UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 2. stopnja

Lara Vukšić

Elementarna ekvivalenca polj z valuacijami in izrek Ax-Kochen-Jeršov

Magistrsko delo

Mentor: prof. dr. Igor Klep

Ljubljana, 2018

Kazalo

Program dela

V magistrskem delu obravnavajte polja z valuacijami. Predstavite Henselova polja in njihove lastnosti ter dokaz izreka Ax-Kochen-Jeršov o elementarni ekvivalenci Henselovih polj.

Osnovna literatura:

- A. Prestel, F. V. Kuhlmann, *On places of algebraic function fields*, Journal für die reine und angewandte Mathematik **353** (1984) 181–195,
- A. Prestel, C. Delzell, *Mathematical Logic and Model Theory*, Springer, London, 2011.

prof. Igor Klep, mentor

Elementarna ekvivalenca polj z valuacijami in izrek Ax-Kochen-Jeršov

Povzetek

Valuacija je homomorfizem, ki slika multiplikativno grupo obrnljivih elementov polja v urejeno abelovo grupo. Če valuacija slika v aditivno grupo celih števil, je diskretna. Chevalleyev izrek nam pove, da lahko vsako valuacijo polja razširimo tudi na nadpolja. Če za vsako algebraično razširitev polja z valuacijo obstaja natanko ena razširitev valuacije, pravimo, da je polje Henselovo. Primeri Henselovih polj so polna polja z diskretno valuacijo.

Dve strukturi v jeziku sta elementarno ekvivalentni natanko tedaj, ko vsak stavek v tem jeziku velja v eni natanko tedaj, ko velja v drugi. Vse izomorfne strukture so elementarno ekvivalentne, obratno pa v splošnem ne velja. Izrek Ax-Kochen-Jeršov za pare Henselovih polj z valuacijo natančno pove, kdaj so elementarno ekvivalentni. Po njegovi posledici vsak stavek velja v polju p-adičnih števil $\mathbb{Q}_p$ za skoraj vsa praštevila p natanko tedaj, ko velja v polju Laurentovih vrst $\mathbb{Z}_p((t))$ za skoraj vsa praštevila p.

Elementary equivalence of valued fields and Ax-Kochen-Eršov theorem

Abstract

A valuation on a field is a homomorphic mapping from the multiplicative group of invertible elements of a field into an ordered abelian group. If it maps into the additive group of integers, it is called discrete. By Chevalley's theorem, every valuation on a field extends to any field extension. Henselian valued fields are those for which valuation extends uniquely to any algebraic field extension. For example, complete discrete valued fields are Henselian.

Two structures of a given language are elementary equivalent if and only if every sentence in this language holds in the first structure if and only if it also holds in the second. All isomorphic structures are elementary equivalent, but the converse is not true in general. The Ax-Kochen-Eršov theorem explains when any two Henselian valued fields are elementary equivalent. As a consequence, a sentence holds in the field of p-adic numbers $\mathbb{Q}_p$ for almost all primes p if and only if it holds in the field of Laurent series $\mathbb{Z}_p((t))$ for almost all primes p.

Math. Subj. Class. (2010): 03C62 , 12J10

Ključne besede: polja z valuacijo, urejene abelove grupe, napolnitev polja z valuacijo, razširitve valuacij, Henselova polja z valuacijo, elementarna ekvivalenca, elementarne razširitve, tipi, nasičene strukture, izrek Ax-Kochen-Jeršov

Keywords: valued fields, ordered abelian groups, completion of valued field, extensions of valuations, Henselian valued fields, elementary equivalence, elementary extensions, types, saturated structures, Ax-Kochen-Eršov theorem

1. Uvod

Glavni rezultat naloge, izrek Ax-Kochen-Jeršov, je zanimiv primer sočasne uporabe sredstev iz različnih matematičnih panog, predvsem komutativne algebre in teorije polj z valuacijami na eni ter teorijo modelov na drugi strani. Leta 1965 sta ga dokazala James Ax in Simon Kochen [2], ameriški in kanadski matematik, prav tako pa neodvisno tudi ruski matematik Juri Jeršov [7].

Naloga je sestavljena iz treh delov. V prvem se pobliže seznanimo z urejenimi abelovimi grupami in valuacijami na poljih. Posebej se osredotočimo na polja z diskretnimi valuacijami in navedemo nekaj algebraičnih lastnosti diskretnih valuacijskih kolobarjev. Na poljih z diskretno valuacijo definiramo absolutno vrednost in napolnitev, ki jo je mogoče predstaviti tudi v obliki potenčnih vrst. Primeri takih napolnitev so polja p-adičnih števil in polja Laurentovih vrst. Spoznamo Chevalleyev izrek, ki nam pove, da lahko vsaki razširitvi polja z valuacijo priredimo tudi razširitev valuacije in nato povemo nekaj lastnosti razširitev valuacij. Pri transcendentni razširitvi polja z netrivialno valuacijo razširitev le-te ni nikoli enolična. Spoznamo polja z valuacijo, za katere velja, da je razširitev valuacije na vsako algebraično razširitev polja enolično določena. Taka polja so Henselova. Kot dokažemo s pomočjo Henselove leme, so vsa polna polja z diskretno valuacijo Henselova.

V drugem delu spoznamo najpomembnejše pojme iz teorije modelov. Po tem, ko definiramo jezik, spoznamo strukture, modele in teorije. Posebej si ogledamo jezik in teorijo urejenih abelovih grup in polj z valuacijami. Spoznamo izomorfnost in elementarno ekvivalenco struktur, potem pa še elementarne vložitve in elementarne razširitve. Poseben primer slednjih so elementarne verige, ki jih v nalogi pogosto uporabljamo. Ogledamo si še konstantne razširitve jezikov, ob katerih spoznamo lemo o diagramu, nato si ogledamo tipe in nasičene strukture, v zvezi s katerimi omenimo nekaj koristnih rezultatov. Potem se seznanimo še z ultrafiltri in ultraprodukti. Posebej si ogledamo ultraprodukta množice polj p-adičnih števil $\mathbb{Q}_p$ oz. polja Laurentovih vrst $\mathbb{Z}_p((t))$ po ultrafiltru, ki je razširitev filtra kokončnih množic.

V zadnjem delu dokažemo še dve verziji izreka Ax-Kochen-Jeršov, ki ima za posledico, da sta zgoraj navedena ultraprodukta elementarno ekvivalentna. Zato vsak stavek v jeziku polj z valuacijami velja v $\mathbb{Q}_p$ za vsa praštevila p razen morda končno mnogo natanko tedaj, ko velja v $\mathbb{Z}_p((t))$ za vsa praštevila p razen morda končno mnogo.

Besedilo naloge predvideva seznanjenost bralca z osnovnimi pojmi iz komutativne algebre, teorije razširitev polj in ordinalne aritmetike, prav tako pa ne škodi seznanjenost z osnovami logike in teorije modelov, četudi najpomembnejše rezultate, potrebne za dokaz izreka Ax-Kochen-Jeršov, dokažemo ali pa vsaj navedemo.

