delta_1) = Y_1 \neq Y_2 = (\delta_2) = (n')(\delta')$, sledi $n \neq n'$. Če bi veljalo $m = m'$, potem bi sledilo $X_1 = (\gamma_1) = (\gamma')(m) = (\gamma')(m') = (\gamma_2) = X_2$. Iz $X_1Y_1 = X_2Y_2$ in iz lastnosti krajšanja, bi potem sledilo protislovje $Y_1 = Y_2$. Torej je $m \neq m'$.

Odtod sledi $mn, m'n', mn', pq \in \{ax, by, cx, dy, au, bv\}$. Ker je $m \neq m'$, se n' dvakrat pojavi na drugem mestu, zato je $n' \in \{x, y\}$. Ker je $n \neq n'$, se m dvakrat pojavi na prvem mestu, zato je $m \in \{a, b\}$. Dokazali smo, da je $mn' \in \{ax, by\}$. Če je $mn' = ax$, potem je $mn = au$ in $m'n' = cx$, Če je $mn' = by$, potem je $mn = bv$ in $m'n' = dy$. Oboje je v nasprotju s predpostavko $mn \sim m'n'$. Q.E.D.

Izrek 9 *Kolobar $\mathbb{Z}[U]$ je brez deliteljev niča.*

Dokaz : Recimo, da velja $\sum k_i X_i \sum l_j Y_j = \sum_{i,j} k_i l_j X_i Y_j = 0$. Ker so elementi različnih dolžin ne krajšajo med seboj, sledi, da je vsota najdaljših elementov med tistimi, ki nastopajo v $\sum_{i,j} k_i l_j X_i Y_j$ enaka 0. Toda najdaljši sumandi iz $\sum_{i,j} k_i l_j X_i Y_j$ so produkti najdaljših sumandov iz $\sum k_i X_i$ in iz $\sum l_j Y_j$. Torej lahko predpostavimo, da so v vsoti $\sum k_i X_i$ vsi elementi enake dolžine in v vsoti $\sum l_j Y_j$ prav tako.

Naj bo torej $\sum k_i X_i \sum l_j Y_j = \sum_{i,j} k_i l_j X_i Y_j = 0$, kjer so vsi elementi X_i med seboj različni in enake dolžine. Naj bodo elementi Y_j med seboj različni in enake dolžine. Poleg tega naj bodo števila $k_i l_j$ neničelna. Da bi element $X_1 Y_1$ v kombinaciji z enim ali več členi dal nič, morata obstajati taka indeksa $i \neq 1$ in $j \neq 1$, da velja $X_1 Y_1 = X_i Y_j$. Tu smo uporabili, da ima polgrupa Malceva lastnost krajšanja.

Element $X_1 Y_j$ se razlikuje od elementa X_1, Y_1. Da bi se pokrajšal z nekim drugim elementom, morata obstajati taka indeksa $i' \neq 1$ in $j' \neq j$, da velja $X_1 Y_j = X_{i'} Y_{j'}$. Spet smo uporabili lastnost krajšanja polgrupe Malceva. Po trditvi 8 odtod sledi bodisi $Y_1 = Y_j$ bodisi $Y_J = Y_{j'}$. Obe možnosti sta protislovni z izbiro indeksov j in j'. Torej vsaj ena od vsot $\sum k_i X_i, \sum l_j Y_j$ ne vsebuje neničenlih sumandov. Q.E.D.

Izrek 10 *Domena Malceva se ne da vložiti v obseg.*

Dokaz : Če bi se dal kolobar $\mathbb{Z}[U]$ vložiti v obseg D. potem bi se polgrupa U dala vložiti v multiplikativno grupo obsega D. To je v nasprotju z izrekom 5. Q.E.D.

Izrek 11 *Na domeni Malceva obstajajo ciklični stožci vseh sodih eksponentov.*

Dokaz : Vsak element $x \in \mathbb{Z}[U]$ lahko enolično izrazimo kot $x = \sum_{i=1}^{r} k_i X_i$, kjer je $X_1 > X_2 > \ldots > X_r$. Za poljubno sodo naravno število n definirajmo $\sigma_n(x) = \mathrm{sgn}(k_1) e^{2\pi i d(X_1)}/n$. Tu je $\mathrm{sgn}(k_1)$ predznak števila k_1 in $d(X_1)$ dolžina besede X_1.

Naj bo $y = \sum_{j=1}^{s} l_j Y_j$, kjer je $Y_1 > Y_2 > \ldots > Y_r$. Iz izreka 6 sledi, da je $X_1 Y_1 > X_i Y_j$ za poljubna $i = 1, \ldots, r$ in $j = 1, \ldots, s$, ki nista hkrati enaka 1. Odtod sledi, da je za vsak n preslikava σ_n polgrupni homomorfizem. Če $x, y \in \sigma_n^{-1}(1)$, potem v vsakem od primerov $X_1 > Y_1$, $Y_1 > X_1$ in $X_1 = Y_1$.očitno sledi, da $x+y \in \sigma_n^{-1}(1)$. Torej je za vsak n preslikava σ_n signatura eksponenta n. Q.E.D.

5.

Presečni izreki za domene

Presečni izrek izvira iz Artin-Schreierjeve teorije formalno realnih obsegov in je pomemben del rešitve sedemnajstega Hilbertovega problema. (glej [27], tretji razdelek tretjega poglavja). Zgodovino posplošitev presečnega izreka kaže naslednja tabela.

	eksponent 2	eksponent 2^k	splošno
komutativni obsegi	E. Artin in O. Schreier, [15]	E. Becker [16]	E. Becker [17]
obsegi	T. Szele [21]	T. Craven [23]	V. Powers [24]
domene	R. E. Johnson, [22]		V. Powers, [33] (za superorejeve)

Domnevamo, da je poljuben zaprt stožec končnega eksponenta na poljubni domeni enak preseku vseh cikličnih stožcev, ki ga vsebujejo. Namen tega poglavja je dokazati to domnevo za stožce eksponenta $n = 2^k$ na poljubnih domenah in za poljubne stožce končnega eksponenta na Orejevih domenah ter poenostaviti obstoječ dokaz za obsege.

5.1 Zaprtje stožca

Po lemi 2 iz četrtega poglavja je podmnožica P domene R stožec natanko tedaj, ko $0 \in P$ in ko je množica $P^\times = P \setminus \{0\}$ predureditev na polgrupi $R^\times = R \setminus \{0\}$, ki je zaprta za seštevanje.

Naj bo $\overline{P^\times}$ zaprtje predureditve $P^\times$ na polgrupi $R^\times$. Množici $\overline{P} = \{0\} \cup \overline{P^\times}$ recimo *zaprtje* stožca P. Stožec P je *zaprt*, če je enak svojemu zaprtju, to velja natanko tedaj, ko je $P^\times$ zaprta predureditev na polgrupi $R^\times$. Vsi ciklični stožci in vsi stožci na obsegih so zaprti.

Po lemi 1 iz prvega poglavja velja $\overline{P} = \{x \in R;\ xP^\times \cap P = \emptyset\} = \{x \in R;\ P^\times x \cap P = \emptyset\}$. Kot v izreku 2 iz prvega poglavja dokažemo, da je $\overline{P}$ zaprt stožec na domeni R. Očitno ima množica P permutacijsko lastnost natanko tedaj, ko jo ima tudi množica $P^\times$. Iz izreka 3 iz prvega poglavja sledi, da ima vsak zaprt stožec permutacijsko lastnost.

Izrek 1 *Naj bo R Orejeva domena in D njen obseg ulomkov. Preslikavi $T \to T(T^\times)^{-1}$ in $T' \to T' \cap R$ podajata bijektivno korespondenco med stožci na obsegu D in zaprtimi stožci na domeni R. Ta korespondenca ohranja inkluzije in slika cikl̆ične stožce v cikl̆ične stožce.*

Dokaz : Uporabimo izreka 8 in 9 iz razdelka 2.4 za $Q = D \setminus \{0\}$ in $S = \Sigma = R \setminus \{0\}$, da dobimo bijektivno korspondenco med zaprtimi polgrupnimi predureditvami na S in polgrupnimi predureditvami na Q (te so vedno zaprte). Ta korespondenca spoštuje inkluzije, eksponent predureditve in lastnost cikl̆ičnosti.

Naj bo sedaj T zaprt stožec eksponenta n na R. Potem je množica $T^\times = T \setminus \{0\}$ zaprta polgrupna predureditev na S. Po izreku 8 iz razdelka 2.4 je množica $T^\times(T^\times)^{-1}$ polgrupna predureditev na Q. Kot v dokazu izreka 3 v razdelku 2.2 sledi iz desne Orejeve lastnosti inkluzija $(T^\times)^{-1}T^\times \subseteq T^\times(T^\times)^{-1}$. Obratna inkluzija sledi iz leve Orejeve lastnosti. Iz enakosti $(T^\times)^{-1}T^\times = T^\times(T^\times)^{-1}$ zlahka izpeljemo, da je množica $T^\times(T^\times)^{-1}$ zaprta za seštevanje. Odtod izpeljemo, da je množica $T' = T^\times(T^\times)^{-1} \cup \{0\}$ stožec na obsegu D.

Če je T cikl̆ičen stožec na R, potem je $T^\times$ cikl̆ična polgrupna predureditev na S. Po izreku 9 v 2.4 je množica $T^\times(T^\times)^{-1}$ cikl̆ična polgrupna predureditev na Q. Torej je množica $T' = T^\times(T^\times)^{-1} \cup \{0\}$ cikl̆ičen stožec na obsegu D. Q.E.D.

Odtod takoj sledi, da je presečni izrek za Orejeve domene posledica presečnega izreka za obsege..

5.2 Presečni izrek za eksponent $n = 2^k$

Naj bo R poljubna domena. Stožec $Q \subseteq R$ je *popoln*, če je zaprt in če za vsak element $x \in R$, ki zadošča $x^2 \in Q$, velja $x \in Q \cup -Q$.

Lema 2 *Za poljuben zaprt stožec Q na kolobarju R in poljuben element $x \notin Q^\times$ velja $Q \cap \Sigma(QxQ) = \{0\}$.*

Dokaz : Naj bo Q poljuben zaprt stožec eksponenta n. Recimo, da obstaja tak element $z \in Q \cap \Sigma(QxQ)$, da velja $z \neq 0$. Odtod sledi, da $x \neq 0$. Po permutacijski lastnosti, je $(Qx)^n \subseteq Q$, zato $z^n x = z(z^{n-1}x) \in Q \cdot \Sigma((Qx)^n) \subseteq Q$. Ker je Q zaprt in ker $z^n \in Q^\times$, dobimo $x \in Q$, kar je v nasprotju z izbiro elementa x. Q.E.D.

Lema 3 *Naj bo Q poljuben zaprt stožec eksponenta n. Naj bo $a \in R$ tak element, da velja $a^2 \subseteq Q$ in $a \notin -Q$. Potem je množica $Q[a] := Q + \Sigma(QaQ)$ stožec.*

Dokaz : Ker je stožec Q zaprt, ima permutacijsko lastnost. Zato iz $a^2 \in Q$ sledi, da $aQa \subseteq Q$. Množica $Q[a]$ je zato zaprta za množenje. Očitno je množica $Q[a]$ zaprta za seštevanje in vsebuje množico $\Pi_n(D)$. Če je $Q[a] \cap -Q[a] \neq \{0\}$, potem obstajajo taki elementi $q, q' \in Q$ in $z, z' \in \Sigma(QaQ)$, da velja $q + z = -q' - z' \neq 0$. Odtod sledi po lemi 2, da je $q + q' = -z - z' \in Q \cap \Sigma(Q(-a)Q) = \{0\}$, kar nam da protislovje $q = q' = z = z' = 0$. Torej je množica $Q[a]$ stožec. Q.E.D.

Izrek 4 *Vsak maksimalen stožec je popoln.*

Dokaz : Naj bo Q poljuben maksimalen stožec. Ker je $\overline{Q}$ stožec, ki vsebuje Q, velja $Q = \overline{Q}$. Naj bo $a \in R$ tak element, da $a^2 \in Q$ in $a \notin -Q$. Po lemi 3 je množica $Q + \Sigma(QaQ)$ stožec, ki vsebuje Q. Odtod sledi, da je $a \in \Sigma(QaQ) \subseteq Q$. Torej je stožec Q popoln. Q.E.D.

Izrek 5 *Vsak popoln stožec, katerega strogi eksponent je potenca števila 2, je cikličen.*

Dokaz : Naj bo P popoln stožec strogega eksponenta $n = 2^k$. Zaradi permutacijske lastnosti obstaja tak element $a \in R$, da velja $a^{2^{k-1}} \notin P$. Ker je stožec P popoln, je $-a^{2^{k-1}} \in P$.

Prvi korak : Za vsak element $x \in R$ obstaja tako naravno število l, da velja $xa^l \in P$.

Naj bo k_0 najmanjše naravno število, ki zadošča $x^{2^{k_0}} \in P$. Če je $k_0 = 0$, potem $x \in P$ in lahko vzamemo $l = 0$. Če je $k_0 > 0$, potem je $-x^{2^{k_0-1}} \in P$. Odtod sledi $a^{2^{k-1}} x^{2^{k_0-1}} \in P$. Zaradi permutacijske lastnosti odtod sledi $(a^{2^{k-k_0}} x)^{2^{k_0-1}} \in P$. Naj bo k_1 najmanjše naravno število, ki zadošča $(a^{2^{k-k_0}} x)^{2^{k_1}} \in P$. Očitno je $k_1 < k_0$. Če je $k_1 = 0$, potem lahko vzamemo $l = 2^{k-k_0}$. Če je $k_1 > 0$, potem je $-(a^{2^{k-k_0}} x)^{2^{k_1-1}} \in P$. Odtod sledi $a^{2^{k-1}} (a^{2^{k-k_0}} x)^{2^{k_1-1}} \in P$. Zaradi permutacijske lastnosti odtod sledi $(a^{2^{k-k_1}} a^{2^{k-k_0}} x)^{2^{k_1-1}} \in P$. Naj bo k_2 najmanjše število, za katerega velja $(a^{2^{k-k_1}} a^{2^{k-k_0}} x)^{2^{k_2}} \in P$. Če je $k_2 = 0$, potem lahko vzamemo $l = 2^{k-k_1} + 2^{k-k_0}$. Če $k_2 \neq 0$, potem s ponavljanjem gornjega postopka konstruiramo naravna števila $k_3 > \ldots > k_i = 0$, kjer je $i \leq k$. Potem lahko vzamemo $l = 2^{k-k_i} + \ldots + 2^{k-k_1} + 2^{k-k_0}$.

Drugi korak : Če je $x \in R \setminus \{0\}$, $xa^l \in P$ in $xa^m \in P$, potem eksponent n deli število $l - m$.

Brez škode lahko predpostavimo, da je $m > l$. Ker je $xa^l \in P$ in $(xa^l)a^{m-l} \in P$ in ker je stožec P zaprt, je $a^{m-l} \in P$. Odtod sledi $n = 2^k | m - l$.

Prvi in drugi korak nam omogočata, da definiramo preslikavo $\phi : R \to \mathbb{Z}_n$ s predpisom $\phi(x) = 0$, če $x = 0$ in $\phi(x) = e^{2\pi i/l}$, če $x \neq 0$ in $xa^l \in P$.

Tretji korak : Preslikava ϕ je polgrupni homomorfizem in $P^\times = \phi^{-1}(1)$.

Vzemimo poljubna elementa $x, y \in R$. Če je vsaj eden od njiju enak nič, potem je trditev očitna. Če sta oba neničelna, potem obstajata taki naravni števili l in m, da velja $xa^l \in P$ in $ya^m \in P$. Odtod sledi $xa^l ya^m \in P$. Iz permutacijske lastnosti dobimo $xya^{l+m} \in P$, torej je ϕ res polgrupni homomorfizem. Zadnje trditev je posledica zaprtosti stožca P. Q.E.D.

Izrek 6 *Vsak zaprt stožec, katerega strogi eksponent je potenca števila 2, je enak preseku vseh cikličnih stožcev, ki ga vsebujejo.*

Dokaz : Naj bo T poljuben zaprt stožec eksponenta 2^k in naj bo I presek vseh cikličnih stožcev, ki ga vsebujejo. Očitno je $T \subseteq I$.

Če $I \not\subseteq T$, potem obstaja element $z \in I \setminus T$. Vzemimo tako naravno število r, da $z^{2^r} \in T$ in $z^{2^{r-1}} \notin T$ in pišimo $u = z^{2^{r-1}}$ in $T[-u] = T - \Sigma(TuT)$.

Če je množica $T[-u]$ stožec, potem je po Zornovi lemi vsebovana v nekem maksimalnem stožcu Q. Po izrekih 4 in 5 je stožec Q cikličen. Očitno je $-u \in T[-u] \subseteq Q$ in $u \in I \subseteq Q$. Odtod sledi protislovje $u = 0$ z izbiro u.

Če množica $T[-u]$ ni stožec, potem je $T[-u] \cap -T[-u] \neq \{0\}$. Obstajajo torej taki elementi $t, t' \in T$ in $z, z' \in \Sigma(TuT)$, da velja $t - z = -(t' - z') \neq 0$. Po lemi 2 je $z + z' = t + t' \in T \cap \Sigma(TuT) = \{0\}$. Odtod sledi protislovje $t = t' = z = z' = 0$. Q.E.D.

5.3 Presečni izrek za popolne stožce

Ta in naslednji razdelek sta posvečena dokazu presečnega izreka za obsege. Lema in izrek iz tega razdelka sta posplošitvi leme 1.3 in izreka 1.4 iz [17]. V nadaljevanju nam bosta zadoščala že originalna rezultata, posplošitvi utegneta pomagati pri dokazu splošnega presečnega izreka.

Lema 7 *Za vsako zaprt stožec P, ki ni popoln, velja $P = \bigcap \overline{P[a]}$, kjer presek teče po vseh elementih $a \in R$, za katere velja $a^2 \in P$ in $a \notin P \cup -P$.*

Dokaz : Ker stožec P ni popoln, je presek neprazen. Če trditev ne drži, potem obstaja nek element $c \in \bigcap \overline{P[a]} \setminus P$. Vzemimo poljuben element $a \in R$, ki zadošča $a^2 \in P$ in $a \notin P \cup -P$. Ker tudi element $-a$ zadošča tem dvem lastnostim, je $c \in \overline{P[a]} \cap \overline{P[-a]}$. Obstajata torej taka elementa $s \in P[a]^\times$ in $t \in P[-a]^\times$, da velja $sc \in P[a]$ in $ct \in P[-a]$. Sledi $s^n, t^n \in \Pi_n \setminus \{0\} \subseteq P^\times$ ter $s^n c \in P[a]$ in $ct^n \in P[-a]$, torej je $b := s^n c t^n \in P[a] \cap P[-a]$.

Trdimo, da element b zadošča $b^2 \in P$ in $b \notin P \cup -P$.

Ker je P zaprta in ker $c \notin P$, je $b \notin P$.

Ker je $b \in P[a] \cap P[-a]$, obstajajo taki elementi $p_0, q_0 \in P$ in $p_1, q_1 \in \Sigma(PaP)$, da velja $b = p_0 + p_1 = q_0 - q_1$.

Če je $b \in -P$, potem je po lemi 2 $q_1 = q_0 - b \in P \cap \Sigma(PaP) = \{0\}$. Sledi $b = q_0 - q_1 = q_0 \in P$. Iz tega protislovja izhaja $b \notin -P$.

Privzemimo, da $b^2 \notin P$. Označimo $r_1 := p_0^2 + p_1^2 \in P$, $r_2 := p_0 p_1 + p_1 p_0 \in \Sigma(PaP)$, $r_3 := q_0^2 + q_1^2 \in P$ in $r_4 := q_0 q_1 + q_1 q_0 \in \Sigma(PaP)$. Imamo $b^2 = r_1 + r_2$ in $b^2 = r_3 - r_4$. Ker je $b^2 \notin P$, imamo $r_2, r_4 \neq 0$. Iz $aPa \subseteq P$ sledi $b^2 a r_4 + r_2 a b^2 = r_1 a r_4 + r_2 a r_3 \in P \cap P b^2 P$. Iz $b^2 \notin P$ in leme 2 sledi $P \cap \Sigma(P b^2 P) = \{0\}$, odtod pa $b^2 a r_4 = r_2 a b^2 = 0$. To je protislovje, saj $b^2, a, r_2, r_4 \neq 0$.

Iz lastnosti $b \notin P \cup -P$ in $b^2 \in P$ sledi, da $-b \notin P \cup -P$ in $(-b)^2 \in P$. Po izbiri element c pripada množici $\overline{P[-b]}$, zato obstaja tak element $z \in P[-b]^\times$, da velja $cz \in P[-b]$. Odtod sledi, da $z^n \in P^\times$ in $cz^n \in P[-b] \subseteq P[-c]$. Naj bo $cz^n = s_0 - s_1$, kjer $s_0 \in P$ in

$s_1 \in \Sigma(PcP)$ zadoščata $cz^n = s_0 - s_1$. Očitno je $cz^n + s_1 = s_0 \in P \cap \Sigma(PcP) = \{0\}$ po lemi 2. Ker $c^n z^n \in P$, $c^{n-1} s_1 \in P$ in $c^n z^n + c^{n-1} s_1 = 0$ sledi, da $c^n z^n = 0$. Torej $c = 0$ ali $z = 0$. Oboje da protislovje. Q.E.D.

Izrek 8 *Vsak zaprt stožec je enak preseku vseh popolnih stožcev, ki ga vsebujejo.*

Dokaz : Naj bo T zaprt stožec, ki ni popoln in $x \notin T$ poljuben element. Zadošča, da konstruiramo tak popoln stožec S, da velja $T \subseteq S$ in $x \notin S$.

Družina $\mathcal{M} = \{P \ ; \ P$ tak zaprt stožec, da $T \subseteq P$ in $x \notin P\}$ je neprazna saj vsebuje stožec T. Pokažimo, da izpolnjuje predpostavko Zornove leme.

Naj bo $(P)_{\lambda \in \Lambda}$ naraščajoča veriga elementov družine $\mathcal{M}$ in naj bo Q unija te verige. Očitno je Q stožec, ki vsebuje T in ki ne vsebuje x. Pokažimo še, da je stožec Q zaprt. Če $z \in \overline{Q}$, potem obstaja tak $t \in Q^\times$, da velja $tz \in Q$. Odtod sledi $t^n \in \Pi_n \setminus \{0\}$ in $t^n z \in Q$. Vzemimo tak $\lambda \in \Lambda$, da velja $t^n z \in P_\lambda$. Ker je $t^n \in \Pi_n \setminus \{0\} \subseteq P_\lambda^+$, in ker je P_λ zaprt stožec, sledi $z \in P_\lambda \subseteq Q$.

Naj bo S poljuben maksimalen element te družine. Če S ni popoln stožec, potem je po lemi 7 $S = \bigcap \overline{S[a]}$, kjer presek teče po vseh elementih a, ki zadoščajo $a^2 \in S$ in $a \notin S \cup -S$. Toda element x je vsebovan v vsaki množici $\overline{S[a]}$ iz preseka, saj so te zaprti stožci, ki strogo vsebujejo stožec S. Q.E.D.

5.4 Valuacijski kolobar popolnega stožca

Lema 9 *Naj bo P popoln stožec na domeni R, Potem velja*

1. $\mathrm{A}(P) \subseteq \mathrm{Arch}(P) \cup -\mathrm{Arch}(P)$.
2. $\mathrm{A}(P) \cap \mathrm{Arch}(P) = (\mathrm{A}(P) \cap P) \cup \mathrm{I}(P)$.
3. $\mathrm{A}(P) \subseteq P \cup -P \cup \mathrm{I}(P)$.

Dokaz : Za dokaz prve točke vzemimo poljuben element $a \in \mathrm{A}(P)$. Naj bo m najmanjše tako naravno število, da $a^m \in P$. Razcepimo $m = 2^r s$, kjer je s liho število. Če je $r = 0$, potem po točki 2 izreka 14 iz razdelka 3.4 sledi, da $a \in \mathrm{Arch}(P)$. Če je $r = 1$, potem $a^s \in -P$, torej $a \in -\mathrm{Arch}(P)$. Če je $r > 1$, potem $a^{2^{r-1}s} \in -P$. Po točki 1 izreka 14 iz

razdelka 3.4 je $a^{2^{r-1}s} = (a^{2^{r-2}s})^2 \in \mathrm{Arch}(P)$. Po točki 3 izreka 14 iz razdelka 3.4 je $\mathrm{I}(P)$ reduciran ideal v $\mathrm{A}(P)$. Torej iz $a^{2^{r-1}s} \in \mathrm{Arch}(P) \cap -P \subseteq \mathrm{I}(P)$ sledi, da $a \in \mathrm{I}(P)$.

Inkluzija $(\mathrm{A}(P) \cap P) \cup \mathrm{I}(P) \subseteq \mathrm{A}(P) \cap \mathrm{Arch}(P)$ v drugi točki je očitna. Za dokaz nasprotne inkluzije vzemimo poljuben element $a \in \mathrm{A}(P)$, ki pripada množici $\mathrm{Arch}(P) \setminus P$. Vzemimo poljuben $k \in \mathbb{N}$. Ker je $2ka - 1 \notin \mathrm{Arch}(P)$, sledi po prvi točki, da $1 - 2ka \in \mathrm{Arch}(P)$, torej je $2(1 - ka) = 1 + (1 - 2ka) \in 1 + \mathrm{Arch}(P) \subseteq P$. Ker je k poljuben, je $-a \in \mathrm{Arch}(P)$. Torej je res $a \in \mathrm{I}(P)$.

Tretja točka sledi iz prvih dveh. Q.E.D.

Naslednji izrek je iz [17], izrek 2.2.

Izrek 10 *Naj bo P popoln stožec na komutativnem obsegu K. Potem je množica $\mathrm{A}(P)$ valuacijski kolobar v K.*

Dokaz : Naj bo n poljuben eksponent stožca P.

Prvi korak : $\mathrm{A}(P)$ je lokalen kolobar in $\mathrm{I}(P)$ je njegov maksimalen ideal.

Zadošča dokazati, da je poljuben element $a \in \mathrm{A}(P) \setminus P$ obrnljiv v $\mathrm{A}(P)$. Naj bo $a \notin \mathrm{I}(P)$ poljuben element. Naj bo $b = a^n$. Ker je $\mathrm{I}(P)$ reduciran ideal, je $b \notin \mathrm{I}(P)$. Obstaja torej tak $m \in \mathbb{N}$, da $\frac{1}{m} - b \notin P$. Odtod sledi, da $\frac{1}{2m} - b \notin \mathrm{Arch}(P)$. Po točki 1 leme 9 mora biti $b - \frac{1}{2m} \in \mathrm{Arch}(P)$. Po definiciji množice $\mathrm{Arch}(P)$ sledi $b - \frac{1}{4m} = (b - \frac{1}{2m}) + \frac{1}{4m} \in P$ odtod pa $b \in P$ in $b + \frac{1}{4m} \in P$. Po množenju z $4mb^{-1}$ dobimo $4m \pm b^{-1} \in P$, kar po definiciji pomeni, da $b^{-1} \in \mathrm{Arch}(P)$. Odtod sledi, da je element a obrnljiv v $\mathrm{A}(P)$.

Drugi korak : Za vsak element $a \in P$ velja bodisi $a \in \mathrm{A}(P)$ bodisi $a^{-1} \in \mathrm{A}(P)$.

Ker velja $1 - \frac{a}{1+a} = \frac{1}{1+a} \in P$ in $1 - \frac{1}{1+a} = \frac{a}{1+a} \in P$, sledi $\frac{1}{1+a}, \frac{a}{1+a} \in \mathrm{A}(P)$. Ker je njuna vsota 1 ne moreta biti elementa $\frac{1}{1+a}$ in $\frac{a}{1+a}$ oba v $\mathrm{I}(P)$, Ker je $\mathrm{A}(P)$ lokalen kolobar, je vsaj eden od njiju obrnljiv. Če je $\frac{1}{1+a}$ obrnljiv, sledi $a \in \mathrm{A}(P)$. Če je $\frac{a}{1+a}$ obrnljiv, sledi $a^{-1} \in \mathrm{A}(P)$.

Tretji korak : Kolobar $\mathrm{A}(P)$ je celostno zaprt v K.

Ideal $\mathrm{I}(P)$ kolobarja $\mathrm{A}(P)$ je vsebovan v maksimalnem idealu M celostnega zaprtja $B = \overline{\mathrm{A}(P)}$. Recimo, da obstaja tak element $a \in B$, da $a^n \notin \mathrm{A}(P)$. Po drugem koraku odtod sledi, da $a^{-n} \in \mathrm{A}(P)$. Ker je $\mathrm{A}(P)$ lokalen kolobar, sledi $a^{-n} \in \mathrm{I}(P) \subseteq M$. Ker je M ideal v B in $a^n \in B$, dobimo protislovje $1 \in M$. Torej za vsak element $a \in B$ velja $a^n \in \mathrm{A}(P)$. Odtod sledi, da velja $a = \frac{1}{n!} \sum_i (-1)^{n-i-1} \binom{n-1}{i} ((z+i)^n - i^n) \in \mathrm{A}(P)$ za vsak element $a \in B$.

Četrti korak : $\mathrm{A}(P)$ *je valuacijski kolobar v* K.

Vzemimo poljuben element $a \in K$. Po drugem koraku je bodisi $a^n \in \mathrm{A}(P)$, bodisi $a^{-n} \in \mathrm{A}(P)$. Po tretjem koraku odtod sledi, da je bodisi $a \in \mathrm{A}(P)$ bodisi $a^{-1} \in \mathrm{A}(P)$. Q.E.D.

Naslednji izrek je iz [45], trditev 2.5.

Izrek 11 *Naj bo* P *popoln stožec na obsegu* D. *Potem je množica* $\mathrm{A}(P)$ *valuacijski kolobar v* D.

Dokaz : Naj bo P popoln stožec na na obsegu D. Vzemimo poljuben element $d \in D$. Obseg $\mathbb{Q}(d)$ je komutativen in vsebuje podkolobar $\mathrm{A}(P) \cap \mathbb{Q}(d) = \mathrm{A}(P \cap \mathbb{Q}(d))$. Toda $P \cap \mathbb{Q}(d)$ je popoln stožec na $\mathbb{Q}(d)$. Po izreku 10 je $\mathrm{A}(P \cap \mathbb{Q}(d))$ valuacijski kolobar v $\mathbb{Q}(d)$. Odtod sledi, da je bodisi $d \in \mathrm{A}(P \cap \mathbb{Q}(d)) \subseteq \mathrm{A}(P)$ bodisi $d^{-1} \in \mathrm{A}(P \cap \mathbb{Q}(d)) \subseteq \mathrm{A}(P)$. Torej je $\mathrm{A}(P)$ res valuacijski kolobar v D. Q.E.D.

Dokaz izreka 12 je podoben dokazu leme 4.1 v [18].

Izrek 12 *Naj bo* P *popoln stožec na obsegu* D *in* U *poljubna podpolgrupa grupe* $D^\times$, *ki vsebuje* $P^\times$ *in ne vsebuje* -1. *Potem je* U *zaprta za seštevanje.*

Dokaz : Ker je $\Pi_n(D^\times) \subseteq P^\times \subseteq U$, velja za vsak element $u \in U$, da $u^{-1} = u^{n-1}(u^{-1})^n \in U \cdot U \subseteq U$. Torej je U podgrupa grupe $D^\times$. Iz $-1 \notin U$ sledi $U \cap -U = \emptyset$.

Vzemimo poljubna elementa $x, y \in U$. Ker je množica $\mathrm{A}(P)$ valuacijski kolobar v D z maksimalnim idealom $\mathrm{I}(P)$, velja bodisi $x^{-1}y \in \mathrm{I}(P)$ bodisi $y^{-1}x \in \mathrm{A}(P)$. Po prvi točki leme 9 je $\mathrm{A}(P) \subseteq P \cup -P \cup \mathrm{I}(P)$.

Če je $x^{-1}y \in \mathrm{I}(P)$, potem je $x + y = x(1 + x^{-1}y) \in U \cdot P^\times \subseteq U$. Če je $y^{-1}x \in \mathrm{I}(P)$, potem je $x + y = y(1 + y^{-1}x) \in U$. Če je $y^{-1}x \in P^\times$, potem je $x = yp$ za nek $p \in P^\times$, torej je $x + y = yp + y = y(p + 1) \in U$. Če je $y^{-1}x \in -P^\times$, potem je $x = -yp$ za nek $p \in P^\times$, torej je presek $U \cap -U$ neprazen, kar je protislovje. Q.E.D.

Naslednji izrek sledi iz posledice 16 v prvem poglavju in iz izreka 12.

Izrek 13 *Poljuben popoln stožec na poljubnem obsegu je enak preseku vseh cikličnih stožcev, ki ga vsebujejo.*

Iz izrekov 8 in 13 sledi presečni izrek za obsege.

6.

Positivstellensatz

Nullstellensatz za kolobar realnih polinomov pripada Duboisu in Rieslerju. V Prestelovem dokazu Nullstellensatza nastopa Positivstellensatz kot pomožna lema, glej izrek 3.3 in lemo 3.4 v [27].

Dve smeri posploševanja Positivstellensatza opisuje naslednja tabela.

	eksponent 2	eksponent 2^k	splošno
komutativni kolobarji	G. Stengle [28]	E. Becker in D. Gondard, [29]	R. Berr [30]
asociativni kolobarji	K.H. Leung, M. Marshall, in Y. Zhang, [32]		

Namen tega poglavja je dokazati Positivstellensatz za ureditve eksponenta $n = 2^k$ na poljubnih asociativnih kolobarjih in za ureditve poljubnega eksponenta na Noetherskih kolobarjih.

6.1 Predureditve in ureditve na kolobarjih

Naj bo R poljuben asociativen kolobar z enico in n poljubno naravno število. Kot pri polgrupah označimo $\Pi_n(R) = \{r \in R$; obstaja tako naravno število $k \in \mathbb{N}$ in taki elementi $r_1, \ldots, r_k \in R$, da je r produkt n kopij elementa r_1, ..., n kopij elementa $r_k\}$. Na primer za poljubna elementa $x, y \in R$ velja $xyxy \in \Pi_2(R)$.

Ker bo kolobar R v nadaljevanju fiksen bomo pisali kar Π_n namesto $\Pi_n(R)$. Označimo z Σ_n množico, ki je aditivno generirana z množico Π_n.

Predstožec T imenujemo *predureditev*, če obstaja tako naravno število n, da velja $\Pi_n \subseteq T$. To število imenujemo *eksponent* predureditve T. Na kolobarju R obstaja kaka predureditev eksponenta n natanko tedaj, ko $-1 \notin \Sigma_n$.

Eksponent predureditve ni enolično določen, kajti vsak večkratnik vsakega ekponenta je tudi eksponent. Vsak eksponent je sodo število. Najmanjšemu eksponentu dane predureditve T pravimo *strogi eksponent* predureditve T. Polovici strogega eksponenta pravimo *red* predureditve T.

Spomnimo se, da je predureditev T izolirana, če je $T = T^e$ in usmerjena, če je $T - T = R$.

Lema 1 *Vsaka izolirana predureditev je usmerjena.*

Dokaz : Naj bo T izolirana predureditev eksponenta n na kolobarju R. Znano je, da za vsak element $r \in R$ velja identiteta $n!r = \sum_{i=0}^{n-1}(-1)^{n-i-1}\binom{n-1}{i}((r+i)^n - i^n)$. Za vsak element $r \in R$ obstajata torej taka elementa $s, t \in \Sigma_n \subseteq T$, da velja $n!r = s - t$. Odtod sledi $n!(r+t) = s + (n!-1)t \in T$. Ker je predureditev T izolirana, je $r + t \in T$. To nam da $r = (r+t) - t \in T - T$. Torej je res $R = T - T$. Q.E.D.

Torej je nosilec vsake izolirane predureditve pravi dvostranski ideal v kolobarju R. Za vsako predureditev T eksponenta n je množica T^e usmerjena predureditev eksponenta n.

Naj bo μ množica vseh kompleksnih števil z dolžino 1.

Lema 2 *Za vsak polgrupni homomorfizem $\phi : R \to \mu \cup \{0\}$ sta ekvivalentni trditvi:*

1. *Velja $\phi(-1) = -1$ in množica $\phi^{-1}(\{0,1\})$ je zaprta za seštevanje.*

2. *Množica $\phi^{-1}(\{0,1\})$ je predstožec na R.*

Dokaz : Očitno iz 1. sledi 2., saj je praslika multiplikativne množice multiplikativna.

Dokažimo nasprotno smer. Naj bo $\phi : R \to \mu \cup \{0\}$ polgrupni homomorfizem in naj bo množica $P := \phi^{-1}(\{0,1\})$ predstožec.

Dokažimo najprej, da je $\phi(1) = 1$. Iz $\phi(1)^2 = \phi(1^2) = \phi(1)$ sledi bodisi $\phi(1) = 0$ ali $\phi(1) = 1$. V prvem primeru bi za vsak $x \in R$ veljalo $\phi(x) = \phi(x \cdot 1) = \phi(x)\phi(1) = 0$, kar je v nasprotju s predpostavko $-1 \notin P$.

Dokažimo sedaj, da je $\phi(-1) = -1$. Iz $\phi(-1)^2 = \phi((-1)^2) = \phi(1) = 1$ sledi bodisi $\phi(-1) = -1$ bodisi $\phi(-1) = 1$. Druga možnost je v nasprotju s predpostavko $-1 \notin P$. Torej iz 2. res sledi 1. Q.E.D.

Polgrupni homomorfizem $\phi : R \to \mu \cup \{0\}$ je *signatura*, če je množica $\phi^{-1}(\{0,1\})$ predstožec. Predstožec P je *cikličen*, če obstaja tak polgrupni homomorfizem ($\Leftrightarrow$ signatura) $\phi : R \to \mu \cup \{0\}$, da velja $P = \phi^{-1}(\{0,1\})$. Nosilec cikličnega predstožca je popoln praideal.

Lema 3 *Za poljubno signaturo ϕ na kolobarju R in za poljubno naravno število n sta ekvivalentni trditvi.*

1. $\phi(R) \subseteq \mu_n \cup \{0\}$,

2. *Predstožec $\phi^{-1}(\{0,1\})$ je predureditev eksponenta n,*

Pravimo, da je signatura ϕ *končnega eksponenta*, če obstaja tako naravno število n (*eksponent signature*), da velja $\phi(R) \subseteq \mu_n \cup \{0\}$. Pravimo, da je dana predureditev *ciklična*, če je ciklična kot predstožec. Cikličnim predureditvam pravimo tudi *ureditve*. Spomnimo se, da predureditvam z nosilcem $\{0\}$ pravimo stožci.

Odnosi med pojmi definiranimi v tem razdelku in v razdelkih 4.1 in 5.1 so:

$$\begin{array}{ccc} \text{ciklični stožci} & \subset & \text{stožci} \\ \cap & & \cap \\ \text{ciklične predureditve} & \subset & \text{predureditve} \\ \cap & & \cap \\ \text{ciklični predstožci} & \subset & \text{predstožci} \end{array}$$

6.2 Osnovni izrek

Naj bo n poljubno naravno število. Podmnožico $U \subset \Pi_n$ imenujemo Π_n-*sistem*, če $1 \in U$ in če za poljubna elementa $x, y \in U$ obstaja tak element $c \in \Pi_n$, da velja $xcy \in U$. Primeri Π_n sistemov so multiplikativne podmnožice v Π_n, ki vsebujejo enico.

Množica T je *krepka predureditev eksponenta n*, če je predureditev eksponenta n in če velja $(rT)^n \subseteq T$ za vsak element $r \in R$.

Izrek 4 *Naj bo R poljuben asociativen kolobar z enico. Naj bo T krepka predureditev eksponenta n. Naj bo U tak Π_n-sistem in M tak modul nad T, da velja $-U \cap M = \emptyset$.*

Naj bo S tak modul nad T, ki vsebuje M in ki je maksimalen glede na relacijo $-U \cap S = \emptyset$. (Obstaja po Zornovi lemi.) Potem je $S \cup -S = R$ in $S \cap -S$ je popoln praideal.

Dokaz : Naj bo $J = S \cap -S$. Ker je S maksimalen modul nad T, je $S = S^e$. Iz leme 1 sledi, da je J pravi dvostranski ideal v kolobarju R.

Prvi korak : Za poljuben element $a \in R$ iz predpostavke $aTa \subseteq J$ sledi $a \in J$.

Recimo, da obstaja tak element $a \in R$, da velja $aTa \subseteq J$ in $a \notin J$. Brez škode lahko predpostavimo, da $a \notin S$. Ker modul $S + \Sigma(TaT)$ strogo vsebuje množico S, mora sekati množico $-U$. Odtod sledi, da obstajajo taki elementi $v \in U$, $m \in S$ in $z \in \Sigma(TaT)$, da velja $-v = m + z$. Ker je U Π_n-sistem, obstajajo taki elementi $c_1, \ldots, c_{n-1} \in \Pi_n$, da velja $u = vc_1vc_2v \cdots c_{n-1}v \in U$. Odtod sledi $(v+z)c_1(v+z)c_2 \cdots (v+z) = u + x + y$, kjer je $x = zc_1vc_2 \cdots v + vc_1zc_2 \cdots v + \ldots + vc_1vc_2 \cdots z$ in $y \in \Sigma(RzTzR) \subseteq \Sigma(RaTaR) \subseteq J$. Velja $x = (-m-v)c_1vc_2 \cdots v + vc_1(-m-v)c_2 \cdots v + \ldots + vc_1vc_2 \cdots (-m-v) = -nu - m'$, kjer je $m' = mc_1vc_2v \cdots c_{n-1}v + vc_1mc_2v \cdots c_{n-1}v + \ldots + vc_1vc_2v \cdots c_{n-1}m \in S$. To nam da $-u = (u + x + y) + (n-2)u + m' - y \in T + T + S + J \subseteq S$, kar je protislovje s predpostavko $-U \cap S = \emptyset$.

Drugi korak : $S \cup -S = R$.