2. Polja z valuacijami

V tem poglavju najprej definiramo urejene abelove grupe in valuacije na poljih v splošnem. Pokažemo, da je valuacijski podkolobar polja natanko določen z valuacijo in da, obratno, vsak valuacijski podkolobar polja natanko določa valuacijo. Po hitri ugotovitvi, da je vsak valuacijski kolobar lokalen, definiramo še residualno polje. Potem se osredotočimo na diskretne valuacije, definiramo napolnitev polja z diskretno valuacijo in razširitve valuacij. Pokažemo, da so polna polja z valuacijo Henselova. Posebej si ogledamo Laurentove vrste s koeficienti v polju praštevilske moči ter p-adična števila.

2.1. **Valuacije.**

2.1.1. *Urejene abelove grupe.* Da definiramo valuacije v splošnem, moramo najprej povedati, kaj so urejene abelove grupe.

Definicija 2.1. Abelova grupa Γ je *urejena*, če obstaja taka relacija $\leq$ na Γ, za katero velja:

(1) $\forall \alpha \in \Gamma : \alpha \leq \alpha$,
(2) $\forall \alpha, \beta \in \Gamma : \alpha \leq \beta \wedge \beta \leq \alpha \Rightarrow \alpha = \beta$,
(3) $\forall \alpha, \beta, \gamma \in \Gamma : \alpha \leq \beta \wedge \beta \leq \gamma \Rightarrow \alpha \leq \gamma$,
(4) $\forall \alpha, \beta \in \Gamma : \alpha \leq \beta \vee \beta \leq \alpha$,
(5) $\forall \alpha, \beta, \gamma \in \Gamma : \alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma$.

Z drugimi besedami, relacija $\leq$ linearno ureja elemente grupe Γ, pri čemer je monotona glede na seštevanje. Z $\alpha < \beta$ označujemo relacijo $\alpha \leq \beta \wedge \alpha \neq \beta$.

S *pozitivnimi* oz. *negativnimi* elementi označimo množico tistih $\alpha \in \Gamma$, za katere velja $0 < \alpha$ oz. $\alpha < 0$, z $\alpha \geq \beta$ pa $\beta \leq \alpha$. Inverz pozitivnega elementa je očitno negativen, iz česar sledi tudi implikacija $\alpha \leq \beta \Rightarrow -\beta \leq -\alpha$.

Očiten primer urejene abelove grupe je aditivna grupa realnih števil $(\mathbb{R}, +)$. Vsaka podgrupa urejene abelove grupe je tudi sama urejena glede na podedovano relacijo. V posebnem sta urejeni abelovi grupi tudi $(\mathbb{Z}, +)$ in $(\mathbb{Q}, +)$.

Vsaka urejena abelova grupa ima trivialen torzijski del. Res: če velja $0 \leq \alpha$, kjer je red elementa $\alpha \in \Gamma$ enak $n \in \mathbb{N}$, iz monotonosti za seštevanje sledi $\alpha \leq (n-1)\alpha$, po drugi strani pa $(n-1)\alpha \leq n\alpha = 0$. Iz tranzitivnosti in antisimetričnosti $\leq$ sledi $\alpha = 0$, kar je mogoče le v primeru $n = 1$. V primeru $\alpha \leq 0$ obrnemo neenakosti in sklepamo analogno. V posebnem velja, da je vsaka netrivialna urejena abelova grupa neskončna.

Definicija 2.2. Urejena abelova grupa Γ je *diskretna*, če obstaja tak element $0 \neq \alpha \in \Gamma$, da velja: $0 \leq \gamma \wedge (\forall \beta \in \Gamma : 0 \leq \beta \Rightarrow \alpha \leq \beta)$. Urejena abelova grupa Γ je *arhimedska*, če za vsaka elementa $\alpha, \beta \in \Gamma$, kjer je $0 < \alpha$, obstaja $n \in \mathbb{N}$, da velja $\beta \leq n\alpha$.

Definicija 2.3. Podgrupa urejene abelove grupe $\Delta \subseteq \Gamma$ je *konveksna*, če za vsaka $\alpha, \beta \in \Gamma$ velja $\beta \in \Delta \wedge 0 \leq \alpha \leq \beta \Rightarrow \alpha \in \Delta$.

Trditev 2.4. *Množica konveksnih podgrup je dobro urejena z relacijo vsebovanosti.*

Dokaz. Relacija vsebovanosti delno ureja $\mathcal{P}(\Gamma)$, zato najprej preverimo, da velja tudi dihotomija. Pa naj bosta $\Delta, \Delta' \subseteq \Gamma$ poljubni in naj velja $\Delta \not\subseteq \Delta'$. Potem obstaja $\alpha \in \Delta \setminus \Delta'$, za katerega lahko brez škode za splošnost predpostavimo $0 \leq \alpha$. Za vsak $\beta \in \Delta'$ velja $\beta < \alpha$, saj bi v nasprotnem primeru zaradi konveksnosti

podgrupe Δ' sledilo $\alpha \in \Delta'$. Ker je tudi Δ konveksna podgrupa Γ, sledi $\beta \in \Delta$ za vsak $\beta \in \Delta'$. Sledi, da relacija vsebovanosti linearno ureja množico vseh konveksnih grup Γ, in ker je, kot ni težko videti, presek poljubne družine konveksnih podgrup tudi sam konveksna podgrupa, je ta urejenost tudi dobra, saj je zaradi linearnosti ureditve najmanjši element poljubne družine konveksnih podrup kar presek vseh elementov. □

Z *rangom* urejene abelove grupe označimo tip ureditve množice vseh konveksnih podgrup z relacijo urejenosti. Urejena abelova grupa ima rang 1 natanko tedaj, ko je netrivialna in nima pravih netrivialnih konveksnih podgrup. $(\mathbb{Z}, +)$ ima rang 1, $(\mathbb{Z}^n, +)$ z leksikografsko ureditvijo pa rang n. Preden definiramo valuacije, bomo karakterizirali grupe ranga 1. Za to bomo najprej pa dokazali kratko lemo.

Lema 2.5. *Urejena abelova grupa ima rang 1 natanko tedaj, ko je arhimedska.*

Dokaz. Naj bo Γ arhimedska grupa. Če bi imela pravo konveksno podgrupo $\Delta \subseteq \Gamma$, bi za poljubna pozitivna $\alpha \in \Delta, \beta \in \Gamma \setminus \Delta$ in poljuben $n \in \mathbb{N}$ veljalo $0 < n\alpha < \beta$, saj je $n\alpha \in \Delta$.

Za dokaz obratne smeri pa predpostavimo, da obtajata taka $\alpha, \beta \in \Gamma, 0 < \alpha$, tako da za vsako naravno število n velja $n\alpha < \beta$. Definirajmo množico $\Delta := \{\gamma \in \Gamma \mid -\gamma, \gamma \leq n\alpha \text{ za nek } n \in \mathbb{N}\}$. Pokažimo, da je ta množica podgrupa. Ker je α pozitiven, velja $0 \in \Delta$. Zaprtost za inverze takoj sledi iz definicije. Naj bosta $\gamma, \delta \in \Delta$. Potem obstajata taka $m, n \in \mathbb{N}$, da je $-\gamma, \gamma \leq m\alpha$ in $-\delta, \delta \leq n\alpha$. Potem je $-(\gamma + \delta), \gamma + \delta \leq (m + n)\alpha$. Pokazali smo, da je Δ podgrupa Γ, ker pa ni niti trivialna niti enaka Γ, saj je $\alpha \in \Delta$ in $\beta \notin \Delta$, prav tako pa je očitno konveksna, sledi, da ima Γ pravo konveksno podgrupo. □

V spodnjem izreku dve urejeni abelovi grupi imenujemo *urejenostno izomorfni* natanko tedaj, ko med njima obstaja izomorfizem, ki ohranja urejenost, ki mu pravimo *urejenostni izomorfizem*. Inverz urejenostnega izomorfizma je očitno tudi sam urejenostni izomorfizem.

Izrek 2.6 ([4, trditev 2.1.1])**.** *Urejena abelova grupa Γ ima rang 1 natanko tedaj, ko je urejenostno izomorfna neki netrivialni podgrupi $(\mathbb{R}, +)$ z urejenostjo, podedovano od $\mathbb{R}$.*

Dokaz. Naj bo $\epsilon \in \Gamma$ poljuben pozitiven. Za vsak $\alpha \in \Gamma$ definiramo množici $L(\alpha) := \{m/n \in \mathbb{Q} \mid n > 0 \text{ in } m\epsilon < n\alpha\}$ in $G(\alpha) := \{m/n \in \mathbb{Q} \mid n > 0 \text{ in } m\epsilon \geq n\alpha\}$. Ker je Γ linearno urejena z $\leq$, za vsak $m/n \in \mathbb{Q}$ velja $m\epsilon < n\alpha$ ali $m\epsilon \geq n\alpha$, torej je $L(\alpha) \cup G(\alpha) = \mathbb{Q}$. Naj velja $m/n \in L(\alpha)$ in $m'/n' \in G(\alpha)$. Pokažimo, da velja $m/n < m'/n'$, pri čemer lahko brez škode za splošnost predpostavimo, da sta imenovalca ulomkov enaka, torej $n = n'$. Potem iz $m\epsilon < n\alpha \leq m'\epsilon$ sledi $m < m'$ in zato tudi $m/n < m'/n$, saj sta tako $\epsilon \in \Gamma$ kot tudi $n \in \mathbb{N}$ pozitivna. Sledi, da sta $L(\alpha)$ in $G(\alpha)$ Dedekindov rez v $\mathbb{Q}$.

Sedaj definiramo preslikavo $r : \Gamma \to \mathbb{R}$, kjer je $r(\alpha)$ za vsak $\alpha \in \Gamma$ tisto realno število, ki pripada Dedekindovem rezu $L(\alpha)$ in $G(\alpha)$. Če pokažemo, da je r urejenostni monomorfizem, smo dokazali trditev. Naj bo $m/n \in L(\alpha)$ in $m'/n' \in L(\beta)$, pri čemer spet predpostavimo $n = n'$. Če je $\alpha \leq \beta$, je očitno $L(\alpha) \subseteq L(\beta)$ in zato $r(\alpha) \leq r(\beta)$. Iz monotonosti za seštevanje iz $m\epsilon < n\alpha$ in $m'\epsilon < n\beta$ sledi $(m + m')\epsilon < n(\alpha + \beta)$, zato velja $(m + m')/n \in L(\alpha + \beta)$. Pokazali smo $L(\alpha) + L(\beta) \subseteq L(\alpha + \beta)$, iz česar sledi $r(\alpha) + r(\beta) \leq r(\alpha + \beta)$. Analogno pokažemo

še $G(\alpha)+G(\beta) \subseteq G(\alpha+\beta)$ in nato sklepamo, da velja $r(\alpha)+r(\beta)=r(\alpha+\beta)$. Preostane nam še, da pokažemo, da je r injektiven. Če za $\alpha \in \Gamma$ velja $r(\alpha)=0$, to med drugim pomeni, da je $-1/n \in L(\alpha)$ in $1/n \in G(\alpha)$ za vsak $n \in \mathbb{N}$. Sledi, da za vsak $n \in \mathbb{N}$ velja $-\epsilon \leq n\alpha \leq \epsilon$. Iz druge neenakosti sledi $\alpha \leq 0$, saj je Γ arhimedska urejena grupa po 2.5. Iz druge neenakosti pa po drugi strani dobimo $-n\alpha = n(-\alpha) \leq \epsilon$, torej je tudi $-\alpha \leq 0$. Iz tega potegnemo sklep, da je r monomorfizem. Trditev je tako dokazana. □

Trditev 2.7. *Vsaka diskretna urejena abelova grupa ranga 1 je urejenostno izomorfna* $(\mathbb{Z},+)$.

Dokaz. Naj bo $\gamma \in \Gamma$ najmanjši pozitiven element. Trdimo, da je $\Gamma = \{n\gamma \mid n \in \mathbb{Z}\}$. Pokazati moramo le inkluzijo iz desne v levo. Pa recimo, da obstaja nek brez škode za splošnost pozitiven $\alpha \in \Gamma$, za katerega velja $n\gamma < \alpha < (n+1)\gamma$. Potem, če od vseh strani neenakosti odštejemo $n\gamma$, dobimo $0 < \alpha - n\gamma < \gamma$, kar je v nasprotju s predpostavko, da je γ najmanjši pozitiven element.

Iz povedanega sledi, da je preslikava, ki vsak $n \in \mathbb{Z}$ slika v $n\gamma$, urejenostni izomorfizem med $(\mathbb{Z},+)$ in Γ. □

2.1.2. *Valuacije na poljih.* Sedaj lahko definiramo valuacije na poljih.

Definicija 2.8. Naj bo K polje, Γ urejena abelova grupa in $\infty \notin \Gamma$. V množici $\Gamma \cup \{\infty\}$ v zgornji definiciji razširimo definicijo seštevanja in relacije neenakosti, tako da za vsak $x \in K$ velja $x < \infty$, $x+\infty = \infty$ in $\infty + \infty = \infty$. *Valuacija na polju* K je surjektivna preslikava $v : K \to \Gamma \cup \{\infty\}$, za katero velja:

(1) $\forall x \in K : v(x) = \infty \Leftrightarrow x = 0$,
(2) $\forall x, y \in K : v(xy) = v(x) + v(y)$,
(3) $\forall x, y \in K : v(x+y) \geq \min\{v(x), v(y)\}$

Pravimo, da je K *polje z valuacijo*, Γ pa *valuacijska grupa.*

V primeru, ko v slika v $(\mathbb{Z},+)$, pravimo, da je v *diskretna valuacija ranga 1* ali, krajše, *diskretna valuacija.* V nalogi se bomo podrobneje posvetili dvem družinam valuacij - valuacijam na racionalnih številih in valuacijam na racionalnih funkcijah nad poljem. Ker gre v obeh primerih za diskretne valuacije, si bomo, potem ko bomo povedali nekaj o valuacijah na splošno, te ogledali podrobneje.

Prva dva aksioma nam povesta, da je v homomorfizem med $(K^\times, \cdot)$ in $(\Gamma,+)$. Najprej pokažimo nekaj preprostih, a pomembnih lastnosti valuacij.