Recimo, da obstaja element $a \notin S \cup -S$. Potem modula $S + \Sigma(TaT)$ in $S - \Sigma(TaT)$ strogo vsebujeta modul S in zato sekata množico $-U$. Obstajajo torej taki elementi $u, v \in U$, $m_1, m_2 \in M$ in $z, w \in \Sigma(TaT)$, da velja $-u = m_1 + z$ in $-v = m_2 - w$. Ker je množica U Π_n-sistem, obstaja tak element $c \in \Pi_n$, da velja $ucv \in U$. Naj bo $z' = zcv \in \Sigma(TaT)$. Vzemimo poljubne elemente $c_1, \ldots, c_{n-1} \in T$ in označimo $t_1 := vc_1z'c_2z' \cdots z'c_{n-1}zcw$ in $t_2 := z'c_1z'c_2 \cdots z'c_{n-1}z$. Ker je predureditev T krepka, je $t_1, t_2 \in (\Sigma(TaT))^n \subseteq T$. Iz $zct_1 = t_2cw$ sledi, da $-uct_1 - t_2cv = (m_1 + z)ct_1 + t_2c(m_2 - w) = m_1ct_1 + t_2cm_2 \subseteq S$. Odtod dobimo $z'c_1z'c_2 \cdots z'c_{n-1}z' = t_2cv \in J$ za poljubne elemente $c_1, \ldots, c_{n-1} \in T$. Ker je $2^n \geq n + 1$, lahko izberemo poljubne elemente $c_n, \ldots, c_{2^n-1} \in T$. Ker je J ideal, je $z'c_1z'c_2 \cdots z'c_{2^n-1}z' \in J$. Po n-kratni uporabi prvega koraka vidimo, da $z' \in J$. To nam da protislovje $-ucv = m_1cv + z' \in -U \cap S = \emptyset$.

Tretji korak : Za vsak element $a \in R$ iz $a^2 \in J$ sledi $a \in J$.

Ker je po drugem koraku $S \cup -S = R$, lahko predpostavimo, da $a \in S$. Vzemimo poljuben element $x \in T$. Velja $ax \in S$, $xa \in S$, $(ax)^n \in T$ in $(xa)^n \in T$. Ločimo dve

možnosti. Če $ax - xa \in S$, potem $(xa)^n(ax - xa) \in S$. Toda $(xa)^n ax \in Ra^2R \subseteq J$ in $(xa)^{n+1} \in T \cdot S \subseteq S$, kar nam da $(xa)^{n+1} \in J$. Če $xa - ax \in S$, potem $(xa - ax)(ax)^n \in J$. Toda $xa(ax)^n \in Ra^2R \subseteq J$ in $(ax)^{n+1} \in S$. Podobno kot zgoraj dobimo $(ax)^{n+1} \in J$. Ker je J ideal in ker $2n > n + 1$, dobimo v obeh primerih $(ax)^{2n-1}a \in J$

Vzemimo sedaj poljubne elemente $c_1, \ldots, c_{2n-1} \in T$. Po prejšnjem odstavku je

$$\sum_{1 \leq j_1, \ldots, j_{2n-1} \leq 2n-1} ac_{j_1} a \cdots c_{j_{2n-1}} a = (a(c_1 + \ldots + c_{2n-1}))^{2n-1} a \in J.$$

Ker je T krepka predureditev, vsak sumand v gornji vsoti pripada $T \subseteq S$, zato morajo vsi sumandi ležati v J. Med drugim odtod sledi, da $ac_1 a \cdots c_{2n-1} a \in J$ za poljubne elemente $c_1, \ldots, c_{2n-1} \in T$. Z večkratno uporabo prvega koraka odtod sledi kot ob koncu drugega koraka, da $a \in J$.

Četrti korak : Ideal J je popoln praideal.

Naj bosta $a, b \in R$ taka elementa, da $ab \in J$. Ker je J ideal, sledi $a^n b^n \in J$. Ločimo dve možnosti. Če je $a^n - b^n \in S$, potem $-b^{2n} = (a^n - b^n)b^n - a^n b^n \in S$. Če je $b^n - a^n \in S$, potem $-a^{2n} = a^n(b^n - a^n) - a^n b^n \in S$. Torej bodisi $a^{2n} \in J$ bodisi $b^{2n} \in J$. Ker je $2^n \geq 2n$ in ker je J ideal, je bodisi $a^{2^n} \in J$ bodisi $b^{2^n} \in J$. Če n-krat uporabimo tretji korak, vidimo, da bodisi $a \in J$ bodisi $b \in J$. Q.E.D.

V nadaljevanju bomo potrebovali tole posledico osnovnega izreka:

Izrek 5 *Naj bo T poljubna predureditev eksponenta n in naj bo U tak Π_n-sistem, da velja $-U \cap T = \emptyset$. Potem obstaja taka predureditev T', da velja $T \subseteq T'$, $-U \cap T' = \emptyset$ in $T' \cap -T'$ je popoln praideal.*

Dokaz : Ker je množica T modul nad krepko predureditvijo Σ_n, obstaja po Zornovi lemi tak modul S nad predureditvijo Σ_n, ki vsebuje T in ki je maksimalen glede na relacijo $-U \cap S = \emptyset$. Naj bo $J = S \cap -S$. Po izreku 4 je množica J popoln praideal.

Naj bo $T' = T + J$. Očitno velja $\Pi_n \subseteq T \subseteq T'$, $T' + T' \subseteq T'$ in $T' \cdot T' \subseteq T'$. Velja $-U \cap T' \subseteq -U \cap S = \emptyset$. Ker $1 \in U$, odtod sledi, da je T' predureditev. Ker je $J \subseteq T' \cap -T' \subseteq S \cap -S = J$, velja tudi $-T' \cap T' = J$. Q.E.D.

Pravimo, da je predureditev T *praidealska*, če je njen nosilec praideal. Praidealom, ki so nosilci kake preureditve pravimo *realni praideali*. Izrek 6 pove, da je vsak realen praideal popoln.

Izrek 6 *Naj bo T poljubna predureditev eksponenta n in $J := T \cap -T$ njen nosilec. Potem so ekvivalentne trditve:*

1. *J je popoln praideal.*

2. *J je praideal.*

3. *Če $a, b \in R$ in $a\Pi_n b \in J$, potem bodisi $a \in J$, bodisi $b \in J$.*

Dokaz : Iz točke 1. očitno sledi 2.

Naj velja točka 2. in naj bosta $a, b \in R$ taka elementa, da velja $a\Pi_n b \subseteq J$. Ker je $n!R \subseteq \Sigma_n - \Sigma_n$, sledi $n!(aRb) \subseteq a(\Sigma_n - \Sigma_n)b \subseteq J$. Ker je J ideal, velja $(n!)RaRb \subseteq J$. Če $n! \in J$, potem $-1 = -n! + (n! - 1) \in J + T \subseteq T$, kar je v nasprotju s predpostavko, da je T predureditev. Ker je J praideal in $n! \notin J$, velja bodisi $a \in J$ bodisi $b \in J$. Torej velja točka 3.

Naj velja točka 3. Očitno odtod sledi, da je $J^e = J$. Po lemi 1 je množica $J = J^e = T^e \cap -T^e$ popoln praideal. Množica $U = \Pi_n \setminus J$ je Π_n-sistem. Ker velja $-U \cap T = \emptyset$, obstaja po izreku 5 taka predureditev T', da velja $T \subseteq T'$, $-U \cap T' = \emptyset$ in $J' = T' \cap -T'$ je popoln praideal. Očitno velja $T \cap \Pi_n = T' \cap \Pi_n$ in zato tudi $J \cap \Pi_n = J' \cap \Pi_n$. Vzemimo sedaj poljuben element $x \in J'$. Potem $(x\Pi_n)^{n-1}x \subseteq J' \cap \Pi_n = J \cap \Pi_n \subseteq J$. Po lastnosti iz točke 3. odtod sledi $x \in J$. Dokazali smo $J' \subseteq J$. Obratna inkluzija je očitna. Torej je množica J popoln praideal. Q.E.D.

Vsaki praidealski predureditvi priredimo njeno *zaprtje* $\overline{T} := \{r \in R \ ; \ rT^+ \cap T \neq \emptyset\}$. Praidealska predureditev je *zaprta*, če je enaka svojemu zaprtju. Če lemo 1 iz razdelka 1.1 uporabimo na polgrupi $S = R \setminus T^0$, vidimo, da velja $\overline{T} := \{r \in R \ ; \ T^+r \cap T \neq \emptyset\}$. Vsaka ciklična predureditev je praidealska in zaprta.

Izrek 7 *Naj bo T praidealska predureditev z nosilcem J. Potem je množica $\overline{T}$ zaprta praidealska predureditev z nosilcem J, ki ima permutacijsko lastnost. Predureditev $\overline{T}$ je eksponenta n natanko takrat, ko vsebuje vse n-te potence elementov kolobarja R.*

Dokaz : Uporabi izreke 2 in 3 ter lemo 4 iz razdelka 1.1 na polgrupi $S = R \setminus J$. Q.E.D.

6.3 Predureditve na faktorskih kolobarjih

Izrek 8 opisuje kako se vedejo predstožci pri prehodu na faktorski kolobar.

Trditev 8 *Naj bo H poljuben usmerjen stožec na kolobarju R in naj bo $\pi : R \to R/H^0$ naravni epimorfizem. Slika in praslika preslikave π podajata bijektivno korespondenco med množico $\mathcal{M}_H = \{P;\ P$ je predstožec na R, $H \subseteq P$ in $P^0 = H^0\}$ in množico $\mathcal{N}_H = \{Q;\ Q$ je predstožec na R, $\pi(H) \subseteq Q$ in $Q^0 = \{0\}\}$.*

Dokaz : Naj bo $P \in \mathcal{M}_H$ poljuben element in naj bo $P' = \pi(P)$. Trdimo, da $P' \in \mathcal{N}_H$. Očitno je množica P' podpolkolobar, ki vsebuje množico $\pi(H)$. Če $-1 \in P'$, potem obstaja tak element $p \in P$, da velja $-1 = \pi(p)$, Odtod sledi $\pi(1+p) = 0$, se pravi, da $1 + p \in H^0 \subseteq -P$, kar je v nasprotju s privzetkom $-1 \notin P$. Dokažimo še, da je $P' \cap -P' = \{0\}$. Če $x \in P' \cap -P'$, potem obstajata taka elementa $p_1, p_2 \in P$, da je $x = \pi(p_1) = \pi(-p_2)$. Odtod sledi $\pi(p_1+p_2) = 0$, torej $p_1+p_2 \in H^0 \subseteq -P$. Odtod dobimo $p_1, p_2 \in P^0 = H^0$, se pravi $x = 0$.

Naj bo $P' \in \mathcal{N}_H$ poljuben element in naj bo $P = \pi^{-1}(P')$. Trdimo, da $P \in \mathcal{M}_H$. Očitno je množica P predstožec. Velja tudi $H \subseteq \pi^{-1}(\pi(H)) \subseteq \pi^{-1}(P') = P$ in $P \cap -P = \pi^{-1}(P') \cap \pi^{-1}(-P') = \pi^{-1}(P' \cap -P') = \pi^{-1}(0) = H^0$.

Pokazati moramo še, da za poljuben element $P' \in \mathcal{N}_H$ velja $\pi(\pi^{-1}(P')) = P'$ in da za poljuben element $P \in \mathcal{M}_H$ velja $\pi^{-1}(\pi(P)) = P$. Prva trditev sledi iz surjektivnosti preslikave π. Drugo trditev dokažemo takole. Če $z \in \pi^{-1}(\pi(P))$, potem $\pi(z) \in \pi(P)$. Torej obstaja tak element $p \in P$, da velja $\pi(z) = \pi(p)$. Odtod sledi $z - p \in H^0 \subseteq P$, torej $z \in P$. Obratna inkluzija je očitna. Q.E.D.

Bijektivna korespondenca iz izreka 8 ohranja vse lastnosti predstožcev, ki so za nas zanimive.

Izrek 9 *Naj bo R asociativen kolobar, J njegov realen praideal, in $\phi : R \to R/J$ naravni epimorfizem.*

Potem slika in praslika preslikave ϕ podajata bijektivno korespondenco med stožci eksponenta n na kolobarju R/J in predureditvami eksponenta n na R z nosilcem J.

Pri tej korespondenci preidejo zaprte predureditve v zaprte stožce in ciklične predureditve v ciklične stožce.

Dokaz : Za poljuben element $z \in R$ velja $\phi(z) \in \Pi_n(R/J)$ natanko tedaj, ko obstajajo taki elementi $r_1, \ldots, r_k \in R$, da velja $\phi(z) \in \Pi'(\phi(r_1)^n \cdots \phi(r_k)^n) = \phi(\Pi'(r_1^n \cdots r_k^n))$. To pa velja natanko tedaj, ko $\phi(z) \in \phi(\Pi_n(R))$. Odtod sledi, da je $\phi(\Pi_n(R)) = \Pi_n(R/J)$. Očitno je $\Pi_n(R) \subseteq \phi^{-1}(\Pi_n(R/J))$. Prva trditev v izreku sledi sedaj iz izreka 8.

Naj bo T zaprt stožec na R z nosilcem J. Trdimo, da je stožec $\phi(T)$ zaprt. Vzemimo poljuben element $\phi(z) \in \overline{\phi(T)}$. Odtod sledi, da je $\phi(z)(\phi(T))^+ \cap \phi(T) \neq \emptyset$. Očitno je $(\phi(T))^+ = \phi(T^+)$. Odtod sledi, da $\phi(zT^+)$ seka $\phi(T)$, torej zT^+ seka $\phi^{-1}(\phi(T)) = T$. Ker je stožec T zaprt, sledi $z \in T$, odtod pa $\phi(z) \in \phi(T)$.

Naj bo T' zaprta predureditev na R/J z nosilcem $\{0\}$. Trdimo, da je predureditev $\phi^{-1}(T')$ zaprta. Vzemimo poljuben element $z \in \overline{\phi^{-1}(T')}$. Odtod sledi, da je $z(\phi^{-1}(T'))^+ \cap \phi^{-1}(T') \neq \emptyset$. Očitno je $(\phi^{-1}(T'))^+ = \phi^{-1}((T')^+)$. Odtod sledi, da $\phi(z)(T')^+$ seka T'. Ker je predureditev T' zaprta, sledi $\phi(z) \in T'$, odtod pa $z \in \phi^{-1}(T')$.

Naj bo P poljubna ureditev na R z nosilcem J in naj bo σ pripadajoča signatura. Očitno velja $\sigma^{-1}(0) = J$, torej σ inducira polgrupni homomorfizem $\tau : R/J \to \mu \cup \{0\}$. Ker je ϕ surjektivna, velja $\phi(P) = \tau^{-1}(\{0, 1\})$. Torej je $\phi(P)$ cikličen stožec na R/J.

Naj bo P' poljubna predureditev na R/J z nosilcem $\{0\}$ in naj bo τ pripadajoča signatura. Potem velja $\phi^{-1}(P') = \phi^{-1}(\tau^{-1}(\{0, 1\}) = (\tau \circ \phi)^{-1}(\{0, 1\})$. Torej je $\phi^{-1}(P')$ ureditev na R. Q.E.D.

Pravimo da ima zaprta praidealska predureditev z nosilcem J *presečno lastnost*, če je enaka preseku vseh cikličnih predureditev z nosilcem J, ki jo vsebujejo. Pravimo, da ima kolobar R *presečno lastnost* eksponenta n, če $-1 \notin \Sigma_n(R)$ in če ima vsaka zaprta praidealska predureditev na R eksponenta n presečno lastnost.

Izrek 10 *Naj bo R poljuben asociativen kolobar in n poljubna potenca števila 2. Potem ima R presečno lastnost eksponenta n natanko tedaj, ko $-1 \notin \Sigma_n(R)$.*

Dokaz : Sledi iz izreka 6 v petem poglavju in iz izreka 9. Q.E.D.

Izrek 11 *Naj bo R poljuben Noetherski kolobar in n poljubno sodo število. Potem ima R presečno lastnost eksponenta n natanko tedaj, ko $-1 \notin \Sigma_n(R)$.*

Dokaz : Sledi iz presečnega izreka za Orejeve domene, izreka 9 in dejstva, da je vsaka Noetherska domena Orejeva. Q.E.D.

6.4 Nullstellensatz in Positivstellensatz

V tem razdelku predpostavljamo, da ima kolobar R presečno lastnost eksponenta n.

Izrek 12 *Za poljubno predureditev T eksponenta n in poljubna $x, y \in R$ sta ekvivalentni:*

1. *Za poljubno ureditev P, ki vsebuje T, velja sklep: če $x \notin P^+$, potem $y \in P^0$.*

2. *Obstaja tako nenegativno celo število k, da velja $-y^{nk} \in T - \Sigma(\Pi_n x \Pi_n)$.*

Dokaz : Dokažimo najprej, da iz 1. sledi 2. Naj bo $U = \{y^{nk}; k \geq 0\}$ in $M = T - \Sigma(\Pi_n x \Pi_n)$. Množica U je multiplikativna in je zato Π_n-sistem. Množica M je modul nad krepko predureditvijo Σ_n. Če točka 2. ne drži, potem je $-U \cap M = \emptyset$. Po Zornovi lemi obstaja tak modul S nad Σ_n, ki vsebuje množico M in ki je maksimalen glede na lastnost $-U \cap S = \emptyset$. Po osnovnem izreku je množica $J = S \cap -S$ popoln praideal in po izreku 5 je množica $T' := T + J$ praidealska predureditev z nosilcem J. Ker je $J \cap -U = \emptyset$ in $y^n \in U$, sledi, da $-y^n \notin J$ in zato $y \notin J$.

Če točka 1. drži, potem iz $y \notin J$ sledi, da je $x \in P^+$ za vsako ureditev P, ki vsebuje T in ima nosilec J. Odtod sledi, da $x \in P$ za vsako ureditev P, ki vsebuje zaprto predureditev $\overline{T'}$ in ima nosilec J. Ker ima kolobar R presečno lastnost reda n, odtod sledi, da $x \in \overline{T'}$. Ker $x \notin J$, obstajata taka elementa $s, t \in (T')^+$, da velja $sx = t$. Velja $s^{n-1}t \in T' \subseteq S$ in $-s^{n-1}t = -s^n x \in M \subseteq S$. Odtod sledi $s^{n-1}t \in J$, kar je v nasprotju s tem, da je J popoln praideal in $s, t \notin J$.

Predpostavimo sedaj, da drži točka 2. Vzemimo tako nenegativno celo število k, da velja $-y^{nk} \in T - \Sigma(\Pi_n x \Pi_n)$. Potem obstaja tak element $t \in T$, da je $y^{nk} + t \in \Sigma(\Pi_n x \Pi_n)$. Vzemimo poljubno ureditev P, ki vsebuje T, in naj bo σ pripadajoča signatura. Očitno $\sigma(y^{nk} + t) \in \{0, 1\}$ in $\sigma(\Sigma(\Pi_n x \Pi_n)) \subseteq \{0.\sigma(x)\}$. Če $x \notin P^+$, potem $\sigma(x) \neq 1$. Odtod sledi, da je $\sigma(y^{nk} + t) = 0$. Odtod dobimo $\sigma(y^{nk}) = \sigma(t) = 0$. torej res $y \in P^0$. Točka 1. je s tem dokazana. Q.E.D.

Posledica 13 (Nullstellensatz) . *Za pojuben element $a \in R$ in poljubno predureditev T eksponenta n sta ekvivalentni trditvi:*

1. *$a \in P^0$ za poljubno ureditev P, ki vsebuje T.*

2. *Obstaja tako nenegativno celo število k, da velja $-a^{nk} \in T$.*

Dokaz : Uporabimo izrek 12 z $x = 0$ in $y = a$. Q.E.D.

Posledica 14 (šibki Positivstellensatz) *Za poljuben element $a \in R$ in poljubno predureditev T eksponenta n sta ekvivalentni trditvi:*

1. *$a \in P$ za poljubno ureditev P, ki vsebuje T.*
2. *Obstaja tako nenegativno celo število k, da velja $-a^{nk} \in T - \Sigma(\Pi_n a \Pi_n)$.*

Dokaz : Uporabimo izrek 12 z $x = a$ in $y = a$. Q.E.D.

Posledica 15 (strogi Positivstellensatz) *Za poljuben element $a \in R$ in poljubno predureditev T eksponenta n sta ekvivalentni trditvi:*

1. *$a \in P^+$ za poljubno ureditev P, ki vsebuje T.*
2. *Velja $-1 \in T - \Sigma(\Pi_n a \Pi_n)$.*

Dokaz : Uporabimo izrek 12 z $x = a$ in $y = 1$. Q.E.D.

Posledica 16 *Naj bosta a in b poljubna elementa kolobarja R in T predureditev eksponenta n. Potem so ekvivalentne trditve:*

1. *$\sigma(a) = \sigma(b)$ za vsako signaturo $\sigma \in Sig_T(R)$.*
2. *Obstajata tako nenegativno celo število k in tak $i = 1, \ldots, n-1$, da velja $-(a^n + b^n)^{nk} \in T - \Sigma(\Pi_n a^i b^{n-i} \Pi_n)$.*
3. *Za vsako število $i = 1, \ldots, n-1$ obstaja tako nenegativno celo število k_i, da velja $-(a^n + b^n)^{nk_i} \in T - \Sigma(\Pi_n a^i b^{n-i} \Pi_n)$ za vsak $i = 1, \ldots, n-1$.*

Dokaz : Implikaciji 2. $\Rightarrow$ 1. in 1. $\Rightarrow$ 3. sledita iz izreka 12, če vzamemo $x = a^i b^{n-i}$ in $y = a^n + b^n$. Implikacija 3. $\Rightarrow$ 2. je očitna. Q.E.D.

7.

Spektralni prostori

Teorija spektralnih prostorov je splošno znana, vendar redko zaide v učbenike. Namen tega poglavja je olajšati branje zadnjih dveh poglavij. Rezultati so iz [1], [35] in [36].

7.1 Predspektralni prostori

Topološki prostor X se imenuje *predspektralen prostor*, če izpolnjuje naslednje lastnosti:

1. je kompakten in T_0,
2. presek poljubnih dveh kompaktnih odprtih množic je kompaktna množica,
3. kompaktne odprte množice tvorijo bazo topologije,

Odtod sledi, da so kompaktne odprte množice zaprte za končne preseke in končne unije.

Končnim presekom kompaktnih odprtih množic in njihovih komplementov pravimo *bazične konstruktibilne množice*. Končnim unijam bazičnih konstruktibilnih množic bomo rekli *konstruktibilne množice*. Končni preseki, končne unije in komplementi konstruktibilnih množic so spet konstruktibilne množice. Družina poljubnih unij bazičnih konstruktibilnih množic zadošča aksiomom za odprte množice topološkega prostora. Tej topologiji pravimo *konstruktibilna topologija*, množico X opremljeno s to novo topologijo pa označimo s X_{con}. Konstruktibilna topologija je očitno Hausdorfova in popolnoma nepovezana. Konstruktibilne množice so v tej topologiji odprte in zaprte.

Množica, ki se ne da izraziti kot unija dveh nepraznih zaprtih podmnožic, se imenuje *nerazcepna množica*. Točka $y \in X$ se imenuje *generična točka* podmnožice $Y \subseteq X$, če

velja $Y = \overline{\{y\}}$. Zaradi lastnosti T_0 nobena množica ne more imeti več kot ene generične točke.

Izrek 1 *Če je X predspektralen prostor. Potem sta ekvivalentni trditvi:*

1. *konstruktibilna topologija je kompaktna,*

2. *Poljubna nerazcepna zaprta množica v X ima generično točko.*

Dokaz : ([35], Proposition 4.) Najprej dokažimo, da iz *1.* sledi *2.* Naj bo Y poljubna zaprta nerazcepna množica. Označimo z $\mathcal{M}$ družino vseh kompaktnih odprtih množic, ki sekajo Y. Ker je Y nerazcepna, je družina $\mathcal{M}$ zaprta za končne preseke. Ker so elementi družine $\mathcal{M}$ zaprti v konstruktibilni topologiji in ker je množica Y kompaktna v konstruktibilni topologiji, je presek $\bigcap \mathcal{M} \cap Y$ neprazen. Naj bo y poljubna točka iz tega preseka. Ker je Y zaprte velja $\overline{\{y\}} \subseteq Y$. Naj bo sedaj $z \in Y$ poljubna točka. Vsaka kompaktna odprta množica, ki vsebuje z, seka Y in zato vsebuje točko y. Po definiciji zaprtja odtod sledi, da je $z \in \overline{\{y\}}$, torej velja $Y \subseteq \overline{\{y\}}$.

Naj sedaj velja točka *2.* Naj bo $\mathcal{J}$ poljubna družina, ki sestoji iz zaprtih in kompaktnih odprtih množic in ki ima neprazne končne preseke. Če dokažemo, da ima družina $\mathcal{J}$ neprazen presek, potem točka *1.* sledi iz leme Aleksandrova. Lemo Aleksandrova namreč lahko formuliramo takole: topološki prostor je kompakten natanko tedaj, ko ima vsaka družina. ki sestoji iz komplementov podbazičnih množic in ki ima neprazne končne preseke, tudi sama neprazen presek. Podbaza konstruktibilne topologije, ki jo imamo v mislih, sestoji iz odprtih množic in komplementov kompaktnih odprtih množic.

Brez škode za splošnost lahko predpostavimo, da je družina $\mathcal{J}$ maksimalna glede na inkluzijo. Naj bo Z presek vseh zaprtih množic iz $\mathcal{J}$. Naj bodo $Z_1, \ldots, Z_k$ poljubne zaprte množice iz $\mathcal{J}$ in $U_1, \ldots, U_l$ poljubne odprte kompaktne množice iz $\mathcal{J}$. Množica $U := U_1 \cap \ldots \cap U_l$ je neprazna. Ker je prostor X predspektralen, je U kompaktna. Odtod sledi, da je množica $Z \cap U$ neprazna. Torej je tudi množica $Z \cap Z_1 \cap \ldots \cap Z_k \cap U_1 \cap \ldots \cap U_l = Z \cap U$ neprazna. S tem smo dokazali, da ima družina $\mathcal{J} \cup \{Z\}$ neprazne končne preseke, Sledi $Z \in \mathcal{J}$.

Dokažimo sedaj, da je množica Z nerazcepna. Če bi veljalo $Z = Z_1 \cup Z_2$, kjer sta Z_1 in Z_2 neprazni zaprti množici, potem Z_1 in Z_2 nista v družini $\mathcal{J}$, saj je Z najmanjša zaprta množica iz te družine. Odtod sledi, da družini $\mathcal{J} \cup \{Z_1\}$ in $\mathcal{J} \cup \{Z_2\}$ nimata vseh končnih

presekov nepraznih. Torej obstajajo take odprte množice $U_1, \ldots, U_k, V_1, \ldots, V_l \in \mathcal{J}$, da velja $Z_1 \cap U_1 \cap \ldots \cap U_k = \emptyset$ in $Z_2 \cap V_1 \cap \ldots \cap V_l = \emptyset$. Odtod sledi, da je $(Z_1 \cup Z_2) \cap U_1 \cap \ldots \cap U_k \cap V_1 \cap \ldots \cap V_k = \emptyset$, kar nasprotuje dejstvu, da $Z \in \mathcal{J}$.

Naj bo x generična točka zaprte nerazcepne množice Z. Ker vsaka odprta množica iz $\mathcal{J}$ seka množico $Z = \overline{\{x\}}$ mora vsebovati x. Torej $x \in \bigcap \mathcal{J}$. Q.E.D.

7.2 Spektralni prostori

Predspektralen prostor, ki zadošča eni od ekvivalentnih lastnosti v izreku 1. imenujemo *spektralen prostor*. Množica, ki je odprta in zaprta v konstruktibilni topologiji spektralnega prostora, je konstruktibilna. Obrat te trditve velja celo v predspektralnih prostorih. Podmnožica spektralnega prostora X je zaprta v konstruktibilni topologiji natanko tedaj, ko je enaka preseku kake družine konstruktibilnih množic. Takim množicam pravimo *prokonstruktibilne množice.* Poljubno pokritje poljubne prokonstruktibilne množice s konstruktibilnimi množicami ima kako končno podpokritje.

Trditev 2 *Če je S prokonstruktibilna množica kakega spektralnega prostora, potem je $\overline{S} = \bigcup_{x \in S} \overline{\{x\}}$. Še več, obstajajo take točke $x_1, \ldots, x_k \in S$, da velja $\overline{S} = \overline{\{x_1\}} \cup \ldots \cup \overline{\{x_k\}}$.*

Dokaz : Ker je $\{\overline{\{x\}}; x \in S\}$ pokritje prokonstruktibilne množice S s konstruktibilnimi množicami, obstaja končno podpokritje $S \subseteq \overline{\{x_1\}} \cup \ldots \cup \overline{\{x_k\}}$. Odtod sledi $\overline{S} = \overline{\{x_1\}} \cup \ldots \cup \overline{\{x_k\}}$. Q.E.D.

Naj bosta x in y poljubni točki poljubnega spektralnega prostora. Če velja $y \in \overline{\{x\}}$, potem pišemo $x \leq y$ in pravimo, da točka y *specializira* točko x, oziroma, da točka x *generizira* točko y.

Trditev 3 *Za poljubno točko poljubnega spektralnega prostora obstaja vsaj ena zaprta točka, ki jo specializira.*

Dokaz : Očitno je dana točka zaprta natanko takrat, ko je maksimalna glede na specializacijo $\leq$. Naj bo $(x_i)_{i \in I}$ poljubno naraščajoče zaporedje točk, ki specializirajo dano točko x. Potem je zaporedje množic $(\overline{\{x_i\}})_{i \in I}$ padajoče. Ker je spektralni prostor kompakten, ima to zaporedje neprazen presek. Vsak element tega preseka je gornja meja zaporedja

$(x_i)_{i\in I}$. Po Zornovi lemi obstaja taka točka, ki specializira x in ki je maksimalna glede na specializacijo. Q.E.D.

Sledita karakterizaciji normalnih in popolnoma normalnih spektralnih prostorov.

Izrek 4 *Za vsak spektralen prostor X so ekvivalentne naslednje trditve:*

1. *Za vsako točko prostora X obstaja natanko ena zaprta točka, ki jo specializira.*

2. *Poljubni dve zaprti točki imata disjunktni okolici.*

3. *X je normalen topološki prostor.*

Dokaz : Očitno iz *3.* sledi *2.* Obrat je posledica trditve 2. Dokažimo sedaj ekvivalenco točk *1.* in *2.* Zaradi trditve 3 lahko v točki *1.* besedo natanko nadomestimo z besedo kvečjemu.

Če točka *1.* ne drži, potem obstaja taka točka z in taki zaprti točki x in y, da velja $z \leq x$, $z \leq y$ in $x \neq y$. Poljubni disjunktni okolici točk x in y vsebujeta točko z, zato imata neprazen presek. Torej tudi točka *2.* ne drži.

Če točka *2.* ne drži, potem obstajata taki zaprti točki $x \neq y$, da poljubna kompaktna odprta okolica točke x seka poljubno kompaktno odprto okolico točke y. Naj bo $\mathcal{M}$ družina vseh takih presekov. Iz druge lastnosti predspektralnih prostorov sledi, da ima družina $\mathcal{M}$ neprazne končne preseke in da so njeni elementi kompaktne odprte množice. Ker je prostor X kompakten v konstruktibilni topologiji, elementi družine $\mathcal{M}$ pa zaprti v konstruktibilni topologiji, ima družina $\mathcal{M}$ neprazen presek. Poljubna točka iz preseka ima dve različni zaprti specializaciji x in y. Torej točka *1.* ne drži. Q.E.D.

Množico zaprtih točk spektralnega prostora X označimo z $\mathrm{Max}(X)$. Če je prostor X normalen, potem obstaja naravna preslikava $X \to \mathrm{Max}(X)$. Izkaže se, da je ta preslikava zvezna in zato zaprta.

Pravimo, da je spektralni prostor *popolnoma normalen*, če za poljubne točke $x, y, z \in X$, ki zadoščajo $z \leq x$ in $z \leq y$, velja bodisi $x \leq y$ bodisi $y \leq x$. To je ekvivalentno z zahtevo, da je množica specializacij dane točke linearno urejena. Vsak popolnoma normalen spektralen prostor je tudi normalen.

7.3 Stoneova antiekvivalenca

Mreža v tem razdelku pomeni omejeno distributivno mrežo. Homomomorfizmi mrež naj vedno ohranjajo največji in najmanjši element mreže. Kategorijo distributivnih mrež in njihovih homomorfizmov označimo z **D01**. Morfizmi spektralnih prostorov so take preslikave, katerih praslike ohranjajo kompaktne odprte množice. Kategorijo spektralnih prostorov in njihovih morfizmov označimo z **SS**.

Vsakemu spektralnemu prostoru X lahko priredimo mrežo $\mathrm{L}(X)$ njegovih kompaktnih odprtih množic. Vsaki mreži L lahko priredimo množico $\mathrm{St}(L)$ vseh homomorfizmov iz mreže L v mrežo $\{0,1\}$. Za vsak element $a \in L$ definirajmo množico $U_a := \{\phi \in \mathrm{St}(L);\ \phi(a) = 1\}$. Ker velja $U_a \cap U_b = U_{a \cup b}$, tvorijo množice U_a bazo neke topologije na $\mathrm{St}(L)$, ki ji recimo *Harrisonova topologija*. Množice U_a in njihovi komplementi tvorijo podbazo neke topologije na $\mathrm{St}(L)$, ki ji recimo *topologija Tihonova*.

Za poljubno mrežo L je prostor $Z_L := \{0,1\}^L$ s topologijo konvergence po točkah naravno homeomorfen produktnemu prostoru $\prod_{l \in L}\{0,1\}$ in zato kompakten.

Izrek 5 *Za poljubno mrežo L je prostor $\mathrm{St}(L)$ s topologijo Tihonova zaprt podprostor v Z_L.*

Dokaz : Množice $M_a := \{1\} \times \prod_{b \in R \setminus \{a\}}\{0,1\}$ in njihovi komplementi tvorijo standardno podbazo prostora Z_L. Ker velja $M_a \cap \mathrm{St}(L) = U_a$ in $M_a^c \cap \mathrm{St}(L) = U_a^c$, se relativna topologija na $\mathrm{St}(L)$ ujema s topologijo Tihonova.

Vzemimo sedaj poljuben element $\phi \in \overline{\mathrm{St}(L)}$. Po definiciji topologije na $\{0,1\}^L$ se ϕ na poljubni končni podmnožici mreže L ujema s kakim elementom iz $\mathrm{St}(L)$. Vzemimo poljubna elementa $a, b \in L$ in izberimo, tak $\chi \in \mathrm{St}(L)$, ki se na $\{a, b, a \cap b, a \cup b, 0, 1\}$ ujema z ϕ. Odtod sledi $\phi(a \cup b) = \chi(a \cup b) = \chi(a) \cup \chi(b) = \phi(a) \cup \phi(b)$. Analogno dokažemo $\phi(a \cap b) = \phi(a) \cap \phi(b)$, $\phi(0) = 0$ in $\phi(1) = 1$. Torej $\phi \in \mathrm{St}(L)$. Q.E.D.

Po izreku 5 je topologija Tihonova kompaktna. Harrisonova topologija je kompaktna zato, ker je šibkejša od topologije Tihonova. Topologija Tihonova je Hausdorfova in popolnoma nepovezana, za Harrisonovo topologijo pa to ne velja nujno.

Izrek 6 *Naj bo $X = \mathrm{St}(L)$ Stoneov prostor mreže L opremljen s Harrisonovo topologijo.*

1. *Prostor X je spektralen.*

2. *Podmnožica $U \subseteq X$ je odprta in kompaktna natanko tedaj, ko obstaja tak $a \in L$, da velja $U = U_a$.*

3. *Konstruktibilna topologija na X se ujema s topologijo Tihonova.*

Dokaz : Ker so množice U_a zaprte v topologiji Tihonova, so v tej topologiji tudi kompaktne, zato so kompaktne tudi v Harrisonovi topologiji. Nasprotno je vsaka kompaktna odprta množica enaka končni uniji $U_{a_1} \cup \ldots \cup U_{a_r} = U_{a_1 \cup \ldots \cup a_r}$. S tem je točka *2.* dokazana. Odtod takoj sledi točka *3.*

Dokažimo, sedaj, da ima prostor X lastnost T_0. Če sta $\phi, \tau \in \mathrm{St}(L)$ različni točki, potem obstaja tak element $a \in L$, da velja $\phi(a) \neq \tau(a)$. Lahko predpostavimo, da je $\phi(a) = 1$ in $\tau(a) = 0$. Potem $\phi \in U_a$ in $\tau \notin U_a$. Iz točk *2.* in *3.* takoj sledi, da je prostor X spektralen, Q.E.D.

Posledica 7 *Preslikava $a \to U_a$ iz mreže L v mrežo $\mathrm{L}(\mathrm{St}(L))$ je izomorfizem mrež.*

Naj bo X poljuben spektralen prostor. Poljubnemu elementu $x \in X$ priredimo preslikavo $\chi_x : \mathrm{L}(X) \to \{0, 1\}$, ki je definirana s predpisom: za poljuben $U \in \mathrm{L}(X)$ velja $\chi_x(U) = 1$ natanko tedaj, ko $x \in U$. Očitno je χ_x mrežni homomorfizem, torej $\chi_x \in \mathrm{St}(\mathrm{L}(X))$.

Posledica 8 *Preslikava $x \to \chi_x$ iz spektralnega prostora X v spektralni prostor $\mathrm{St}(\mathrm{L}(X))$ je homeomorfizem topoloških prostorov.*

Dokaz : Dokažimo najprej injektivnost. Če za elementa $x, y \in X$ velja $\chi_x = \chi_y$, potem poljubna kompaktna odprta množica, ki vsebuje eno točko, vsebuje tudi drugo. Ker kompaktne odprte množice tvorijo bazo topologije prostora X, sta točki x in y topološko nerazločljivi. Ker ima X lastnost T_0, sledi $x = y$.

Dokažimo sedaj surjektivost. Vzemimo poljuben element $\chi \in \mathrm{St}(\mathrm{L}(X))$. Naj bo $\mathcal{M} \subseteq \mathrm{L}(X)$ družina vseh množic, ki jih χ preslika v 1. Ker ima družina $\mathcal{M}$ neprazne končne preseke in ker so njeni elementi zaprti v topologiji Tihonova, je njen presek $J := \bigcap \mathcal{M}$ neprazen. Za poljuben element $x \in J$ velja $\chi = \chi_x$.

Iz točke *2.* izreka 6 sledi, da je preslikava $x \to \chi_x$ homeomorfizem. Q.E.D.

Kako preslikavi St in L razširimo do funktorjev. Naj bosta X in Y spektralna prostora in $f : X \to Y$ morfizem spektralnih prostorov. Njena praslika f^* ohranja kompaktne

odprte množice, ter spoštuje preseke in unije. Torej je $f^* : \mathrm{L}(Y) \to \mathrm{L}(X)$ homomorfizem mrež. Naj bosta sedaj M in N poljubni mreži in $\phi : M \to N$ mrežni homomorfizem. Naj bo $F_\phi : \mathrm{St}(N) \to \mathrm{St}(M)$ preslikava, definirana z $F_\phi(\chi) = \chi \circ \phi$. Ker velja $F_\phi^{-1}(U_a) = U_{\phi(a)}$ za vsak $a \in M$, je F_ϕ prava zvezna preslikava.

Izrek 9 *Preslikavi* L *in* St *sta kontravariantna funktorja, ki zadoščata* $\mathrm{St} \circ \mathrm{L} = \mathrm{id}$ *in* $\mathrm{L} \circ \mathrm{St} = \mathrm{id}$.

Dokaz : Po krajšem premisleku sledi iz posledic 7 in 8. Q.E.D.

Kategoriji **D01** and **SS** sta torej antiekvivalentni. Tej antiekvivalenci pravimo *Stoneova antiekvivalenca* in je posplošitev bolj znane antiekvivalence med kategorijo Booleovih prostorov **BS** in kategorijo Booleovih algeber **BA**.

Množico komplementiranih elementov mreže L označimo z $\mathrm{C}(L)$. Množica $\mathrm{C}(L)$ je Booleova algebra. Množico komplementiranih kompaktnih odprtih množic spektralnega prostora X označimo s $\mathrm{D}(X)$. Očitno so elementi $\mathrm{D}(X)$ ravno odprto-zaprte množice prostora X. Homomorfizmi mrež ohranjajo množico komplementiranih elementov.

Rezultate tega razdelka strnimo v naslednji komutativni diagram

$$\begin{array}{ccc} \mathbf{DO1} & \overset{\mathrm{C}}{\to} & \mathbf{BA} \\ \mathrm{St} \downarrow\uparrow \mathrm{L} & & \mathrm{St} \downarrow\uparrow \mathrm{L} \\ \mathbf{SS} & \overset{\mathrm{D}}{\to} & \mathbf{BS} \end{array}$$

8.

Realen spekter višjega eksponenta

Algebraičen pristop k klasični semialgebraični geometriji temelji na bijektivni kores–pondenci med semialgebraičnimi množicami v $\mathbb{R}^k$ in konstruktibilnimi množicami v $\mathrm{Sper}(\mathbb{R}[X_1, \ldots, X_k])$.

Ta korespondenca je motivirala študij realnega spektra poljubnega komutativnega kolobarja (glej 3. del v [1]). Kasneje so se pojavili tudi članki o realnem spektru višjega eksponenta komutativnih kolobarjev ([37], [41]) in o realnem spektru nekomutativnih kolobarjev ([32]). V tem poglavju dajemo skupno posplošitev teh teorij na realen spekter višjega reda za nekomutativne kolobarje. Teorije p-realnega spektra ([40],[41]) ne obravnavamo.

V tem poglavju ni pomembnejših originalnih prispevkov. Dokazi so v glavnem enostavne posplošitve dokazov iz [37] in [38].

V tem poglavju predpostavljamo, da je n dano naravno število, R dan kolobar s presečno lastnostjo eksponenta n in T dana prava predureditev s strogim eksponentom n.

8.1 Prostor T-signatur

Signatura σ na kolobarju R se imenuje *T-signatura*, če velja $\sigma(T) = 1$. Vsaka T-signatura je eksponenta n. Ker ima kolobar R presečno lastnost eksponenta n, je množica $\mathrm{Sig}_T(R)$ neprazna. Če število n ni potenca števila 2, potem ne vemo, ali množica $\mathrm{Sig}_T(R)$ vsebuje kako signaturo strogega eksponenta n.