Trditev 2.9. *Za vsako valuacijo* $v : K \to \Gamma \cup \{\infty\}$ *velja:*

(1) $v(1) = 0$,
(2) $\forall x \in K : v(x^{-1}) = -v(x)$.
(3) $\forall x \in K : v(-x) = v(x)$,
(4) $\forall x, y \in K : v(x) < v(y) \Rightarrow v(x+y) = v(x)$.
(5) $\forall x_1, \ldots, x_n \in K : v(x_1 + \ldots + x_n) \geq \min\{v(x_1), \ldots, v(x_n)\}$. *Če obstaja tak* $i, 1 \leq i \leq n$, *da je* $v(x_i) < v(x_j)$ *za vsak* $j \neq i$, *velja enakost.*

Dokaz. Prvi dve lastnosti trditve sledita neposredno iz dejstva da je v homomorfizem grup. Po drugem aksiomu valuacij nato sklepamo, da je tudi $v(-1) = 0$, saj je $0 = v(1) = v((-1)^2) = 2v(-1)$, Γ pa nima elementov končnega reda. Sedaj predpostavimo, da za $x, y \in K$ velja $v(x) < v(y)$. Potem po tretjem aksiomu in pravkar dokazanem velja

$$v(x+y) \geq v(x) \text{ in } v(y) = v(x+y-x) \geq \min\{v(x+y), v(-x)\} = v(x).$$

Če bi veljalo $v(x+y) > v(x)$, bi zaradi predpostavke $v(y) > v(x)$ tako veljalo $v(x) = v(x+y-y) \geq \min\{v(x+y), v(y)\} > v(x)$, kar pa ni mogoče. Zadnjo točko trditve pokažemo z indukcijo po n: v primeru $n = 1$ neenakost velja trivialno. Če je $v(x_1) < v(x_2)$, po prejšnji točki velja $v(x_1 + x_2) = v(x_1)$. V indukcijskem koraku pa izračunamo $v(x_1 + \ldots + x_n + x_{n+1}) \geq \min\{v(x_1 + \ldots + x_n), v(x_{n+1})\} \geq \min\{v(x_1), \ldots, v(x_n), v(x_{n+1})\}$ po indukcijski predpostavki. Če za nek i med 1 in n velja $v(x_i) < v(x_j)$ za vsak $j \neq i$, velja

$$\begin{aligned} v(x_1 + \ldots + x_{n+1}) &= v(x_i + x_1 + \ldots + x_{i-1} + x_{i+1} + \ldots x_{n+1}) \\ &\geq \min\{v(x_i + x_1 + \ldots + x_{i-1} + x_{i+1} + \ldots x_n), v(v_{n+1})\} \\ &= \min\{v(x_i), v(x_n)\} = v(x_i), \end{aligned}$$

spet po indukcijski predpostavki. □

Če si ogledamo podmnožico $\mathcal{O} = \{x \in K \mid v(x) \geq 0\}$ polja z valuacijo K, iz aksiomov valuacije takoj sledi, da je zaprta za množenje in seštevanje ter da vsebuje element 0. Iz tretje točke 2.9 pa sledi, da je zaprta za aditivne inverze. Iz povedanega sledi, da je $\mathcal{O}$ podkolobar polja K.

Definicija 2.10. Naj bo K polje. Podkolobar $R \subseteq K$ je *valuacijski*, če za vsak $x \in K^\times$ velja $x \in K \vee x^{-1} \in K$.

Primer 2.11. Naj bo p praštevilo. Množica $\mathcal{O}_p = \{m/n \mid n > 0, m \perp n, p \perp n\}$ je valuacijski podkolobar $\mathbb{Q}$. ♢

Vsak valuacijski kolobar je očitno cel, komutativen in vsebuje enoto. Iz tretje točke 2.9 sledi, da je za vsako valuacijo v na polju zgoraj definirana množica $\mathcal{O}$ valuacijski kolobar in da je vsak $x \in \mathcal{O}$ obrnljiv v $\mathcal{O}$ natanko tedaj, ko je $v(x) = 0$. Na enak način kot za $\mathcal{O}$ se prepričamo, da je tudi množica $\mathcal{M} = \{x \in K \mid v(x) > 0\}$ zaprta za seštevanje, množenje in aditivne inverze, torej je podkolobar $\mathcal{O}$. Iz drugega aksioma valuacij sledi za vsak $x \in \mathcal{M}, y \in \mathcal{O} : v(xy) = v(x) + v(y) > 0$. Torej je $\mathcal{M}$ ideal kolobarja $\mathcal{O}$. Ker vsebuje vse v $\mathcal{O}$ neobrnljive elemente, sledi, da je $\mathcal{O}$ lokalen kolobar z maksimalnim idealom $\mathcal{M}$. Polje $\overline{K} := \mathcal{O}/\mathcal{M}$ imenujemo *polje ostankov*.

Za vsako valuacijo v na polju K lahko, kor smo ravnokar videli, enolično določimo valuacijski kolobar K. Sedaj pokažimo, da velja tudi obratno, torej da vsak valuacijski pokolobar $\mathcal{O}$ polja K enolično določa valuacijo na polju K.

Izrek 2.12 ([4, trditev 2.1.2])**.** *Naj bo K polje in $\mathcal{O}$ valuacijski kolobar. Potem obstaja urejena abelova grupa Γ in valuacija $v : K \to \Gamma \cup \{\infty\}$, da velja $\mathcal{O} = \{x \in K \mid v(x) \geq 0\}$.*

Dokaz. Z $\mathcal{O}^\times$ označimo multiplikativno grupo obrnljivih elementov $\mathcal{O}$, ki je podgrupa $K^\times$, z Γ pa kvocientno grupo $K^\times/\mathcal{O}^\times$, pri kateri zavoljo lažje razvidnosti uporabimo aditiven zapis: $x\mathcal{O}^\times + y\mathcal{O}^\times := xy\mathcal{O}^\times$. Na Γ definiramo relacijo $x\mathcal{O}^\times \leq y\mathcal{O}^\times \Leftrightarrow x^{-1}y \in \mathcal{O}$. Preverimo, da ta relacija linearno ureja Γ. Njena refleksivnost je očitna. Če velja $x^{-1}y \in \mathcal{O}$ in $y^{-1}x \in \mathcal{O}$, sledi, da je $x^{-1}y$ obrnljiv v $\mathcal{O}$. Zato je $x^{-1}y \in \mathcal{O}^\times$, iz česar sledi $x\mathcal{O}^\times = y\mathcal{O}^\times$. Torej je $\leq$ antisimetrična na Γ. Če pa velja $x^{-1}y \in \mathcal{O}$ in $y^{-1}z \in \mathcal{O}$, je tudi njun produkt $x^{-1}z \in \mathcal{O}$, iz česar sledi tranzitivnost $\leq$ na Γ. Ker je $\mathcal{O}$ valuacijski kolobar, za vsaka $x, y \in K^\times$ velja $x^{-1}y \in \mathcal{O}$ ali $y^{-1}x \in \mathcal{O}$. Pokazali smo, da $\leq$ res linearno ureja Γ.