Za poljuben element $a \in R$ in poljuben element $\omega \in \mu_n \cup \{0\}$ definirajmo množico

$O_T(a,\omega) = \{\sigma \in \mathrm{Sig}_T(R); \sigma(a) = \omega\}$. Množicam oblike $O_T(a,\omega)$ recimo *t-podbazične množice*, njihovim končnim presekom pa *t-bazične* množice. Množicam, ki se dajo izraziti kot unija t-bazičnih množic, recimo *t-odprte* množice, družini, ki jo tvorijo, pa *topologija Tihonova.*

Označimo $N_T(a) = O(a,0)$ in $D_T(a,i) = O(a,\zeta^i)$. Vsem množicam oblike $D_T(a,i)$ recimo *h-podbazične* množice. Analogno kot zgoraj definiramo *h-bazične* množice, *h-odprte* množice in *Harrisonovo topologijo.* Če je kolobar R obseg, potem se Harrisonova topologija in topologija Tihonova na $\mathrm{Sig}_T(R)$ ujemata. Ta primer bomo obravnavali v naslednjem poglavju.

Trditev 1 *Vzemimo na množici $\mu_n^0 := \mu_n \cup \{0\}$ diskretno topologijo, na množici $Z = \prod_{a\in R} \mu_n^0$ produktno topologijo in na množici $\mathrm{Sig}_T(R)$ topologijo Tihonova.*

Preslikava $\Phi : \mathrm{Sig}_T(R) \to Z$ definirana s predpisom $\Phi(\sigma) = (\sigma(a))_{a\in R}$ je zaprta vložitev.

Dokaz : Dokažimo najprej injektivnost preslikave Φ. Naj bosta σ in τ taki T-signaturi na R, da velja $\Phi(\sigma) = \Phi(\tau)$. Potem je $(\sigma(a))_{a\in R} = (\tau(a))_{a\in R}$, kar pomeni $\sigma(a) = \tau(a)$ za vsak $a \in R$, torej $\sigma = \tau$.

Za dokaz zaprtosti slike preslikave Φ potrebujemo tole pomožno trditev: *Za poljuben element $x = (x_a)_{a\in R}$ iz zaprtja slike preslikave Φ in za poljubne elemente $a_1, \ldots, a_k \in R$ obstaja taka T-signatura τ, da velja $\tau(a_1) = x_{a_1}, \ldots, \tau(a_k) = x_{a_k}$.*

Definirajmo $U_{a_i} = \{x_{a_i}\}$ za $i - 1, \ldots, k$, $U_a = \mu_n^0$, če $a \in R \setminus \{a_1, \ldots, a_k\}$ in $U = \prod_{a\in R} U_a$. Množica U je odprta okolica elementa x, zato seka sliko preslikave Φ. Torej obstaja taka T-signatura τ, da je $\Phi(\tau) \in U$. Odtod sledi pomožna trditev.

Da bi dokazali zaprtost slike preslikave Φ zadošča dokazati, da je preslikava χ, ki je definirana s $\chi(a) = x_a$, T-signatura za vsak element $x = (x_a)_{a\in R}$ iz zaprtja slike preslikave Φ.

Vzemimo najprej poljubna elementa $a, b \in R$. Po pomožni trditvi obstaja taka T-signatura σ, da velja $\sigma(a) = x_a$, $\sigma(b) = x_b$ in $\sigma(ab) = x_{ab}$. Odtod sledi $x_{ab} = x_a x_b$, torej je preslikava χ polgrupni homomorfizem.

Vzemimo sedaj taka elementa $a, b \in R$, da je $x_a = x_b = 1$. Po pomožni trditvi obstaja taka T-signatura σ, da velja $\sigma(a) = x_a$, $\sigma(b) = x_b$ in $\sigma(a + b) = x_{a+b}$. Odtod sledi $x_{a+b} = 1$. Torej je množica $\chi^{-1}(1)$ zaprta za seštevanje.

Da bi dokazali zveznost in odprtost preslikave Φ definirajmo podbazične množice $M(a,\omega) = \{\omega\} \times \prod_{b \in R \setminus \{a\}} \mu_n^0$ na prostoru Z in opazimo relaciji $\Phi^{-1}(M(a,\omega)) = O(a,\omega)$ ter $\Phi(O(a,\omega)) = M(a,\omega) \cap \Phi(\mathrm{Sig}_T(R))$. Slika in praslika preslikave Φ torej ohranjata podbazne množice. S tem je trditev dokazana. Q.E.D.

Iz te trditve sledi, da je topologija Tihonova kompaktna, Hausdorfova in popolnoma nepovezana. Harrisonova topologija je tudi kompaktna, saj je šibkejša od topologije Tihonova.

Izrek 2 *1. Prostor $X = \mathrm{Sig}_T(R)$ s Harrisonovo topologijo je spektralen prostor.*

2. Podmnožica prostora X je h-kompaktna in h-odprta natanko tedaj, ko je enaka končni uniji h-bazičnih množic.

3. Podmnožica prostora X je konstruktibilna natanko tedaj, ko je enaka končni uniji t-bazičnih množic.

4. Konstruktibilna topologija prostora X se ujema s topologijo Tihonova.

Dokaz : Pokazali smo že, da je prostor X h-kompakten. Za poljubni različni točki $\sigma, \tau \in X$ obstaja tak element $a \in R$, da velja $\sigma(a) \neq \tau(a)$. Lahko predpostavimo, da je $\sigma(a) = \zeta^i$ za nek i. Potem je $\sigma \in D_T(a,i)$ in $\tau \notin D_T(a,i)$. S tem smo dokazali, da ima prostor X lastnost T_0, torej zadošča prvi lastnosti predspektralnih prostorov.

Dokažimo točko *2.* Vsaka h-podbazična množica je t-zaprta, zato je tudi vsaka končna unija h-bazičnih množic t-zaprta. Odtod sledi, da je končna unija h-bazičnih množic t-kompaktna in zato tudi h-kompaktna. Nasprotno je vsaka h-odprta množica enaka uniji kake družine h-bazičnih množic, zato je vsaka h-kompaktna h-odprta množica enaka končni uniji h-bazičnih množic.

Iz točke *2.* takoj sledi, da je prostor X predspektralen.

Dokažimo sedaj točko *3.* Vsaka t-podbazična množica je konstruktibilna, saj je bodisi enaka množici oblike $D_T(a,i)$, ki je h-kompaktna in h-odprta, bodisi je enaka množici oblike $N_T(a)$, ki je enaka končnemu preseku komplementov h-kompaktnih h-odprtih množic. Odtod sledi, da je vsaka končna unija t-bazičnih množic konstruktibilna. Nasprotno je vsaka h-podbazična množica ali njen komplement očitno enaka končni uniji t-bazičnoh množic. Iz točke *2.* sledi, da je vsaka kompaktna odprta množica ali njen komplement

enaka končni uniji t-bazičnih množic. Odtod takoj sledi, da je vsaka konstruktibilna množica enaka končni uniji t-bazičnih množic.

Iz točke *3.* takoj sledi točka *4.* Iz točke *4.* sledi, da je prostor X spektralen. Q.E.D.

Naš naslednji cilj je karakterizirati specializacijo na spektralnem prostoru $\mathrm{Sig}_T(R)$. Za vsako signaturo $\sigma \in \mathrm{Sig}_T(R)$ označimo $\sigma^0 = \sigma^{-1}(0)$, $\sigma_i = \sigma^{-1}(\{0, \zeta^i\})$ in $\sigma_i^+ = \sigma^{-1}(\zeta^i)$.

Izrek 3 *Naj bosta σ in τ poljubni T-signaturi na R. Naslednje trditve so ekvivalentne:*

1. τ specializira σ,

2. za vsak $a \in R$ velja sklep $\tau(a) \neq 0 \Rightarrow \tau(a) = \sigma(a)$,

3. $\tau_i^+ \subseteq \sigma_i^+$ za vsak $i = 1, \ldots, n$,

4. $\sigma_i \subseteq \tau_i$ za vsak $i = 1, \ldots, n$.

Dokaz : Točki *2.* in *3.* sta očitno ekvivalentni.

Po definiciji zaprtja je točka *1.* ekvivalentna z lastnostjo, da vsaka odprta množica, ki vsebuje τ vsebuje tudi σ. Ker množice $D_T(a, i)$ tvorijo podbazo Harrisonove topologije, je ta lastnost ekvivalentna z lastnostjo, da vsaka množica oblike $D_T(a, i)$, ki vsebuje τ, vsebuje tudi σ. Toda ta lastnost je očitno ekvivalentna s točko *3.*

Dokažimo, da iz *4.* sledi *2.* Naj bo $\tau(a) \neq 0$. Če je $\sigma(a) = 0$, potem po točki *4.* velja $\tau(a) \in \{0, \zeta^j\}$ za vsak j med 1 in n. To je v nasprotju s predpostavko $\tau(a) \neq 0$. Če je $\sigma(a) = \zeta^i$ za nek i med 1 in n, potem po točki *4.* sledi $\tau(a) \in \{0, \zeta^i\}$. Iz predpostavke $\tau(a) \neq 0$ sledi $\tau(a) = \zeta^i = \sigma(a)$. S tem je točka *2.* dokazana.

Dokažimo še, da iz *2.* sledi *4.* Vzemimo poljubno število i med 1 in i in poljuben element $a \in R$, ki zadošča $\sigma(a) \in \{0, \zeta^i\}$. Če je $\tau(a) = 0$ potem $\tau(a) \in \{0, \zeta^i\}$. V primeru $\tau(a) \neq 0$ sledi iz *1.*, da velja $\tau(a) = \sigma(a) \in \{0, \zeta^i\}$. S tem je točka *4.* dokazana. Q.E.D.

Iz naslednjega izreka sledi, da je spektralni prostor $\mathrm{Sig}_T(R)$ popolnoma normalen.

Izrek 4 *Za poljubni točki $\sigma, \tau \in \mathrm{Sig}_T(R)$ sta ekvivalentni trditvi:*

1. σ in τ imata disjunktni h-odprti okolici,

2. $\sigma \not\leq \tau$ in $\tau \not\leq \sigma$.

Dokaz : Očitno iz *1.* sledi *2.* Dokazujemo nasprotno smer. Po izreku 3 obstajata taki števili $1 \leq i, j \leq n$, da velja $\sigma_i \not\subseteq \tau_i$ in $\tau_j \not\subseteq \sigma_j$. Potem obstajata taka elementa $a, b \in R$ in taki števili $1 \leq m, l \leq n$, da velja $a \in \sigma_i$, $a \in \tau_m^+$, $m \neq i$ ter $b \in \tau_j$, $b \in \sigma_l^+$, $l \neq j$.

Če $a \notin \sigma^0$, potem velja $\sigma \in D_T(a, i)$, $\tau \in D_T(a, m)$ in $D_T(a, i) \cap D_T(a, m) = \emptyset$. Če $b \notin \tau^0$, potem velja $\sigma \in D_T(b, l)$, $\tau \in D_T(b, j)$ in $D_T(b, l) \cap D_T(b, j) = \emptyset$. Če velja $a \in \sigma^0$, $b \in \tau^0$ in $m \neq l$, potem je $a + b \in \sigma^0 + \sigma_l^+ \subseteq \sigma_l$ in $a + b \in \tau_m^+ + \tau^0 \subseteq \tau_m$. Torej je $\sigma \in D_T(a + b, m)$, $\tau \in D_T(a + b, l)$ in $D_T(a + b, m) \cap D_T(a + b, l) = \emptyset$. Če velja $a \in \sigma^0$, $b \in \tau^0$ in $m = l$, potem je kot prej $a - b \in \tau_m^+ - \tau^0 \subseteq \tau_m$. Če upoštevamo, da $-1 \in \sigma_{n/2}$ in izberemo tak $1 \leq r \leq n$, da velja $l + (n/2) \equiv r \ (n)$, potem je $a - b \in \sigma^0 - \sigma_l^+ \subseteq \sigma_r$. Torej je $\sigma \in D_T(a - b, r)$, $\tau \in D_T(a - b, l)$ in $D_T(a - b, r) \cap D_T(a - b, l) = \emptyset$. Q.E.D.

Pozorni bralec bo opazil, da lahko v točki *1.* besedo h-odprta nadomestimo s h-podbazična.

8.2 Prostor T-ureditev

Ureditev P na kolobarju R, ki vsebuje predureditev T se imenuje T-ureditev. Naj bo $\mathrm{Sper}_T(R)$ množica vseh T-ureditev. Kot v prejšnjem razdelku je ta množica neprazna, vsi njeni elementi imajo eksponent n in ne vemo, ali vsebuje kak element strogega eksponenta n.

Definirajmo naslednje podmnožice množice $\mathrm{Sper}_T(R)$.

$$U_T(a) = \{P \in \mathrm{Sper}_T(R);\ a \in P^+\}$$
$$Z_T(a) = \{P \in \mathrm{Sper}_T(R);\ a \in P^0\}$$
$$W_T(a) = \{P \in \mathrm{Sper}_T(R);\ a \in P\}$$

Vpeljimo na množico $\mathrm{Sper}_T(R)$ dve topologiji: *Harrisonova topologija* naj ima za podbazo množice oblike $U_T(a)$ in $W_T(a)^c$. *Topologija Tihonova* naj ima za podbazo množice oblike $W_T(a)$ in $W_T(a)^c$.

Trditev 5 *Vzemimo na množici* $\{0, 1\}$ *diskretno topologijo, na množici* $Z' = \prod_{a \in R}\{0, 1\}$ *produktno topologijo in na množici* $\mathrm{Sper}_T(R)$ *topologijo Tihonova.*

Preslikava $\Psi : \mathrm{Sper}_T(R) \to Z'$ *definirana s predpisom* $\Phi(P) = (c_P(a))_{a \in R}$, *kjer je* c_P *karakteristična funkcija množice* P *je zaprta vložitev.*

Dokaz : Če je $\Psi(P) = \Psi(Q)$, potem je $c_P = c_Q$, torej je $P = Q$. Torej je preslikava Ψ injektivna. Za poljuben $a \in R$ definirajmo množico $W'(a) = \{1\} \times \prod_{b \in R \setminus \{a\}} \{0,1\}$. Veljata relaciji $\Psi^{-1}(W'(a)) = W_T(a)$, $\Psi(W_T(a)) = W'(a) \cap Z'$ iz katerih sledi $\Psi^{-1}(W'(a)^c) = W_T(a)^c$ in $\Psi(W_T(a)^c) = W'(a)^c \cap Z'$. Preslikava Ψ ohranja podbazne množice, torej je homeomorfizem na svojo sliko.

Naj bo $P : \ \mathrm{Sig}_T(R) \to \mathrm{Sper}_T(R)$ preslikava definirana s $P(\sigma) = \sigma^{-1}(\{0,1\})$. Naj bo $\alpha : \ \mu_n^0 \to \{0,1\}$ preslikava definirana z $\alpha(0) = 0$ in $\alpha(\omega) = 1$, če $\omega \neq 0$. Preslikava $F := \prod_{a \in R} \alpha : \ Z \to Z'$ je zvezna in zato zaprta. Ker velja $\Psi \circ P = F \circ \Phi$ in ker je P surjektivna preslikava, velja $F(\mathrm{Im}(\Phi)) = \mathrm{Im}(\Psi)$. Po izreku 1 je množica $\mathrm{Im}(\Phi)$ zaprta v Z, torej je množica $\mathrm{Im}(\Psi)$ zaprta v Z' zaradi zaprtosti preslikave F. Q.E.D.

Dokaz naslednjega izreka je podoben dokazu izreka 2 zato ga opustimo.

Izrek 6 *1. Prostor $X = \mathrm{Sper}_T(R)$ s Harrisonovo topologijo je spektralen prostor.*

2. Podmnožica prostora X, je h-odprta in h-kompaktna natanko tedaj, ko je enaka končni uniji h-bazičnih množic.

3. Podmnožica prostora X je konstruktibilna natanko tedaj, ko je enaka končni uniji t-bazičnih množic.

4. Konstruktibilna topologija prostora X se ujema s topologijo Tihonova.

Naslednji izrek karakterizira specializacijo na spektralnem prostoru $\mathrm{Sper}_T(R)$.

Izrek 7 *Naj bosta P in Q poljubni T-ureditvi na R. Naslednje trditve so ekvivalentne:*

1. Q specializira P,

2. $P \subseteq Q$ in $Q^+ \subseteq P^+$,

3. $P \subseteq Q$ in $Q \setminus P \subseteq Q^0$.

Dokaz : Lastnost $P \subseteq Q$ je ekvivalentna z lastnostjo, da za vsak $a \in R$ iz $a \notin Q$ sledi $a \notin P$, ta pa je ekvivalentna z lastnostjo, da za vsak $a \in R$ iz $Q \in W_T(a)^c$ sledi $P \in W_T(a)^c$. Podobno je lastnost $Q^+ \subseteq P^+$ ekvivalentna z lastnostjo, da za vsak $a \in R$ iz $Q \in U_T(a)$ sledi $P \in U_T(a)$. Tako smo dokazali, da je lastnost *2.* ekvivalentna z lastnostjo,

da vsaka podbazna množica, ki vsebuje Q, vsebuje tudi P. Ta lastnost je ekvivalentna z lastnostjo, da vsaka odprta množica, ki vsebuje Q vsebuje tudi P, kar je ekvivalentno lastnostjo *1.*

Če velja točka *2.*, potem je $Q \setminus P \subseteq Q \setminus P^+ \subseteq Q \setminus Q^+ = Q^0$, torej velja točka *3.* Nasprotno iz točke *3.* sledi $Q^+ = Q \setminus Q^0 \subseteq Q \setminus (Q \setminus P) \subseteq P$ in $P^0 \subseteq Q^0$. Odtod sledi točka *2.* Q.E.D.

Iz naslednjega izreka sledi, da je spektralni prostor $\mathrm{Sper}_T(R)$ popolnoma normalen.

Izrek 8 *Za poljubni točki $P, Q \in \mathrm{Sper}_T(R)$ sta ekvivalentni trditvi:*

1. *P in Q imata disjunktni h-odprti okolici,*

2. *$P \not\leq Q$ in $Q \not\leq P$.*

Dokaz : Naj velja točka *2.* Ker $P \neq Q$, lahko privzamemo $P \not\subseteq Q$. Vzemimo poljuben $a \in P \setminus Q$. Če $a \notin P^0$, potem je $P \in U_T(a)$ in $Q \in W_T(a)^c$. Če tak a ne obstaja, je $P \setminus Q \subseteq P^0$. Ker $Q \not\leq P$, sledi po točki *3.* izreka 7, da je $Q \not\subseteq P$. Vzemimo poljuben element $b \in Q \setminus P$. Če $b \notin Q^0$, potem $Q \in U_T(b)$ in $P \in W_T(b)^c$. V nasprotnem primeru vzemimo poljubna elementa $a \in P \setminus Q \subseteq P^0$ in $b \in Q \setminus P \subseteq Q^0$. Velja $Q \in U_T(a^n - b^n)$ in $P \in W_T(a^n - b^n)^c$. Q.E.D.

Za poljuben element $a \in R$ iz za poljubno število m med 1 in n definirajmo množici

$$\begin{aligned} U_T(a,m) &= U_T(a^m) \cap \bigcap_{\substack{k|m \\ k \neq m}} W_T(a^k)^c, \\ W_T(a,m) &= W_T(a^m) \cap \bigcap_{\substack{k|m \\ k \neq m}} U_T(a^k)^c. \end{aligned}$$

Velja $W_T(a,m) = U_T(a,m) \cup Z_T(a)$. Za komplemente velja

$$\begin{aligned} U_T(a,m)^c &= \bigcup_{\substack{k|n \\ k \neq m}} W_T(a,k), \\ W_T(a,m)^c &= \bigcup_{\substack{k|n \\ k \neq m}} U_T(a,k). \end{aligned}$$

Za poljubne elemente $a_1, \ldots, a_k \in R$ in za poljubna naravna žtevila $1 \leq m_1, \ldots, m_k \leq n$ definirajmo

$$U_T(a_1, \ldots, a_k; m_1, \ldots, m_k) = U_T(a_1, m_1) \cap \ldots \cap U_T(a_k, m_k),$$

$$W_T(a_1,\ldots,a_k;m_1,\ldots,m_k) \;=\; W_T(a_1,m_1)\cap\ldots\cap W_T(a_k,m_k).$$

Tem množicam recimo *temeljne odprte* oziroma *temeljne zaprte* množice. Iz zvez $U_T(a) = U_T(a,1)$ in $W_T(a) = W_T(a,1)$ in iz formul za komplemente sledi, da temeljne odprte množice tvorijo bazo Harrisonove topologije in da preseki temeljnih odprtih množic z množicami oblike $Z_T(b)$ tvorijo bazo konstruktibilne topologije.

Trditev 9 *Vsaka odprta konstruktibilna množica je enaka končni uniji temeljnih odprtih množic. Vsaka zaprta konstruktibilna množica je enaka končni uniji temeljnih zaprtih množic.*

Dokaz : Prva trditev sledi direktno iz kompaktnosti konstruktibilne topologije. Odtod sledi, da je vsaka zaprta konstruktibilna množica enaka končnemu preseku komplementov temeljnih odprtih množic. Odtod in iz formul za komplemente množic $U_T(a,m)$ sledi druga trditev. Q.E.D.

8.3 Naravna projekcija iz $\mathrm{Sig}_T(R)$ na $\mathrm{Sper}_T(R)$

Preslikavi $P:\ \mathrm{Sig}_T(R)\to\mathrm{Sper}_T(R)$ definirani s $P(\sigma)=\sigma^{-1}(\{0,1\})$ bomo rekli *naravna projekcija*. Očitno se strogi eksponent poljubne T-signaturo σ ujema z strogim eksponentom pripadajoče T-ureditve $P(\sigma)$. Naj bo ϕ Eulerjeva funkcija iz teorije števil.

Lema 10 *Naj bo σ poljubna T-signatura na kolobarju R in naj bo m njen strogi eksponent. Potem poljubna signatura τ pripada množici $P^{-1}(P(\sigma))$ natanko tedaj ko obstaja tako naravno število r med 1 in m, ki je tuje proti m in velja $\tau=\sigma^r$. Moč množice $P^{-1}(P(\sigma))$ je enaka $\phi(m)$.*

Dokaz : Če je $P(\tau)=P(\sigma)$, potem iz opombe pred lemo sledi, da imata signaturi τ in σ enak strogi eksponent. Naj bosta a,b poljubna elementa kolobarja R. Izjava $\tau(a)=\tau(b)$ je ekvivalentna z $ab^{m-1}\in P(\tau)$, ta je po izbiri τ ekvivalentna z $ab^{m-1}\in P(\sigma)$, ki je ekvivalentna z izjavo $\sigma(a)=\sigma(b)$. Odtod sledi, da je s $f(\zeta^k)=\tau(\sigma^{-1}(\zeta^k))$ podana injektivna preslikava $f:\ \mu_m\to\mu_m$. Očitno je ta preslikava bijektiven homomorfizem grup, za te pa vemo, da so ravno potenciranja s števili tujimi proti m. Po definiciji Eulerjeve funkcije ϕ je med 1 in m, ravno $\phi(m)$ števil, ki so tuja proti m. Ko potenciramo σ s temi števili dobimo različne signature. Q.E.D.

Naslednja lema nam pove, da je naravna projekcija zvezna glede na Harrisonovo topologijo.

Lema 11 *Za poljuben element $a \in R$ in poljubno naravno število m, ki deli n, velja $P^{-1}(U_T(a,m)) = \bigcup D_T(a,r)$, kjer r teče po vseh številih med 1 in n, ki zadoščajo $(n,r) = \frac{n}{m}$.*

Dokaz : Naj bo r poljubno število, ki zadošča $(n,r) = \frac{n}{m}$. Za poljubno T-signaturo $\sigma \in D_T(a,r)$ velja $\sigma(a^m) = \zeta^{mr} = 1$. Če za nek k, ki strogo deli m, velja $\sigma(a^k) = 1$, potem je $\zeta^{rk} = 1$, torej $n|rk$. Odtod sledi protislovje, da $m = \frac{n}{(n,r)}$ deli k. Tako smo dokazali, da $a^m \in P(\sigma)$ in $a^k \notin P(\sigma)$ za vsak k, ki strogo deli m. Torej $P(\sigma) \in U_T(a,m)$.

Vzemimo tako signaturo σ, da velja $P(\sigma) \in U_T(a,m)$. Naj bo $\sigma(a) = \zeta^r$, torej $\sigma \in D_T(a,r)$. Dokazati moramo še, da velja $(n,r) = \frac{n}{m}$. Po definiciji množice $U_T(a,m)$ je $\zeta^{mr} = \sigma(a^m) = 1$ in $\zeta^{kr} = \sigma(a^k) \neq 1$ za vsak k, ki strogo deli m. Ker n deli mr, sledi, da $\frac{n}{(n,r)}$ deli m. Ker n ne deli mk, za noben k, ki strogo deli m, sledi $\frac{n}{(n,r)} = m$, torej je $(n,r) = \frac{n}{m}$. Q.E.D.

Naj bo $p_k : \mathrm{Sig}_T(R) \to \mathrm{Sig}_T(R)$ preslikava definirana s $p_k(\sigma) = \sigma^k$.

Lema 12 *Če je število k tuje proti n, potem je p_k avtohomeomorfizem prostora $\mathrm{Sig}_T(R)$ in za vsako število m, ki deli n, njegova slika tranzitivno deluje na družino množic $\{D_T(a,r);\ 1 \leq r \leq n,\ (n,r) = \frac{n}{m}\}$.*

Dokaz : Ker je število k tuje proti n, obstajata taki števili c in d, da velja $ck + dn = 1$. Preslikava ϕ_c je inverz preslikave ϕ_k.

Za poljuben $a \in R$ in poljubno število i med 1 in n velja $p_k(D_T(a,i)) \subseteq D_T(a,ki)$ in $p_c(D_T(a,ki)) \subseteq D_T(a,cki) = D_T(a,i)$, torej je $p_k(D_T(a,i)) = D_T(a,ki)$. Odtod sledi, da je p_k homoemorfizem in da njegova slika deluje na omenjeno družino.

Tranzitivnost delovanja je posledica naslednje pomožne trditve: *Za poljubni naravni števili r in t velja $(n,r) = (n,t)$ natanko tedaj, ko obstaja tako število l tuje proti n, da velja $lr \equiv t\ (n)$.*

Naj bo $r' = \frac{r}{(n,r)}$ in $t' = \frac{t}{(n,t)}$. Ker je r' tuj proti n obstajata taki števili p in q, da velja $pn + qr' = 1$. Naj bo $l = qt'$. Ker sta q in t' tuja proti n je tudi l tuje proti n. Velja tudi $t - lr = t - qt'r'(n,r) = t - qr't = tpn$, torej je $lr \equiv t\ (n)$. Nasprotna smer je očitna. Q.E.D.

Označimo s Spec(n) množico vseh T-ureditev strogega eksponenta n. Naj bo Sig(n) množica vseh T-ureditev strogega eksponenta n. Množica Spec(n) je neprazna natanko tedaj, ko je množica Sig(n) neprazna.

Naj bo P poljubna T-ureditev strogega eksponenta n. Potem obstaja tak element $a \in R$, da velja $P \in U_T(a, n)$. Toda očitno množica $U_T(a, n)$ vsebuje samo ureditve strogega eksponenta n. Množica Spec(n) je torej odprta v Spec$_T(R)$. Ker je P zvezna preslikava, je tudi množica Sig(n) odprta v Sig$_T(R)$.

Izrek 13 *Prostor* Sig(n) *je* $\phi(n)$*-listen krovni prostor prostora* Spec(n).

Za vsako naravno število k *tuje proti* n *je preslikava* p_k *krovna transformacija.*

Dokaz : Po lemi 10 preslikava p_k ohranja vlakna. Po lemi 12 je p_k avtohomeomorfizem. Torej je p_k krovna transformacija. Po lemi 11 velja $P^{-1}(U_T(a, n)) = \bigcup D_T(a, r)$, kjer r teče po vseh številih med 1 in n, ki so tuja proti n. Očitno so množice iz gornje unije med seboj disjunktne in po lemi 12 so med seboj homeomorfne. Torej je preslikava $P|_{\text{Sig(n)}}$ $\phi(n)$-listna krovna projekcija. Q.E.D.

Trditev 14 *Preslikava* P *je zvezna in zaprta glede na topologijo Tihonova.*

Dokaz : Vemo, da množice $U_T(a, m)$ in $Z_T(a)$ tvorijo podbazo topologije Tihonova. Za poljuben element $a \in R$ in za poljubno T-signaturo σ na R velja $a \in P(\sigma)^0$ natanko tedaj ko velja $\sigma(a) = 0$. Torej velja $\sigma \in N_T(a)$ natanko tedaj, ko velja $P(\sigma) \in Z_T(a)$. Zveznost preslikave P v topologiji Tihonova sedaj sledi iz leme 11. Zaprtost sledi is dejstva, da sta topologiji Tihonova kompaktni in Hausdorfovi. Q.E.D.

8.4 Prostor T-realnih praidealov

Na prostoru Sig$_T(R)$ lahko definiramo *topologijo Zariskega* s podbazo $\{N_T(a)^c;\ a \in R\}$ in *konstruktibilno topologijo Zariskega* s podbazo $\{N_T(a);\ a \in R\} \cup \{N_T(a)^c;\ a \in R\}$. Ker sta obe topologiji šibkejši od topologije Tihonova na Sig$_T(R)$ sta kompaktni.

Ali je prostor Sig$_T(R)$ s topologijo Zariskega spektralen? Žal je odgovor na to vprašanje negativen. Obstaja lahko namreč več T-signatur z istim nosilcem. Take signature so v topologiji Zariskega nerazločljive in zato topologija Zariskega nima niti lastnosti T_0. Torej prostor Sig$_T(R)$ s topologijo Zariskega v splošnem ni niti predspektralen. Podobno

lahko definiramo topologijo Zariskega in konstruktibilno topologijo Zariskega na prostoru $\mathrm{Sper}_T(R)$. Tudi tu ne dobimo spektralnega prostora iz istih razlogov.

Kaj pa če bi lastnost T_0 prisilno uvedli tako, da bi identificirali topološko nerazločljive točke? Bolj elegantna rešitev je, da se omejimo na množico vseh praidealov, ki so nosilci kake T-signature. Takim idealom recimo *T-realni* ideali. Množico vseh T-realnih idealov na katero uvedemo relativno topologijo iz $\mathrm{Spec}(R)$ označimo s $\mathrm{Spec}_T(R)$.

Pravimo, da je praideal $\mathbf{p}$ na kolobarju R *T-kompatibilen*, če zadošča $\mathbf{p} \cap 1 + T = \emptyset$ in če za poljubna elementa $t_1, t_2 \in T$ iz predpostavke $t_1 + t_2 \in \mathbf{p}$ sledi $t_1, t_2 \in \mathbf{p}$. Iz osnovnega izreka in presečne lastnosti kolobarja R sledi, da je poljuben praideal $\mathbf{p}$ na R T-realen natanko tedaj, ko je T-kompatibilen.

Ali prostor $\mathrm{Spec}_T(R)$ podeduje spektralno strukturo prostora $\mathrm{Spec}(R)$? Žal je to vprašanje nesmiselno, saj spekter nekomutativnega kolobarja v splošnem ni spektralni prostor. Znano je, da se da spekter nekomutativnega kolobarja gosto vložiti v primeren spektralen prostor (glej [39]). V nadaljevanju bomo direktno, brez uporabe tega rezultata, dokazali, da je ob stalnih predpostavkah na R in T, prostor $\mathrm{Spec}_T(R)$ spektralen.

Množicam oblike $O_T(a) = \{\mathbf{p} \in \mathrm{Spec}_T(R);\ a \notin \mathbf{p}\}$ recimo z-podbazične množice. Množicam, ki so bodisi z-podbazične bodisi komplementi z-podbazičnih množic recimo, cz-podbazične množice. Končnim presekom z-podbazičnih množic pravimo z bazične množice, končnim presekom cz-podbazičnih množic pa cz-bazične množice. Prve tvorijo bazo topologije Zariskega, druge pa bazo *konstruktibilne topologije Zariskega.* Kot smo že navajeni velja naslednji izrek.

Izrek 15 *Če na množici* $\mathrm{Spec}_T(R)$ *vzamemo topologijo Zarskega, potem velja:*

1. $\mathrm{Spec}_T(R)$ *je spektralen prostor.*
2. *Podmnožica prostora* $\mathrm{Spec}_T(R)$ *je z-kompaktna in z-odprta natanko tedaj, ko je enaka končni uniji z-bazičnih množic.*
3. *Podmnožica prostora* $\mathrm{Spec}_T(R)$ *je konstruktibilna natanko tedaj, ko je enaka končni uniji cz-bazičnih množic.*
4. *Konstruktibilna topologija na* $\mathrm{Spec}_T(R)$ *je enaka konstruktibilni topologiji Zariskega.*

Dokaz : Očitno ima prostor $\mathrm{Spec}_T(R)$ lastnost T_0. *Naravna preslikava* $S:\ \mathrm{Sper}_T(R) \to \mathrm{Spec}_T(R)$ definirana z $S(P) = P^0$ je surjektivna in njena praslika ohranja podbazične

množice za konstruktibilno topologijo Zariskega, zato je P v tej topologijhi zvezna. Odtod sledi, da sta obe topologiji na $\mathrm{Spec}_T(R)$ kompaktni. Preostanek dokaza je podoben dokazu izreka 2. Q.E.D.

8.5 Hörmander-Lojasiewiczeva neenakost

V tem razdelku predpostavljamo, da je eksponent prave predureditve T enak potenci števila 2. To ima za Harrisonovo topologijo pomembne posledice.

Trditev 16 *Pri gornjih predpostavkah velja:*

1. *Temeljne odprte množice so oblike $U_T(a_1) \cap \ldots \cap U_T(a_k)$.*
2. *Temeljne zaprte množice so oblike $W_T(a_1) \cap \ldots \cap W_T(a_l)$.*

Dokaz : Za vsak naraven k velja $U_T(a, 2k) = U_T(-a^k)$ in $U_T(a, 2k+1) = \emptyset$. Odtod sledi prva trditev. Druga trditev sledi iz zveze $W_T(a, m) = U_T(a, m) \cup Z_T(a)$ in iz prve trditve. Q.E.D.

Trditev 17 *Pri gornjih predpostavkah za vsako zaprto konstruktibilno množico S obstaja tako naravno število r in take prave predureditve $T_1, \ldots, T_r$, ki vsebujejo T in zadoščajo*

$$S = \mathrm{Sper}_{T_1}(R) \cup \ldots \cup \mathrm{Sper}_{T_r}(R).$$

Dokaz : Po trditvi 9 je vsaka zaprta konstruktibilna množica enaka končni uniji temeljnih konstruktibilnih množic. Po trditvi 16 je vsaka temeljna zaprta množica oblike $W_T(a_1) \cap \ldots \cap W_T(a_l)$, kjer $a_1, \ldots, a_l \in R$. Velja $W_T(a_1) \cap \ldots \cap W_T(a_l) = \mathrm{Sper}_{T'}(R)$, kjer je T' najmanjša predureditev, ki vsebuje predureditev T in elemente $a_1, \ldots, a_l$. Če T' ni prava predureditev, potem velja $\mathrm{Sper}_{T'}(R) = \emptyset$. Q.E.D.

Naslednji izrek je posplošitev abstraktne Hörmander-Lojasiewiczeve neenakosti.

Izrek 18 *Naj bo eksponent prave predureditve T potenca števila 2, Naj bo $S \subseteq \mathrm{Sper}_T(R)$ zaprta konstruktibilna množica in naj bosta $a, b \in R$ taka elementa, da velja $S \cap Z_T(b) \subseteq Z_T(a)$. Potem obstaja tako naravno število k, da velja*

$$a^{nk+1} \in P - \Sigma(Tb^nT)$$

za vsako T-ureditev $P \in S$.

Dokaz : Po trditvi 17 obstaja tako naravno število r in take prave predureditve $T_1, \ldots, T_r$, ki vsebujejo T in zadoščajo $S = \mathrm{Sper}_{T_1}(R) \cup \ldots \cup \mathrm{Sper}_{T_r}(R)$.

Naj bo i poljubno naravno število med 1 in r. Vzemimo poljubno T-ureditev P, ki vsebuje T_i in ki zadošča $b^n \notin P^+$. Potem je $b \in P^0$, torej velja $P \in \mathrm{Sper}_{T_1}(R) \cap Z_T(b) \subseteq S \cap Z_T(b) \subseteq Z_T(a)$. Zato je $a \in P^0$. Po izreku 12 iz šestega poglavja odtod sledi, da obstaja tako naravno število k_i, da velja $-a^{nk_i} \in T_i - \sum(\Pi_n b^n \Pi_n)$.

Naj bo $k = k_1 + \ldots + k_r$. Potem za vsak $i = 1, \ldots, r$ obstajajo taki elementi $s_i \in T_i$ in $u_{ij}, v_{ij} \in \Pi_n$, da velja $-a^{nk} = s_i + \sum_j u_{ij} b v_{ij}$. Naj bosta $s, t \in T^e$ taka elementa, da velja $a = s - t$. Za poljubno naravno število m med 1 in r velja $t \sum_{i=1}^r \sum_j u_{ij} b^n v_{ij} + a^{nk+1} = t(\sum_{i=1}^r \sum_j u_{ij} b^n v_{ij} - a^{nk}) + s a^{nk} = t(\sum_j u_{mj} b^n v_{mj} t - a^{nk}) + (t \sum_{i \neq m} \sum_j u_{ij} b^n v_{ij} + s a^{nk}) \in T_m^e + \Sigma_n \subseteq T_m^e$. Za poljubno T-ureditev $P \in S$ velja $\bigcap_{m=1}^r T_k^e \subseteq P^e = P$, zato je $t \sum_{i=1}^r \sum_j u_{ij} b^n v_{ij} + a^{nk+1} \in P$. S tem je izrek dokazan. Q.E.D.

9.

Reducirana teorija form

Ko želimo teorijo kvadratnih form na komutativnih obsegih posplošiti bodisi na nekomutativne obsege bodisi ne forme višjega reda, naletimo na mnoge težave. Najbolj priljubljen izhod iz teh težav je, da se omejimo na reducirane teorije form. Splet teorij, ki nastopajo ob teh vprašanjih kaže naslednji komutativni diagram teorij in njihovih posplošitev.

linearno		abstraktni		
urejeni	$\rightarrow$	prostori		
obsegi		ureditev		
$\downarrow\uparrow$		$\downarrow\uparrow$		
reducirane		reducirane		teorija
kvadratne forme	$\rightarrow$	specialne	$\overset{\rightarrow}{\leftarrow}$	Booleovih
na obsegih		grupe		algeber
$\downarrow$		$\downarrow$		$\downarrow$
reducirane forme		reducirane		
višjega reda	$\rightarrow$	formne sheme	$\overset{\rightarrow}{\leftarrow}$	?
na obsegih		višjega reda		
$\uparrow\downarrow$		$\uparrow\downarrow$		
ureditve		abstraktni		
višjega reda	$\rightarrow$	prostori		
na obsegih		signatur		

Abstraktne prostore ureditev in reducirane specialne grupe je vpeljal Murray Marshall. V svojih člankih je dokazal, da sta si ta dva pojma dualna in da prostor (linearnih) ureditev

na (lahko nekomutativnem) obsegu zadošča aksiomomo abstraktnega prostora ureditev.

Abstraktne prostore signatur je vpeljal Culm Mulcahy. Teorijo formnih shem višjega reda sta razvila Murray Marshall in Victoria Powers in pokazala, da so reducirane formne sheme dualne abstraktnim prostorom signatur. Reducirano teorijo form višjega reda za komutativne obsege sta razvila Eberhared Becker in Alex Rosenberg v članku [44]. Na nekomutativne obsega jo je posplošila Victoria Powers. V člankih [45] in [24] je pokazala, da so izpolnjeni aksiomi prostora signatur.

Zvezo med teorijo kvadratnih form in teorijo Booloeovih algeber je razvil Thomas Craven v svoji disertaciji. Na abstraktne prostore signatur sta jo posplošila Max Dickmann in Francesco Miraglia, [48].

V prvih dveh razdelkih bomo povzeli dualnost med abstraktnimi prostori signatur in formalno realnimi reduciranimi formnimi shemami. V tretjem razdelku bomo povzeli osnove teorije Postovih algeber. Četrti in peti razdelek vsebujeta originalne prispevke. Konstruirali bomo Postovo ovojnico abstraktnega prostora signatur. S tem želimo pokazati, da Postove algebre dobro nadomestijo ? v gornjem diagramu.

Nastanek tega poglavja ne bil bil mogoč brez pogovorov z Maxom Dickmannom, Daniello Gondard in Andrejo Prijatelj.

9.1 Prostori signatur

Vse Abelove grupe v tem razdelku bodo multiplikativne in njihov nevtralni element bomo vedno označili z 1. Označimo z μ grupo vseh kompleksnih števil z absolutno vrednostjo 1. Za vsako naravno število n označimo z μ_n podgrupo grupe μ, ki vsebuje vse kompleksne n-te korene enice. Za poljubno Abelovo grupo G označimo z $G^* = \mathrm{Hom}(G, \mu)$ njeno *grupo karakterjev*. Množenje in invertiranje sta definirana po točkah. Če eksponent grupe G deli n, potem je $G^* = \mathrm{Hom}(G, \mu_n)$. Na grupi G^* vzamemo relativno topologijo iz prostora $\mu^G = \prod_{g \in G} \mu$. Njeno podbazo tvorijo množice $O(g, \omega) := \{\phi \in G^*;\ \phi(g) = \omega\}$, kjer sta $g \in G$ in $\omega \in \mu$ poljubna. V tej topologiji je G^* Booleov prostor.

Urejeno trojko $(X, G, -1)$, kjer je G Abelova grupa končnega eksponenta, $-1 \in G$ in $X \subset G^*$ imenujemo *predprostor signatur*, če velja

1. Za vsak $\sigma \in X$ in vsako liho naravno število l je $\sigma^l \in X$.

2. Množica X je zaprta v G^*.

3. Za vsak element $\sigma \in X$ velja $\sigma(-1) = -1$.

4. Če za nek element $x \in G$ velja $\sigma(x) = 1$ za vsak $\sigma \in X$, potem je $x = 1$.

Iz tretjega aksioma sledi, da $-1 \neq 1$. Iz tretjega in četrtega aksioma sledi, da je $(-1)^2 = 1$. Odtod sledi, da je eksponent grupe G sodo število. Eksponentu grupe G recimo *strogi eksponent* prostora signatur $(X, G, -1)$. Iz drugega aksioma sledi, da je X Booleov prostor.