Sedaj definiramo preslikavo $v : K \to \Gamma \cup \{\infty\}$ na naslednji način: $v(0) = \infty$ in $v(x) = x\mathcal{O}^\times$ za $x \in K^\times$. Iz definicije v sledi, da je v, zožena na $(K^\times, \cdot)$, (naravni)

homomorfizem grup, zato nam preostane, da preverimo še tretji aksiom valuacij. Naj za $x, y \in K$ brez škode za splošnost velja $v(x) \leq v(y)$ oz., po definiciji relacije $\leq$, $x^{-1}y \in \mathcal{O}$. Ker je $1 \in \mathcal{O}$, je tudi $1 + x^{-1}y = x^{-1}(x + y) \in \mathcal{O}$ oz. $v(x + y) \geq v(x) = \min\{v(x), v(y)\}$. □

V primeru, ko za valuacijski kolobar vzamemo kar celo polje, dobimo *trivialno valuacijo*, ki vse obrnljive elemente polja slika v 0. Ker lahko na vsakem polju očitno definiramo trivialno valuacijo, primer 2.11 kaže, da v splošnem valuacijski kolobar polja ni enolično določen. Valuaciji $v : K \to \Gamma \cup \{\infty\}$ in $v' : K \to \Gamma' \cup \{\infty\}$ sta *ekvivalentni*, če jima pripada isti valuacijski kolobar $\mathcal{O} \subseteq K$.

Trditev 2.13 ([4, trditev 2.1.3])**.** *Valuaciji $v_i : K \to \Gamma_i \cup \{\infty\}$ za $i = 1, 2$ sta ekvivalentni če in samo če obstaja urejenostni izomorfizem $\tau : \Gamma_1 \to \Gamma_2$ za katerega je $\tau \circ v_1 = v_2$.*

Dokaz. Če obstaja $\tau : \Gamma_1 \to \Gamma_2$ kot v izreku, je očitno $\mathcal{O}_{v_1} = \mathcal{O}_{v_2}$. Obratno: ker je $v_i : K^\times \to \Gamma_i$ za $i = 1, 2$ surjekcija z jedrom $\mathcal{O}_{v_i}^\times$, obstaja izomorfizem $\tau_i : K^\times/\mathcal{O}_{v_i}^\times \to \Gamma_i$. Če velja $\mathcal{O}_{v_1} = \mathcal{O}_{v_2}$, sledi $K^\times/\mathcal{O}_{v_1}^\times \cong K^\times/\mathcal{O}_{v_2}^\times$, in ker sta $\tau_i : \Gamma_i \to K^\times/\mathcal{O}_{v_i}^\times$ izomorfizma, je $\tau := \tau_2 \circ \tau_1^{-1}$ iskani izomorfizem med Γ_1 in Γ_2. □

Pravimo, da sta valuacijska kolobarja $\mathcal{O}_1$ in $\mathcal{O}_2$ *odvisna*, če je njun produkt $\mathcal{O}_1\mathcal{O}_2$ različen od K. Če velja $\mathcal{O}_1 \subseteq \mathcal{O}_2$, pravimo, da je $\mathcal{O}_2$ *nadkolobar* $\mathcal{O}_1$, in če je $\mathcal{O}_2$ različen od K, sta kolobarja v tem primeru odvisna. Nadkolobar valuacijskega kolobarja je, očitno, tudi sam valuacijski.

Lema 2.14. *Naj bo $\mathcal{O}$ netrivialni valuacijski kolobar polja K. Vsak pravi nadkolobar $\mathcal{O}$ je lokalizacija $\mathcal{O}_P$ pri nekem praidealu $P \subseteq \mathcal{O}$.*

Dokaz. Naj bo $\mathcal{O}'$ nadkolobar valuacijskega kolobarja $\mathcal{O}$ z maksimalnim idealom $\mathcal{M}'$. Potem velja $\mathcal{M}' \subseteq \mathcal{M}$, saj vsak $x \in \mathcal{O}'$, ki ni obrnljiv v $\mathcal{O}'$, ni obrnljiv niti v $\mathcal{O}$. Torej velja $x^{-1} \notin \mathcal{O}$, iz česar sledi $x \in \mathcal{M}$.

Ker je $\mathcal{M}'$ kot maksimalen ideal praideal $\mathcal{O}'$, je tudi praideal $\mathcal{O}$. Če $\mathcal{O}$ lokaliziramo pri $\mathcal{M}'$, je dobljeni kolobar $\mathcal{O}_{\mathcal{M}'}$ enak $\mathcal{O}'$. Res: elementi $\mathcal{O}_{\mathcal{M}'}$ so oblike y/x za $x, y \in \mathcal{O}, y \notin \mathcal{M}'$ in zato vsebovani v $\mathcal{O}'$. Obratno lahko vsak element $x \in \mathcal{O}'$ zapišemo kot $x/1 \in \mathcal{O}_{\mathcal{M}'}$, če je $x \in \mathcal{O}$ in kot $1/x \in \mathcal{O}_{\mathcal{M}'}$ sicer, saj noben $x \in \mathcal{O}' \setminus \mathcal{O}$ ni obrnljiv v $\mathcal{O}'$.

□

Obratno lahko hitro vidimo, da je za vsak praideal $P \subseteq \mathcal{O}$ lokalizacija $\mathcal{O}_P$ nadkolobar $\mathcal{O}$. Spodnja trditev bo s pomočjo zgornje pokazala, da lahko vse nadkolobarje valuacijskega kolobarja $\mathcal{O}$ linearno uredimo z inkluzijo.

Trditev 2.15 ([4, lema 2.3.1])**.** *Naj bo $\mathcal{O}$ netrivialni valuacijski kolobar polja K, ki pripada valuaciji $v : K \to \Gamma \cup \{\infty\}$. Potem je množica konveksnih podgrup Γ v bijektivni korespondenci s praideali $\mathcal{O}$ in zato tudi z množico njegovih nadkolobarjev. Bijekcijo dobimo tako, da:*

- *Konveksni podgrupi $\Delta \subseteq \Gamma$ priredimo množico $P_\Delta := \{x \in K \mid v(x) > \delta \ \ \forall \delta \in \Delta\}$, ki je praideal $\mathcal{O}$,*
- *Praidealu $P \subseteq \mathcal{O}$ priredimo konveksno podgrupo $\Delta_P := \{\gamma \in \Gamma \mid -\gamma, \gamma < v(x) \ \ \forall x \in P\}$.*

Če ima Γ končen rang, sledi, da je ta enak Krullovi dimenziji $\mathcal{O}$.

Opomba 2.16. Iz trditve bo posebej sledilo, da ima vsako polje z diskretno valuacijo Krullovo dimenzijo 1.

Dokaz. Naj bo Δ konveksna podgrupa Γ. Ker za vse $x, y \in P_\Delta$ in $z \in \mathcal{O}$ velja $v(-x) = v(x)$, $v(xz) = v(x) + v(z) > \delta$ in $v(x+y) \geq \min\{v(x), v(y)\} > \delta$ za vsak $\delta \in \Delta$, je P_Δ ideal $\mathcal{O}$. Če $x, y \in K$ nista vsebovana v P_Δ, potem obstajata taka $\delta, \delta' \in \Delta$, da velja $v(x) \leq \delta$ in $v(y) \leq \delta'$, iz česar sledi $v(xy) \leq \delta + \delta' \in \Delta$, torej velja $xy \notin P_\Delta$. P_Δ je zato res praideal kolobarja $\mathcal{O}$.