Za poljubna elementa $a, b \in G$ označimo z $D\langle a, b\rangle$ množico vseh tistih elementov $z \in G$ za katere obstaja tak element $x \in G$, da za vsak $\sigma \in X$ velja $\sigma(a) + \sigma(b) = \sigma(z) + \sigma(x)$. (Vsote jemljemo v kompleksnih številih in lahko padejo ven iz μ!) Predprostor signatur $(X, G, -1)$ se imenuje *prostor signatur*, če zadošča naslednji lastnosti.

5. za poljubna $x, y \in G$ velja $\bigcup_{s \in D\langle 1,x\rangle} D\langle y, s\rangle = \bigcup_{t \in D\langle 1,y\rangle} D\langle x, t\rangle$.

Prvi izrek daje najpomembnejši primer prostora signatur. Za dokaz glej reference v uvodu tega poglavja.

Izrek 1 *Naj bo D poljuben obseg in T poljubna prava predureditev na D. Definirajmo $G_T = D^\times/T^\times$. Vsaka T-signatura σ inducira nek karakter na G_T. Množico vseh takih karakterjev označimo z X_T. Naj bo $-1_T = -1 + T^\times \in G_T$. Potem je $(X_T, G_T, -1_T)$ prostor signatur.*

Naslednja elementarna lema bo zelo koristna v nadaljevanju.

Lema 2 *Naj bo n poljubno sodo naravno število. Za poljubne elemente $a, b, c, d \in \mu_n$ se ekvivalentne trditve:*

1. *$a + b = c + d$,*

2. *$a = -b$ in $c = -d$ ali $a = c$ in $b = d$ ali $a = d$ in $b = c$,*

3. *$a^l + b^l = c^l + d^l$ za vsako liho naravno število l.*

Izrek 3 *Naj bo n sodo naravno število,* id $: \mu_n \to \mu_n$ *identična preslikava in $X_n = \{\mathrm{id}, \mathrm{id}^3, \mathrm{id}^5, \ldots, \mathrm{id}^{n-1}\}$. Potem je trojka $(X_n, \mu_n, -1)$ prostor signatur.*

Dokaz : Očitno je $(X_n, \mu_n, -1)$ predprostor signatur. Preverimo sedaj dodatni aksiom prostora signatur. Za poljuben element $z \in \mu_n$ so ekvivalentne trditve:

1. $z \in \bigcup_{s \in D\langle 1,x\rangle} D\langle y, s\rangle$.

2. Obstajajo taki elementi $p, q, r \in \mu_n$, da velja $z + p = y + q$ in $q + r = 1 + x$.

3. Velja bodisi $z = y$ bodisi $x = -1$ bodisi se množici $\{z, -y\}$ in $\{x, 1\}$ sekata

4. $x = -1$ ali $y = -1$ ali $y = -x$ ali $z = x$ ali $z = y$ ali $z = 1$.

5. Velja bodisi $z = x$ bodisi $y = -1$ bodisi se množici $\{z, -x\}$ in $\{y, 1\}$ sekata.

6. Obstajajo taki elementi $u, v, w \in \mu_n$, da velja $z + u = x + v$ in $v + w = 1 + y$.

7. $z \in \bigcup_{t \in D\langle 1,y\rangle} D\langle x, t\rangle$.

Ekvivalenci med 1. in 2. ter med 6. in 7. sledita iz definicij in leme 2. Ekvivalentnost med 3., 4. in 5. je očitna. Če velja 2., in $z \neq y$ in $x \neq -1$, potem je $\{z, -y\} = \{q, -p\}$ in $\{q, r\} = \{1, x\}$, torej $q \in \{z, -y\} \cap \{x, 1\}$ in zato velja 3. Naj velja 3.. Če je $z = y$, potem vzemimo $p = q = 1$ in $r = x$. Če je $x = -1$, potem vzemimo $p = y$, $q = z$ in $r = -z$. Če $z \neq y$ in $x \neq -1$, potem vzemimo $q \in \{z, -y\} \cap \{x, 1\}$. Potem je $p := y + q - z \in \mu_n$, $r = 1 + x - q \in \mu_n$ in velja $z + p = y + q$ ter $q + r = 1 + x$. Torej velja 2. Analogno dokažemo ekvivalentnost trditev 5. in 6. Q.E.D.

Izrek 4 *Naj bo $(X, G, -1)$ prostor signatur in $\chi \in G^*$ tak element, da velja $\chi(-1) = -1$ in $\chi(a) + \chi(b) = \chi(c) + \chi(d)$ za poljubne elemente $a, b.c, d \in G$, ki zadoščajo $\sigma(a) + \sigma(b) = \sigma(c) + \sigma(d)$ za poljuben $\sigma \in X$. Potem je $\chi \in X$.*

Dokaz : Glej [43] diskusijo lastnosti S_5 in S_5^* ter Corollary 2.2. Q.E.D.

Vsakemu homomorfizmu grup $\phi : G \to G'$ priredimo njegov *dualni homomorfizem* $\phi^* : G'^* \to G^*$ s predpisom $\phi^*(\chi) = \chi \circ \phi$. Ker za poljubna $g \in G$ in $\omega \in \mu_n$ velja $(\phi^*)^{-1}(O(g, \omega)) = \{\chi \in G'^*;\ \phi^*(\chi)(g) = \omega\} = \{\chi \in G'^*;\ \chi(\phi(g)) = \omega\} = O'(\phi(g), \omega)$, je ϕ^* zvezna preslikava.

Izrek 5 *Naj bosta $(X, G, -1)$ in $(X', G', -1)$ poljubna prostora signatur in $\phi : G \to G'$ poljuben homomorfizem grup. Potem so naslednje trditve ekvivalentne:*

1. $\phi(-1) = -1$ in za vsak element $a \in G$ velja $\phi(D\langle 1, a\rangle) \subseteq D'\langle 1, \phi(a)\rangle$,

2. $\phi(-1) = -1$ *in za poljubne elemente* $a, b, c, d \in G$, *ki zadoščajo* $\sigma(a) + \sigma(b) = \sigma(c) + \sigma(d)$ *za vsak* $\sigma \in X$, *velja* $\tau(\phi(a)) + \tau(\phi(b)) = \tau(\phi(c)) + \tau(\phi(d))$ *za vsak* $\tau \in X'$.

3. $\phi^*(X') \subseteq X$.

Dokaz : Ker je G grupa in ϕ homomorfizem grup, lahko v točki 2. brez škode za splošnost predpostavimo $b = 1$. Ekvivalenca med 1. in 2. je sedaj direktna posledica definicije množic $D\langle ., . \rangle$. Iz 3. takoj sledi 2, obratna smer, pa sledi iz izreka 4. Q.E.D.

Homomorfizem grup $\phi : G \to G'$, ki zadošča eni od ekvivalentnih lastnosti v izreku 5 imenujemo *homomorfizem prostorov signatur* $(X, G, -1)$ in $(X', G', -1)$. Kategorijo prostorov signatur in njihovih homomorfizmov označimo z **Sos**. Naj bo $\mathbf{Sos}_n$ polna podkategorija prostorov signatur strogega eksponenta n.

9.2 Prostori form, dualnost

Naj bo G množica. Elementom množice $\bigcup_{m=0}^{\infty} G^m$, kjer je G^m kartezični produkt m kopij množice G, pravimo *forme* na G. Poljubno relacijo $\simeq$ na množici $G^2 = G \times G$ lahko razširimo do relacije $\simeq_m$ na G^m. Naj bosta $\simeq_0$ in $\simeq_1$ enakosti in $\simeq_2 = \simeq$. Ostale relacije defiramo rekurzivno. Za poljubne elemente $a_1, \ldots, a_m, b_1, \ldots, b_m \in G$ in poljubno naravno število $m \geq 3$ definirajmo $(a_1, \ldots, a_m) \simeq_m (b_1, \ldots, b_m)$ natanko tedaj, ko obstajajo taki elementi $x, y, c_3, \ldots, c_m \in G$, da je $(a_2, \ldots, a_m) \simeq_{m-1} (x, c_3, \ldots, c_m)$, $(b_2, \ldots, b_m) \simeq_{m-1} (y, c_3, \ldots, c_m)$ in $(a_1, x) \simeq_2 (b_1, y)$. Če je $\simeq$ ekvivalenčna relacija, potem ni nujno, da so tudi relacije $\simeq_m$ ekvivalenčne.

Naj bo sedaj G Abelova grupa končnega eksponenta, $-1 \in G$ in naj bo $\simeq$ relacija na $G \times G$. Urejeno trojko $(G, \simeq, -1)$ imenujemo *prostor form*, (= form scheme, special group) če velja:

1. $(a, b) \simeq (b, a)$ za poljubna $a, b \in G$,

2. Za poljubne $a, b, c \in G$ iz $(a, b) \simeq (a, c)$ sledi $b = c$.

3. Relacija $\simeq_3$ je tranzitivna.

4. Za vsak $a \in G$ velja $(a, -a) \simeq (1, -1)$.

5. Če je $(a,b) \simeq (c,d)$, potem je $(xa,xb) \simeq (xc,xd)$ za vsak $x \in G$.

Iz druge in četrte lastnosti sledi, da je $(-1)^2 = 1$. Prostor form je *reduciran*, če velja

6. Za poljubna elementa $a,b \in G$ iz $(a,b) \simeq (1,1)$ sledi $a = b = 1$.

Prostor form je *formalno realen*, če velja

7. Za poljubno naravno število m velja $(-1,\ldots,-1) \not\simeq_m (1,\ldots,1)$.

Zgodovinsko najpomembnejši prostor form je prostor kvadratnih form na danem komutativnem obsegu F s karakteristiko različno od 2. Definirajmo $G = F^\times/(F^\times)^2$. Tej grupi se reče *grupa kvadratičnih razredov.* Za poljubne elemente $\overline{a},\overline{b},\overline{c},\overline{d} \in G$ definirajmo $(\overline{a},\overline{b}) \simeq (\overline{c},\overline{d})$ natanko tedaj, ko sta matriki $\mathrm{diag}(a,b)$ in $\mathrm{diag}(c,d)$ kongruentni. Očitno je ta definicije neodvisna od izbire predstavnikov kvadratičnih razredov. Potem je trojka $(G,\simeq,-1)$ prostor form. V tem primeru je relacija $\simeq_m$ inducirana s kongruenčno relacijo na diagonalnih nesingularnih $m\times m$ matrikah. Ta prostor form je reduciran natanko tedaj, ko je F Pitagorejski obseg in formalno realen natanko tedaj, ko je obseg F formalno realen. Ker tega primera v nadaljevanju ne bomo potrebovali, dokaz opustimo.

Izrek 6 *Naj bo $(X,G,-1)$ prostor signatur in $a,b,c,d \in G$. Definirajmo $(a,b) \simeq_X (c,d)$ natanko tedaj, ko za vsak $\sigma \in X$ velja $\sigma(a)+\sigma(b) = \sigma(c)+\sigma(d)$. Potem je $(G,\simeq_X,-1)$ reduciran formalno realen prostor form.*

Dokaz : Glej [42], stran 4087, zgled (3). Q.E.D.

Prostor form, ki po izreku 5 pripada prostoru T-signatur iz izreka 1, pravimo *prostor T-reduciranih form.* Prostor form, ki po izreku 5 pripada prostoru signatur iz izreka 3 označimo s S_n. Naj bodo $a,b,c,d \in \mu_n$ poljubni elementi. Po lemi 2 je $(a,b) \simeq_{X_n} (c,d)$ natanko tedaj, ko je $a+b = c+d$.

Homomorfizem iz prostora form $(G,\simeq,-1)$ v prostor form $(G',\simeq' .-1')$ je tak grupni homomorfizem $f:\ G \to G'$, da velja $f(-1) = -1'$ in za poljubne elemente $a,b,c,d \in G$ iz $(a,b) \simeq (c,d)$ sledi $(f(a),f(b)) \simeq' (f(c),f(d))$. Kategorijo reduciranih formalno realnih prostorov form in njihovih homomorfizmov označimo z **Rsg**.

Naj bo G Abelova grupa eksponenta n. Homomorfizmom iz danega prostora form $S = (G,\simeq,-1)$ v prostor form S_n, pravimo *signature* na S. Množico vseh signatur na S označimo z $X(S)$.

Izrek 7 *Naj bo S reduciran prostor form. Potem je množica $X(S)$ neprazna natanko tedaj, ko je prostor S formalno realen.*

Dokaz : Glej [42], Corollary 6.8. Q.E.D.

Naslednji izrek je posplošitev Pfisterjevega lokalno-globalnega principa.

Izrek 8 *Naj bo $S = (G, \simeq, -1)$ reduciran formalno realen prostor signatur in $a_1, \ldots, a_m$, $b_1, \ldots, b_m \in G$ poljubni elementi. Potem velja $(a_1, \ldots, a_m) \simeq_m (b_1, \ldots, b_m)$ natanko tedaj, ko za vsak $\sigma \in X(S)$ velja $\sigma(a_1) + \ldots + \sigma(a_m) = \sigma(b_1) + \ldots + \sigma(b_m)$.*

Dokaz : Glej [42], Theorem 6.7. Q.E.D.

Izrek 9 *Za vsak reduciran formalno realen prostor form $S = (G, \simeq, -1)$ je $(X(S), G, -1)$ prostor signatur.*

Dokaz : . Prva lastnost prostora signatur sledi neposredno iz leme 2. Tretja lastnost sledi iz definicije signature, četrta iz izreka 8, peta pa iz [42], Theorem 1.2. Dokazujemo drugo lastnost. Po definiciji topologije na G^* je zaprtje množice $X(S)$ enako množici vseh takih karakterjev iz G^*, ki se na vsaki končni podmnožici grupe G ujemajo s kakim elementom iz $X(S)$. Vzemimo poljuben $\sigma \in \overline{X(S)}$. Ker se σ na množici $\{-1\}$ ujema z nekim elementom iz $X(S)$, velja $\sigma(-1) = -1$. Vzemimo poljubne elemente $a, b, c, d \in G$, ki zadoščajo $(a, b) \simeq (c, d)$. Ker se σ na množici a, b, c, d ujema z nekim elementom iz $X(S)$, velja $\sigma(a) + \sigma(b) = \sigma(c) + \sigma(d)$. Torej $\sigma \in X(S)$. Q.E.D.

Za vsak prostor form $S = (G, \simeq, -1)$ definirajmo $\Phi(S) = (X(S), G, -1)$. Za vsak prostor signatur $(X, G, -1)$ definirajmo $\Psi((X, G, -1)) = (G, \simeq_X, -1)$. Homomorfizme naj Φ in Ψ kar ohranjata. Po izrekih izrekih 6 in 9 sta Φ in Ψ funktorja med kategorijama **Rsg** in **Sos**. Očitno so morfizmi v eni kategoriji natanko isti homomorfizmi grup kot morfizmi v drugi kategoriji in očitna sta v tem smislu oba funktorja konstantna na morfizmih.

Izrek 10 (Dualnost) *Funktorja Φ in Ψ sta si inverzna.*

Dokaz : Za vsak prostor form $S = (G, \simeq, -1)$ velja $\Phi(\Psi(S)) = \Phi((X(S), G, -1)) = (G, \simeq_{X(S)}, -1)$. Toda po izreku 7 je $\simeq_{X(S)} = \sigma$. Za poljuben prostor signatur $(X, G, -1)$

velja $\Psi(\Phi((X,G,-1))) = \Psi((G,\simeq_X,-1))$. Izrek 4 da $\Psi((G,\simeq_X,-1)) = (X,G,-1)$. Q.E.D.

9.3 Postove algebre

Za vsak Booleov prostor X obstaja bijektivna korespondenca med njegovimi odprto-zaprtimi množicami in zveznimi funkcijami iz X v diskreten topološki prostor $\mu_2 = \{1,-1\}$. Odtod sledi, da je vsaka Booleova algebra izomorfna Booleovi algebri oblike $(C(X,\mu_2),\cap,\cup,1,-1)$, kjer je X Booleov prostor 1 in -1 konstantni funkciji in $\cap$ ter $\cup$ definirani po točkah.

Kaj pa če namesto μ_2 vzamemo μ_n, kjer je n poljubno naravno število? Definirajmo na μ_n ureditev $1 \leq \zeta \leq \cdots \leq \zeta^{n-1}$. Na množici $L := C(X,\mu_n)$ definirajmo operaciji $\cap$ in $\cup$ po točkah. Za vsak $i \in \{0,\cdots,n-1\}$ naj bo c_i konstantna funkcija ζ^i. Očitno je $(L,\cap,\cup,c_0,c_{n-1})$ omejena distributivna mreža, ki zadošča $c_0 \leq c_1 \leq \ldots \leq c_{n-1}$. Njena množica komplementiranih elementov C(L) sestoji iz natanko tistih zveznih funkcij, katerih zaloga vrednosti je vsebovana v $\{c_0,c_{n-1}\}$.

Izrek 11 *1. Za vsak element $a \in L$ obstajajo taki $a_1,\ldots,a_{n-1} \in C(L)$, da je $a = (a_1 \cap c_1) \cup \ldots \cup (a_{n-1} \cap c_{n-1})$,*

2. Za vsak element $a \in C(L)\backslash\{c_0\}$ in za vsak indeks $i \in \{0,\ldots,n-2\}$ velja $a \cap c_{i+1} \not\leq c_i$.

Dokaz : Naj bo $a_i(x) = c_{n-1}$, če je $a(x) \geq i$ in naj bo $a_i(x) = c_0$, če je $a(x) < i$. Druga trditev je očitna. Q.E.D.

Ta izrek motivira definicijo Postove algebre: (omejena distributivna) mreža L je *Postova algebra*, če obstajajo taki elementi $c_0 \leq c_1 \leq \ldots \leq c_{n-1} \in L$, ki izpolnjujejo točki 1. in 2. iz izreka 11

Izkaže se, da so število n in elementi $c_0,c_1,\ldots,c_{n-1}$ enolično določeni. Številu n pravimo *red* Postove algebre L. V točki 2. lahko zahtevamo $a_1 \leq \ldots \leq a_{n-1}$. V tem primeru so elementi $a_1,\ldots,a_{n-1}$ enolično določeni ([47]).

Izrek 12 *Vsaka Postova algebra L reda n je izomorfna Postovi algebri oblike $C(X,\mu_n)$, kjer je X Booleov prostor Boolove algebre $C(L)$.*

Dokaz : [46] Theorem 16. Q.E.D.

Naj bo **BS** kategorija Boolovih prostorov in $\mathbf{PS}_n$ kategorija Postovih algeber reda n z mrežnimi homomorfizmi, ki ohranjajo konstante. Definirajmo funktor $P_n : \mathbf{BS} \to \mathbf{PA}_n$. Za vsak Booleov prostor K definirajmo $P_n(K) = C(K, \mu_n)$. Za vsako pravo preslikavo $\phi : K' \to K$ Booleovih prostorov K' in K definirajmo $P_n(\phi)(f) = f \circ \phi$ za vsak $f \in C(K, \mu_n)$.

Izrek 13 *Za vsako naravno število n je funktor P_n antiekvivalenca kategorij* **BS** *in* $\mathbf{PA}_n$.

Dokaz : Funktorialnost je očitna. Bijektivnost na objektih sledi iz prejšnjega izreka. Zaradi enoličnosti razcepa v prvi definicijski lastnosti Postovih algeber sledi po krajšem računu, da je vsak morfizem Postovih algeber natanko določen že s svojo skrčitvijo na množico komplementiranih elementov. Odtod sledi, da so morfizmi v $\mathbf{PA}_n$ v bijektivni korespondenci z morfizmi v **BA**, ti pa so v bijektivni korespondenci z morfizmi v **BS**. Q.E.D.

Spektralne prostore, ki po Stoneovi antiekvivalenci ustrezajo Postovim algebram imenujemo *Postovi prostori*. Red Postovega prostora naj bo red pripadajoče Postove algebre. Naj bo n dano fiksno naravno število.

Rezultate tega rezdelka lahko strnemo v naslednji komutativni diagram kategorij in funktorjev.

$$\begin{array}{ccccc} \mathbf{PA}_n & \to & \mathbf{D01} & \to & \mathbf{BA} \\ \downarrow & & \downarrow & & \downarrow \\ \mathbf{PS}_n & \to & \mathbf{SS} & \to & \mathbf{BS} \end{array}$$

V gornji vrsti so kategorije Postovih algeber reda n, omejenih distributivnih mrež in Booleovih algeber. V spodnji vrsti se nahajajo kategorije Postovih prostorov reda n, spektralnih prostorov in Booleovih prostorov. Navpični funktorji so skrčitve Stoneove antiekvivalence. Leva vodoravna funktorja sta pozabljiva funktorja. Desna vodoravna funktorja sta C in D.

Gornja vodoravna funktorja nista ekvivalenci kategorij, njun kompozitum pa je Analogno velja za spodnja funktorja. To sledi iz dejstva, da je funktor $P_n : \mathbf{BS} \to \mathbf{PA}_n$ iz izreka 13 antiekvivalenca kategorij in da komutira z ostalimi funktorji v diagramu.

9.4 Prostor signatur Postove algebre

Naj bo K poljuben Booleov prostor in n poljubno sodo naravno število. Funkcija $f : K \to \mu_n$ je zvezna natanko tedaj, ko obstaja taka particija prostora K na odprto-zaprte množice, da je f na vsakem elementu te particije konstantna. Naj bo $G_K = C(K, \mu_n)$ grupa vseh zveznih funkcij iz K v μ_n, kjer je množenje definirano po točkah. Grupa G_K je Abelova in ima eksponent n. Naj bo G_K^* grupa karakterjev grupe G_K s topologijo iz razdelka 1. Vsakemu elementu $x \in K$ lahko priredimo njegovo *evaluacijo* $e_x \in G_K^*$, ki je definirana s predpisom $e_x(f) = f(x)$. Množico vseh evaluacij in vseh njihovih lihih potenc označimo z E_K. Naj bo $-1 \in G_K$ konstantna funkcija -1.

Izrek 14 *Naj bo K poljuben Booleov prostor in n poljubno sodo naravno število, Potem je $(E_K, G_K, -1)$ prostor signatur.*

Dokaz : Lastnosti 1. 3. in 4. prostora signatur sledijo direktno iz definicij.

Dokažimo najprej lastnost 2. Iz lastnosti 4. sledi, da je naravna $i : K \to G_K^*$, ki je definirana z $i(x) = e_x$, injektivna. Ker je množica $i^{-1}(O(g, \omega)) = \{x \in K;\ e_x(g) = \omega\} = g^{-1}(\omega)$ odprta v K za vsak $g \in G_K$ in vsak $\omega \in \mu_n$, je i zvezna preslikava. Ker slika iz kompaktnega v Hausdorfov prostor, je i zaprta vložitev. Za vsako naravno število l naj bo $p_l : G_K^* \to G_K^*$ potenciranje z l. Kar je $p_l^{-1}(O(g, \omega)) = O(g^l, \omega)$, je funkcija p_l zvezna. Kar je G_K^* kompakten in Hausdorfov je preslikava p_l tudi zaprta. Ker je $E_K = \bigcup p_l(i(K))$, kjer unija teče po vseh lihih številih med 1 in n, je E_K res zaprta množica.

Dokažimo še lastnost 5. Naj bosta $x, y \in G_K$ poljubna elementa. Vzemimo poljuben element $z \in \bigcup_{s \in D\langle 1,x\rangle} D\langle y, s\rangle$. Po definiciji te množice obstajajo taki elementi $p, q, r \in G_K$, da velja $e(z) + e(p) = e(y) + e(q)$ in $e(q) + e(r) = e(1) + e(x)$, kjer je e poljubna liha potenca poljubna evaluacije. Odtod sledi $z + p = y + q$ in $q + r = 1 + x$. Naj bo $K = \bigcup_{i=1}^r C_i$ taka particija prostora K na odprto zaprte množice, da so za vsak $i = 1, \ldots, r$ skrčitve funkcij x, y, z, p, q, r na C_i konstantne. Naj bo $x_i = x(C_i)$, in naj bodo y_i, z_i, p_i, q_i, r_i definirani analogno. Po izreku 3 obstajajo za vsak $i = 1, \ldots, r$ taki elementi $u_i, v_i, w_i \in \mu_n$, da velja $z_i + u_i = x_i + v_i$ in $v_i + w_i = 1 + y_i$. Definirajmo $u = \sum_{i=1}^r u_i\chi_i$, $v = \sum_{i=1}^r v_i\chi_i$ in $w = \sum_{i=1}^r w_i\chi_i$, kjer je χ_i karakteristična funkcija množice C_i. Ker so funkcije u, v, w konstantne na vsakem elementu odprto-zaprte particije $K = \bigcup_{i=1}^r C_i$, so te funkcije zvezne, torej pripadajo G_X. Ker velja $z + u = x + v$ in $v + w = 1 + y$, velja po lemi 2 tudi $e(z) + e(u) = e(x) + e(v)$ in $e(v) + e(w) = e(1) + e(y)$, kjer je e poljubna liha

potenca poljubne evaluacije. Odtod sledi $z \in \bigcup_{t \in D\langle 1,y\rangle} D\langle x,t\rangle$. Dokaz nasprotne inkluzije je simetričen. Q.E.D.

Po lemi 2 je izometrična relacija $\simeq$, ki pripada prostoru signatur $(X, G, -1)$ definirana s $(a,b) \simeq (c,d)$ natanko tedaj, ko $a+b=c+d$, kjer a,b,c,d gledamo kot kompleksne funkcije na G in jih seštevamo po točkah.

Naš naslednji namen je odgovoriti na tole vprašanje. *Ali se homomorfizmi Postovih algeber v kategoriji prostorov form ujemajo s homomorfizmi v kategoriji omejenih distributivnih mrež?* Odgovor na to vprašanje je pritrdilen v primeru $n = 2$. (glej [48], Proposition 4.6) V primeru $n \neq 2$ to v splošnem ne drži kot kaže naslednji enostavni primer. Edini endomorfizem Postove algebre μ_n je identiteta, endomorfizmi pripadajočega prostora form, pa so vse lihe potence. Velja pa naslednji izrek:

Izrek 15 *Vsak homomorfizem Postovih algeber je tudi homomorfizem pripadajočih prostorov signatur,*

Dokaz : Po izreku 13 je vsak homomorfizem Φ Postovih algeber $C(K,\mu_n)$ in $C(K',\mu_n)$ oblike $P_n(\phi)$, kjer je $\phi : K' \to K$ zvezna preslikava. Odtod takoj sledi, da je Φ tudi homomorfizem pripadajočih grup G in G', da je $\Phi(-1) = -1$ in da Φ zadošča točki 2. iz izreka 5. Q.E.D.

V primeru $n = 2$ se da izometrična ralacija na Booleovi algebri preprosto opisati z njenimi mrežnimi operacijami. Velja $(a,b) \simeq (c,d)$ natanko tedaj, ko je $a \cup b = c \cup d$ in $a \cap b = c \cap d$. V splošnem primeru dobimo samo naslednjo karakterizacijo.

Izrek 16 *Naj bo n poljubno naravno število in K poljuben Booleov prostor. Za poljubne elemente $a,b,c,d \in C(K,\mu_n)$ sta ekvivalentni trditvi:*

1. $a+b=c+d$,
2. *Velja* $(a \cup b) \cup (-c \cup -d) = (-a \cup -b) \cup (c \cup d)$, $(a \cup b) \cap (-c \cup -d) = (-a \cup -b) \cap (c \cup d)$, $(a \cap b) \cup (-c \cap -d) = (-a \cup -b) \cap (c \cap d)$ *in* $(a \cap b) \cap (-c \cap -d) = (-a \cap -b) \cap (c \cap d)$.

Dokaz : Po lemi 2 velja prva točka natanko tedaj, ko za vsak $x \in K$ velja bodisi $a(x) = c(x)$ in $b(x) = d(x)$ bodisi $a(x) = d(x)$ in $b(x) = c(x)$ bodisi $a(x) = -b(x)$ in $c(x) = -d(x)$.

Ker za vsak $x \in K$ velja $a(x) \neq -a(x)$ in $b(x) \neq -b(x)$ velja ta trditev natanko tedaj, ko za vsak $x \in K$ velja $\{\{a(x), b(x)\}, \{-c(x), -d(x)\}\} = \{\{-a(x), -b(x)\}, \{c(x), d(x)\}\}$.

Ker sta dve dvoelementni množici enaki natanko tedaj, ko imata enak minimum in enak maksimum, je druga točka ekvivalentna z naslednjo trditvijo: za vsak element $x \in K$ velja: $\{a(x) \cup b(x), -c(x) \cup -d(x)\} = \{-a(x) \cup -b(x), c(x) \cup d(x)\}$ in $\{a(x) \cap b(x), -c(x) \cap -d(x)\} = \{-a(x) \cap -b(x), c(x) \cap d(x)\}$.

Odtod takoj vidimo, da iz prve točke sledi druga, obratna smer pa zahteva še nekaj dodatnega dela. Naj velja trditev iz drugega odstavka. Za vsak element $x \in K$ ločimo tri možnosti:

1. $a(x) \cup b(x) \neq c(x) \cup d(x)$
2. $a(x) \cap b(x) \neq c(x) \cap d(x)$.
3. $a(x) \cup b(x) = c(x) \cup d(x)$ in $a(x) \cap b(x) = c(x) \cap d(x)$.

V prvem primeru dobimo $a(x) \cup b(x) = -a(x) \cup -b(x)$ in $c(x) \cup d(x) = -c(x) \cup -d(x)$. V drugem primeru dobimo $a(x) \cap b(x) = -a(x) \cap -b(x)$ in $c(x) \cap d(x) = -c(x) \cap -d(x)$. V obeh primerih množica $\{a(x), b(x)\}$ seka množico $\{-a(x), -b(x)\}$ in množica $\{c(x), d(x)\}$ seka množico $\{-c(x), -d(x)\}$, torej velja $\{a(x), b(x)\} = \{-a(x), -b(x)\}$ in $\{-c(x), -d(x)\} = \{c(x), d(x)\}$. Iz tretjega primera takoj sledi $\{a(x), b(x)\} = \{c(x), d(x)\}$ in $\{-c(x), -d(x)\} = \{-a(x), -b(x)\}$. V vseh treh primerih torej velja trditev iz prvega odstavka. Q.E.D.

9.5 Postova ovojnica prostora signatur

Naj bo n fiksno sodo naravno število. V tem razdelku predpostavljamo, da so vsi prostori signatur strogega eksponenta n in da sa vse Postove algebre reda n.

Naj bo $(X, G, -1)$ poljuben prostor form. Vsakemu elementu $g \in G$ lahko priredimo neko preslikavo $\epsilon(g) : X \to \mu_n$ s predpisom $\epsilon(g)(\chi) = \chi(g)$. Ker je $\epsilon(g)^{-1}(\omega) = \{\chi \in X;\ \chi(g) = \omega\} = X \cap O(g, \omega)$, je $\epsilon(g) \in C(X, \mu_n) = G_X$.

Predpis $g \to \epsilon(g)$ definira neko preslikavo $\epsilon : G \to C(X, \mu_n)$. Zaradi lastnosti 4. prostorov signatur, je ta preslikava injektivna. Po lemi 2 velja $\epsilon^*(E_X) \subseteq X$, torej je ϵ homomorfizem prostorov signatur.

Naj bo $\phi : \ (X, G, \mu_n) \to (Y, H, \mu_n)$ homomorfizem prostorov signatur. Po izreku 5 velja $\phi^*(Y) \subseteq X$. Po diskusiji pred izrekom 5, je ϕ^* zvezna preslikava. Torej je $f \to f \circ \phi^*|Y$ dobro definirana preslikava iz $G_X = C(X, \mu_n)$ v $G_Y = C(Y, \mu_n)$, ki jo lahko izrazimo tudi kot $P_n(\phi^*|Y)$. Ta preslikava je homomorfizem grup in slika -1 v -1. Iz leme 2 in točke 2. izreka 5 sledi, da je preslikava $P_n(\phi^*|_Y)$ homomorfizem iz prostora signatur $(E_X, G_X, -1)$ v prostor signatur $(E_Y, G_Y, -1)$. Funktorialnost te preslikave je očitna.

Funktorju $PH_n : \ \mathbf{Sos_n} \to \mathbf{PA}_n$, ki je definiran z $PH_n((X, G, -1)) = (E_X, G_X, -1)$ in $PH_n(\phi : (X, G, -1) \to (Y, H, -1)) = P_n(\phi^*|Y)$ pravimo *Postova ovojnica*. Ime ovojnica opravičuje naslednja univerzalna lastnost:

Izrek 17 *Naj bo G grupa eksponenta n, $(X, G, -1)$ prostor signatur, in $\epsilon : \ (X, G, -1) \to (E_X, G_X, -1)$ naravna vložitev. Za poljubno Postovo algebro G_K in poljuben homomorfizem $\phi : \ (X, G, -1) \to (E_K, G_K, -1)$ prostorov signatur, obstaja natanko en tak homomorfizem $h : \ G_X \to G_K$ Postovih algeber, da velja $\phi = h \circ \epsilon$.*

Dokaz : Dokažimo najprej enoličnost preslikave h. Ker je h homomorfizem Postovih algeber, obstaja po izreku 13 taka zvezna preslikava $\alpha : \ K \to X$, da je $h = P_n(\alpha)$. Naj bo $i : \ K \to E_K$ preslikava definirana z $i(x) = e_x$, kjer je e_x evaluacija v točki x. Ker velja $\phi = P_n(\alpha) \circ \epsilon$, lahko za poljuben $x \in K$ in poljuben $g \in G$ napravimo naslednji račun: $(\phi^* \circ i)(x)(g) = \phi^*(e_x)(g) = (e_x \circ \phi)(g) = \phi(g)(x) = (P_n(\alpha) \circ \epsilon)(g)(x) = P_n(\alpha)(\epsilon(g))(x) = (\epsilon(g) \circ \alpha)(x) = \epsilon(g)(\alpha(x)) = \alpha(x)(g)$. Odtod sledi, da je $\alpha = \phi^* \circ i$, torej je enoličnost preslikave h dokazana.

Dokažimo sedaj eksistenco preslikave h. Definirajmo preslikavo $\alpha = \phi^* \circ i$. Ker je ϕ homomorfizem prostorov signatur, je $\phi^*(E_K) \subseteq X$, torej je zaloga vrednosti preslikave α vsebovana v X. Po diskusiji pred izrekom 5 je preslikava ϕ^* zvezna. Ker za poljubna $f \in G_K$ in $\omega \in \mu_n$.velja $i^{-1}(O_K(f, \omega)) = \{x \in K; i(x)(f) = \omega\} = \{x \in K; f(x) = \omega\} = f^{-1}(\omega)$, je preslikava i zvezna. Torej je $\alpha : \ K \to X$ zvezna preslikava. Definirajmo $h := P_n(\alpha)$. Po izreku 13 je h homomorfizem Postovih algeber. Za poljubna $g \in G$ in $x \in K$ velja $(h \circ \epsilon)(g)(x) = P_n(\alpha)(\epsilon(g))(x) = (\epsilon(g) \circ \alpha)(x) = \epsilon(g)(\alpha(x)) = \alpha(x)(g) = (\phi^* \circ i)(x)(g) = \phi^*(e_x)(g) = (e_x \circ \phi)(g) = e_x(\phi(g)) = \phi(g)(x)$, torej je $h \circ \epsilon = \phi$. Q.E.D.

Literatura

[1] Knebusch, Manfred and Claus Scheiderer, *Einführung in die reelle Algebra*, Friedr. Vieweg & Sohn, Braunschweig/Wiesbaden 1989.

[2] Lavrič, Boris, *Delno urejene grupe in delno urejeni kolobarji*. DMFA Slovenije, Ljubljana 1993.

1. poglavje

[3] Rotman, J. J., *Introduction to the theory of groups*, 4th edition, Graduate Texts in Mathematics **148**, Springer, New York 1995.

[4] Cimprič, Jaka, On homomomorphisms from semigroups onto cyclic groups, to appear in Semigroup Forum.

2. poglavje

[5] Weinert, H. J., On the extension of partial orders on semigroups of right quotients, Trans. Amer. Math. Soc. **142** (1969), 345–353.

[6] Hebisch, Udo, Partial orders in semigroups and semirings of right quotients, Semigroup Forum **49** (1994), 165–174.

[7] Cimprič, Jaka, Preorderings on semigroups and semirings of right quotients, to appear in Semigroup Forum.

3. poglavje

[8] Kadison, Richard V., A representation theory for commutative topological algebra, Mem. Amer. Math. Soc., **7** (1951), no. 7, 39 pp.

[9] Harrison, D. K., Finite and infinite primes for rings and fields, Mem. Amer. Math. Soc. No. **68** (1966), 62 pp.

[10] Dubois, D. W., A note on David Harrison's theory of preprimes, Pacific J. Math. **21** (1967), 15–19.

[11] Dubois, D. W., Second note on David Harrison's theory of preprimes, Pacific J. Math. **24** (1968), 57–68.

[12] Becker, Eberhard and Niels Schwartz, Zum Darstellungssatz von Kadison-Dubois, Arch. Math. (Basel) **40** (1983), no. 5, 421–428.

4. poglavje

[13] Malcev, A., On the immersion of an algebraic ring into a field, Math. Ann. **113** (1937), 686–691.

[14] Vinogradov, A. A., On the theory of ordered semigroups, Sci. Proc. Ivanovo Pedagogical Inst. **4** (1953), 19–21.

5. poglavje

[15] Artin, E. and O. Schreier, Algebraische Konstruktion reeller Korper, Abh. Math. Sem. Univ. Hamburg **5** (1927), 85–99.

[16] Becker, Eberhard, *Hereditarily-Pythagorean fields and orderings of higher level*, Inst. Mat. Pura Apl., Rio de Janeiro, 1978.

[17] Becker, Eberhard, Summen n-ter Potenzen in Körpern, J. Reine Angew. Math. **307/308** (1979), 8–30.

[18] Becker, Eberhard, Partial orders on a field and valuation rings, Comm. Algebra **7** (1979), no. 18, 1933–1976

[19] Becker, Eberhard, The real holomorphy ring and sums of $2n$th powers, in *Real algebraic geometry and quadratic forms (Rennes, 1981)*, 139–181, Lecture Notes in Math., 959, Springer, Berlin, 1982.

[20] Becker, Eberhard, Extended Artin-Schreier theory of fields, Rocky Mountain J. Math. **14** (1984), no. 4, 881–897.

[21] T. Szele, On ordered skew fields, Proc. Amer. Math. Soc. **3** (1952), 410–413.

[22] R. E. Johnson, On ordered domains of integrity, Proc. Amer. Math. Soc. **3** (1952) 414–416.

[23] T. C. Craven, Witt rings and orderings of skew fields, J. Algebra **77** (1982), 74–96.

[24] Powers, Victoria, Holomorphy rings and higher level orders on skew fields, J. Algebra **136** (1991), no. 1, 51–59.

[25] Becker, E. et al., Hilbert's 17th problem for sums of $2n$th powers, J. Reine Angew. Math. **450** (1994), 139–157.

[26] M. D. Choi, T. Y. Lam, A. Prestel in B. Reznick, Sums of $2m$-th powers of rational functions in one variable over real closed fields, *Math. Z.* **221** (1996), no 1, 93-112.

6. poglavje

[27] Scharlau, Winfried, *Quadratic and Hermitian forms*, Springer-Verlag Berlin, 1985 .

[28] G. Stengle, A Nullstellensatz and Positivestellensatz in semialgebraic geometry, *Math. Ann.* **207** (1974) 87-97.

[29] Becker, Eberhard and Gondard, Danielle, On rings admitting orderings and 2-primary chains of orderings of higher level, Manuscripta Math. **65** (1989), no. 1, 63–82.

[30] Berr, Ralph, The intersection theorem for orderings of higher level in rings, Manuscripta Math. **75** (1992), no. 3, 273–277.

[31] Berr, Ralph, Null- and Positivstellensätze for generalized real closed fields, J. Pure Appl. Algebra **125** (1998), no. 1-3, 19–53.

[32] Leung, Ka Hin, Marshall, Murray and Zhang, Yufei, The real spectrum of a noncommutative ring, J. Algebra **198** (1997), no. 2, 412–427.

[33] Powers, V., Higher level orders on noncommutative rings, J. Pure Appl. Algebra **67** (1990), no. 3, 285–298.

[34] Cimprič, Jaka, Orderings of 2-power exponent on noncommutative rings, to appear in J. Pure Appl. Algebra.

7. poglavje

[35] Hochster, M., Prime ideal structure in commutative rings, Trans. Amer. Math. Soc. **142** (1969), 43–60.

[36] Carral, Michel and Coste, Michel, Normal spectral spaces and their dimensions, J. Pure Appl. Algebra **30** (1983), no. 3, 227–235.

8. poglavje

[37] Barton, Susan Maureen, The real spectrum of higher level of a commutative ring, Canad. J. Math. **44** (1992), no. 3, 449–462.

[38] Walter, L., *Orders and signatures of higher level on commutative rings*, Ph. D. thesis, University of Saskatchewan, Saskatoon, Canada, 1994.

[39] Belluce, L. P., Spectral closure for noncommutative rings, Comm. Algebra **25** (1997), no. 5, 1513-1526.

[40] Berr, Ralph, Real algebraic geometry over p-real closed fields, in *Recent advances in real algebraic geometry and quadratic forms(Berkeley, CA, 1990/1991; San Francisco, CA, 1991)*, 47–73, Contemp. Math., 155, Amer. Math. Soc., Providence, RI, 1994.

[41] Berr, Ralph, The p-real spectrum of a commutative ring, Comm. Algebra **20** (1992), no. 10, 3055–3103.

9. poglavje

[42] Marshall, Murray and Powers, Victoria, Higher level form schemes, Comm. Algebra **21** (1993).

[43] Marshall, Murray and Mulcahy, Colm, The Witt ring of a space of signatures, J. Pure Appl. Algebra **67** (1990), no. 2, 179–188.

[44] Becker, Eberhard and Rosenberg, Alex, Reduced forms and reduced Witt rings of higher level, J. Algebra **92** (1985), no. 2, 477–503.

[45] Powers, Victoria, Higher level reduced Witt rings of skew fields, Math. Z. **198** (1988), no. 4, 545–554.

[46] Epstein, George, The lattice theory of Post algebras, Trans. Amer. Math. Soc. **95** (1960), 300–317.

[47] Panti, Giovanni, *Multi-valued Logics*, preprint.

[48] Dickmann, M. and F. Miraglia, *Applications of boolean alhebras in the theory of quadratic forms*, preprint.

Disertacija je plod lastnega
raziskovalnega dela

Cimprič Jaka