Sedaj naj bo $P \subseteq \mathcal{O}$ praideal. Pokažimo, da je Δ_P konveksna podgrupa Γ. Iz definicije je razvidno, da je zaprta za aditivne inverze in da iz $0 \leq \gamma \leq \delta, \delta \in \Delta_P$ sledi $\gamma \in \Delta_P$, zato moramo pokazati le še zaprtost Δ_P za seštevanje. Naj bosta $\gamma, \delta \in \Delta_P$. Potem zaradi surjektivnosti v obstajata taka $x, y \in \mathcal{O} \setminus P$, da je $v(x) = \gamma$ in $v(y) = \delta$. Sedaj recimo, da obstaja tak $z \in P$, da je $v(z) \leq \gamma + \delta = v(xy)$. Naj bo $w \in \mathcal{O}$ tak, da je $v(w) = \gamma + \delta - v(z) \geq 0$. Potem velja $v(xy) = v(zw)$, zato obstaja tak $c \in \mathcal{O}^\times$, da je $xyc = zw \in P$. To pa ni mogoče, saj je je P praideal in $x, y, c \notin P$. Pokazali smo, da je Δ_P konveksna podgrupa grupe Γ. Ker je, kot je jasno razvidno iz definicije, $\Delta_{P_\Delta} = \Delta$ in $P = P_{\Delta_P}$, smo pokazali bijektivno korespondenco med konveksnimi podgrupami Γ in praideali $\mathcal{O}$. □

Opomba 2.17. Ko smo dokazovali, da je za konveksno podgrupo Δ P_Δ praideal $\mathcal{O}$, nismo eksplicitno uporabili dejstva, da je Δ konveksna množica, toda bijektivna korespondenca iz trditve še vedno velja, saj za Δ pripadajoč ideal P_Δ sledi, da je $P_\Delta = P_{\Delta'}$, kjer je Δ' neka konveksna podgrupa Γ.

2.2. **Diskretne valuacije.** Kot smo zgoraj že povedali, se bomo v nalogi podrobneje posvetili diskretnim valuacijam, torej tistim, ki slikajo iz polja K v $\mathbb{Z} \cup \{\infty\}$. Preden navedemo nekaj njihovih pomembnih algebraičnih lastnosti, predstavimo primera družin valuacij, ki ju bomo obravnavali skozi celo nalogo.

2.2.1. *Valuacije na racionalnih številih in racionalnih funkcijah.*

Primer 2.18. Naj bo p praštevilo. Definiramo preslikavo $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$: naj bo za $m, n \in \mathbb{Z}, m, n \neq 0$, $v_p(m/n) := \alpha - \beta$, kjer je $m = p^\alpha m', n = p^\beta n', \alpha, \beta \in \mathbb{Z}$ in $p \perp m', n'$ ter $v_p(0) := \infty$. Ta preslikava je dobro definirana, saj če tako števec kot imenovalec pomnožimo z $l \in \mathbb{Z} \setminus \{0\}, l = p^\gamma l', \gamma \in \mathbb{Z}, p \perp l'$, potem je $v_p(ml/nl) = (\alpha + \gamma) - (\beta + \gamma) = v_p(m/n)$.

Preverimo, da za v_p veljajo aksiomi valuacije. Prvi, $v_p(0) = \infty$, velja po definiciji. Za $m_1, n_1, m_2, n_2 \in \mathbb{Z} \setminus \{0\}, m_1 = p^{\alpha_1} m_1', m_2 = p^{\alpha_2} m_2', n_1 = p^{\beta_1} n_1', n_2 = p^{\beta_2} n_2'$ izračunamo

$$v_p(m_1/n_1 \cdot m_2/n_2) = v_p(m_1 m_2/n_1 n_2) = (\alpha_1 + \alpha_2) - (\beta_1 + \beta_2) = v_p(m_1/n_1) + v_p(m_2/n_2).$$

Za izračun v_p vsote lahko brez škode za splošnost predpostavimo, da velja $n_1 = n_2 = p^\beta n$. Zato je $m_1/n_1 + m_2/n_2 = (p^{\alpha_1} m_1' + p^{\alpha_2} m_2')/p^\beta n' = p^\alpha m'/p^\beta n'$, kjer je $m' \perp p$, iz česar sledi $\alpha \geq \{\alpha_1, \alpha_2\}$. Sledi:

$$\begin{aligned} v_p(m_1/n_1 + m_2/n_2) =& \alpha - \beta \geq \min\{\alpha_1, \alpha_2\} - \beta \\ &= \min\{\alpha_1 - \beta, \alpha_2 - \beta\} = \min\{v_p(m_1/n_1), v_p(m_2/n_2)\}. \end{aligned}$$

Valuacijski kolobar, ki pripada v_p, je $\mathcal{O}_p = \{m/n \mid n > 0, m \perp n, p \perp n\}$ iz primera 2.11. Ob ponovnem ogledu definicije je jasno, da je $\mathcal{O}_p = \mathbb{Z}_{(p)}$, lokalizacija kolobarja $\mathbb{Z}$ pri praidealu (p), iz česar sledi, da je $\mathcal{M}_p = p\mathbb{Z}_{(p)}$. Polje ostankov $\overline{K_p}$ je izomorfno $O_p/M_p = \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} = \mathbb{Z}_p$. ♢

Primer 2.19. Tokrat bomo za polje z valuacijo vzeli polje racionalnih funkcij $k(x)$. Naj bo $r \in k[x]$ nerazcepen. Valuacijo $v_r : k(x) \to \mathbb{Z} \cup \{\infty\}$ definiramo tako: za $p, q \in k[x], p = r^\alpha p', q = r^\beta q'$, kjer je $\alpha, \beta \in \mathbb{Z}$ in $r \perp p', q'$, naj bo $v_r(p/q) := \alpha - \beta$ in $v_r(0) = \infty$. Da je v_r dobro definirana valuacija na $k(x)$, se prepričamo na enak način kot pri prejšnjem primeru. ♢

Primer 2.20. Na polju racionalnih funkcij lahko definiramo še eno valuacijo - označimo jo z v_∞. Definiramo $v_\infty : k(x) \to \mathbb{Z} \cup \{\infty\}$ s $v_\infty(p/q) := \deg(q) - \deg(p)$ za $p, q \in k[x] \setminus \{0\}$ in $v_\infty(0) = \infty$. Ker je razlika v razliki stopenj števca in imenovalca enaka, če oba pomnožimo s poljubnim neničelnim polinomom, je v_∞ dobro definirana preslikava. Kot v prejšnjih primerih velja tudi za v_∞ prvi aksiom valuacije po definiciji. Preverimo, da velja še drugi:

$$\begin{aligned} v_\infty(p_1/q_1 \cdot p_2/q_2) =& v_\infty(p_1p_2/q_1q_2) = \deg(q_1q_2) - \deg(p_1p_2) \\ =& (\deg(q_1) + \deg(q_2)) - (\deg(p_1) + \deg(p_2)) \\ =& v_\infty(p_1/q_1) + v_\infty(p_2/q_2). \end{aligned}$$

Tako kot zgoraj bomo pri preverjanju, da velja za vrednost v_∞ vsote racionalnih funkcij $p_1/q_1 + p_2/q_2$ tretji aksiom valuacij, predpostavili $q := q_1 = q_2$.

$$\begin{aligned} v_\infty(p_1/q + p_2/q) =& v_\infty(p_1 + p_2/q) = \deg(q) - \deg(p_1 + p_2) \\ \geq& \deg(q) - \max\{\deg(p_1), \deg(p_2)\} \\ =& \min\{\deg(q) - \deg(p_1), \deg(q) - \deg(p_2)\} \\ =& \min\{v_\infty(p_1/q), v_\infty(p_2/q)\}. \end{aligned}$$

♢

Izrek 2.21 ([4, izrek 2.1.4])**.** *a) Vsaka netrivialna diskretna valuacija, ki slika iz $\mathbb{Q}$, je enaka v_p za neko praštevilo p.*
b) Vsaka netrivialna diskretna valuacija, ki slika iz $k(x)$ in slika $k^\times$ v 0, je enaka bodisi v_p za nek nerazcepen $p \in k[x]$ bodisi v_∞.

Dokaz. a) Naj bo $v : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ netrivialna valuacija. Ker je $v(1) = 0$, za vsak $n \in \mathbb{Z}$ po peti točki 2.9 velja $v(n) \geq 0$. Najprej se prepričajmo, da obstaja tako praštevilo p, da je $v(p) > 0$. V nasprotnem primeru bi namreč za vsako celo število m s primarnim razcepom $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ veljalo $v(m) = \alpha_1 v(p_1) + \dots + \alpha_k v(p_k) = 0$, zato bi za vsak $m/n \in \mathbb{Q}$ veljalo $v(m/n) = v(mn^{-1}) = 0$, kar je v nasprotju s predpostavko, da je v netrivialna valuacija. Torej obstaja neko praštevilo p, da je $v(p) > 0$. Pokažimo, je $v(q) = 0$ za vsa druga praštevila $q \neq p$. Pa recimo, da ni. Torej obstajata dve različni praštevili p, q, ki ju v slika v strogo pozitivno število. Ker sta p in q tuji, obstajata taki celi števili m in n, da velja $mp + nq = 1$, iz česar sledi $v(1) = v(mp + nq) \geq \min\{mp, nq\} \geq \min\{p, q\} > 0$, kar pa ne drži. Naj bo $n \in \mathbb{Z}$ in $\alpha \geq 0$ največja potenca p, ki deli $n = p^\alpha n', n' \perp n$. Potem je $v(n) = v(p^\alpha n') = \alpha v(p)$. Iz tega za vsak $m/n \in \mathbb{Q} \setminus \{0\}$ sledi $v(m/n) = (\alpha - \beta)v(p)$, kjer je $m = p^\alpha m', n = p^\beta n', \alpha, \beta \in \mathbb{Z}$ in $p \perp m', n'$. Če bi bilo $v(p) = n > 1$, bi bila $\mathrm{Im}(v) \subseteq n\mathbb{Z}$, kar je v nasprotju s surjektivnostjo v. Iz povedanega lahko sklepamo, da je $v = v_p$.

b) Naj bo $\mathcal{O}$ valuacijski kolobar, ki pripada netrivialni valuaciji $v : k(x) \to \mathbb{Z} \cup \{\infty\}$. Ločimo dve možnosti: $x \in \mathcal{O}$ in $x \notin \mathcal{O}$. V prvem primeru velja $k[x] \subseteq \mathcal{O}$ in postopamo podobno kot v točki *a)*: najprej ugotovimo, da obstaja nerazcepen $p \in k[x]$, za katerega je $v(p) > 0$, sicer bi bila v trivialna valuacija. Pa recimo,

da p ni enolično določen. Izmed vseh polinimov q, za katere je $v(q) > 0$, naj bo p eden tistih z minimalno stopnjo. Po izreku o deljenju polinomov zato za vsak drug nerazcepen polinom q, za katerega je $v(q) > 0$ in posledično $\deg(q) \geq \deg(p)$, obstajata taka $a, r \in k[x], \deg(r) < \deg(p), r \neq 0$, da je $q = ap + r$ in zato $v(q) = v(ap + r) = v(r) = 0$, saj ima r manjšo stopnjo kot p, zato je $v(r) = 0 < v(p)$. Torej je nerazcepen $p \in k[x]$ enolično določen polinom, za katerega je $v(p) > 0$. Od tu na analogen način kot v točki *a)* pridemo do sklepa, da je $v = v_p$.

Če pa je $x \notin \mathcal{O}$, je $v(x) < 0$. Iz tega sledi $v(x^m) < v(x^n)$ za $m > n$ in ker je $v(ax^m) = v(x^m)$ za vsak $m \in \mathbb{N}, a \in k^\times$, je za vsak polinom $p(x) = a_n x^n + \cdots + a_1 x + a_0, a_n \neq 0$, $v(p) = v(a_n x^n + \cdots + a_1 x + a_0) = v(a_n x^n) = v(x^n) = nv(x)$. Za $p/q \in k(x)$ tako velja $v(p/q) = v(x)(\deg(p) - \deg(q))$, iz česar sledi $\mathrm{Im}(v) \subseteq v(p)\mathbb{Z}$. Iz surjektivnosti v in $v(x) < 0$ sledi $v(x) = -1$, zato sklepamo $v = v_\infty$. □

Kot bomo pokazali kasneje, lahko vsako, tudi netrivialno valuacijo v na polju k razširimo na valuacijo w na polju $k(x)$. Mi pa se bomo sedaj posvetili valuacijskim kolobarjem, ki pripadajo diskretnim valuacijam in jih karakterizirajo.

2.2.2. *Algebraične lastnosti diskretnih valuacijskih kolobarjev.* Kot smo že pokazali, je za vsako (diskretno) valuacijo v pripadajoč valuacijski kolobar $\mathcal{O} = \{x \in K \mid v(x) \geq 0\}$ lokalen, njegov maksimalen ideal pa je $\mathcal{M} = \{x \in K \mid v(x) > 0\}$. Prav tako smo s pomočjo leme videli, da ima $\mathcal{O}$ Krullovo dimenzijo 1, torej je $\mathrm{Spec}(\mathcal{O}) = \{\{0\}, \mathcal{M}\}$. Pokažimo še nekaj drugih lastnosti diskretnih valuacijskih kolobarjev. Pri tem z (x) označimo ideal, generiran z elementom x.

Lema 2.22. *Naj bo $t \in \mathcal{O}$ in $v(t) = 1$. Potem je $\mathcal{M} = (t)$. Še več: vsak netrivialen ideal $I \subseteq \mathcal{O}_t$ je enak (t^n) za nek $n \in \mathbb{N}_0$. Tak element t imenujemo* parameter *kolobarja $\mathcal{O}$.*

Dokaz. Za $x \in \mathcal{M}$ je $v(x) \geq 1$ in zato $v(xt^{-1}) = v(x) - v(t) \geq 0$. Torej je $xt^{-1} \in \mathcal{O}$ in zato je $x = (xt^{-1})t \in (t)$.

Če je $0 \neq I \subseteq \mathcal{O}$ ideal, označimo $n_I := \min\{\nu \in \mathbb{N}_0 \mid \exists x \in I, v(x) = \nu\}$. Za $x \in I$ je tako $v(x) \geq n_I$, zato je $v(xt^{-n_I}) = v(x) - n_I \geq 0$ in sledi $xt^{-n_I} \in \mathcal{O}$. Torej je $x = (xt^{-n_I})t^{n_I} \in (t^{n_I})$. Sledi $I \subseteq (t^{n_I})$. Da dokažemo obratno inkluzijo, vzamemo poljuben $x \in I$, za katerega je $v(x) = n_I$, in ker je $v(t^{n_I}x^{-1}) = 0$, je $t^{n_I} = (t^{n_I}x^{-1})x \in I$. □

Posebej smo pokazali, da je vsak ideal valuacijskega kolobarja $\mathcal{O}$ končno generiran oz. da so diskretni valuacijski kolobarji Noetherski. Še več, ker je vsak ideal $\mathcal{O}$ generiran samo z enim elementom, je $\mathcal{O}$ glavni kolobar. Kot bomo pokazali spodaj, so diskretni valuacijski kolobarji edini Noetherski valuacijski kolobarji. Najprej pokažimo par pomožnih trditev.

Lema 2.23 ([11, lema 8.3])**.** *Naj bo A cel Noetherski kolobar in $t \in A$ neobrnljiv. Potem je $\cap_{n=1}^{\infty}(t^n) = \{0\}$.*

Dokaz. Za poljuben $x_0 \in A$ velja bodisi $x_0 \notin (t)$ bodisi $x_0 = tx_1$. Iz tega sledi $(x_0) \subset (x_1)$, ta inkluzija pa je stroga, saj bi sicer obstajal tak $y \in A$, da bi bil $x_1 = yx_0$ in zato $x_0 = tx_1 = ytx_0$, iz česar bi, ker je A cel, sledilo $y = t^{-1}$, kar pa ni mogoče, saj je po predpostavki t neobrnljiv. V primeru $x_0 = tx_1$ postopek ponovimo za x_1, za katerega velja bodisi $x_1 \notin (t)$ bodisi $x_1 = tx_2$. V slednjem primeru nadaljujemo s postopkom, ki pa se slej ko prej ustavi, saj bi v nasprotnem primeru dobili strogo naraščajočo verigo idealov $(x_0) \subset (x_1) \subset (x_2) \subset \ldots$, kar pa je

v nasprotju z dejstvom, da je A Noetherski. Torej za $x_0 \in A$ obstaja tak $n \in \mathbb{N}$, da je $x_0 \in (t^n) \setminus (t^{n+1})$. □

Trditev 2.24 ([11, lema 8.3])**.** *Naj bo A cel lokalen kolobar z glavnim maksimalnim idealom $M = (t), t \neq \{0\}$ in naj velja $\cap_{n=1}^{\infty}(t^n) = 0$. Potem velja:*

(1) *Vsak $x \in A$ je oblike $x = t^n u$, kjer je $n \in \mathbb{N}_0$ in $u \in A$ obrnljiv.*
(2) *Naj bo $K := FracA$ (polje ulomkov za A). Na A definiramo preslikavo $v(0) := \infty$ in $v(x) = n$, kjer je $x = t^n u$, $u \in A$ obrnljiv, in jo s predpisom $v(x/y) = v(x) - v(y)$ razširimo na K. Potem je v diskretna valuacija na K, A pa pripadajoč valuacijski kolobar.*

Dokaz. 1) Iz $\cap_{n=1}^{\infty}(t^n) = 0$ sledi, da za vsak $x \in A$ obstaja tak n, da je $x \in (t^n) \setminus (t^{n+1})$. To pomeni, da je $x = t^n u$, kjer je $u \notin (t) = M$, torej je u obrnljiv v A.

2) Naj za $x/y \in K$ velja $v(x/y) \geq \{0\}$. Potem je $v(x) \geq v(y)$ oz. $x = t^m u$ in $y = t^n v$, kjer je $m \geq n$ in $u, v \in A^{\times}$. Torej je $x/y = t^{m-n}(uv^{-1}) \in A$. Torej je za $z \in K$ $v(z) \geq 0$ natanko tedaj, ko je $z \in A$. Iz te ekvivalence bo, ko bomo dokazali, da je v valuacija na K, sledilo, da je A pripadajoč valuacijski kolobar. Najprej preverimo, da veljajo aksiomi valuacije za $x, y \in A$, saj bo iz tega takoj sledilo, da veljajo tudi na K. Kot vedno moramo preveriti samo valuacije produkta in vsote. Naj bo $x = t^m u$ in $y = t^n v$ za $u, v \in A^{\times}$. Potem je $xy = t^{m+n}(uv)$ in $x + y = t^{\min\{m,n\}}a$ za $a \in A$. Sledi $v(xy) = m + n = v(x) + v(y)$ in $v(x + y) = v(t^{\min\{m,n\}}) + v(a) \geq v(t^{\min\{m,n\}})$, saj je $v(a) \geq 0$. □

S pomočjo dokazanih izrekov lahko med valuacijskimi kolobarji karakteriziramo diskretne na še en način.

Izrek 2.25 ([11, lema 8.6])**.** *Valuacijski kolobar A je diskreten natanko tedaj, ko je Noetherski.*

Dokaz. Ker iz leme 2.2.3 vemo, da je diskreten valuacijski kolobar Noetherski, moramo preveriti samo še drugo smer ekvivalence. Naj bo A Noetherski valuacijski kolobar. Maksimalni ideal A je tako končno generiran, iz česar sledi, da je glavni. Res: naj bo $M = (x_1, \ldots, x_n)$ in naj za i velja $v(x_i) \leq v(x_j)$ za $1 \leq j \leq n$. Potem je $x_j x_i^{-1} \in A$ za vsak j, zato je $x_j = (x_j x_i^{-1})x_i \in (x_i)$. Ugotovili smo, da velja $M = (x_i)$, torej je M glavni kolobar. Za x_i velja $\cap_{n=1}^{\infty}(x_i^n) = \{0\}$, saj je A Noetherski. Sedaj so izpolnjene vse predpostavke trditve 2.24, torej je A diskreten valuacijski kolobar. □

Spomnimo se, da je kolobar A *celostno zaprt* v nadkolobarju S, če za vsak $x \in S$ in vse $a_{n-1}, \ldots, a_0 \in A$, iz $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ sledi $x \in A$. Če je A celostno zaprt v kolobarju ulomkov Frac$A$, pravimo, da je A *normalen*. Ker je diskreten valuacijski kolobar glavni in ima zato vsak njegov element enoličen razcep, bo iz spodnje leme sledilo, da je vsak diskreten valuacijski kolobar normalen.

Lema 2.26 ([8, trditev 8.8])**.** *Vsak kolobar z enoličnim razcepom je normalen.*

Dokaz. Naj bodo $x, y, a_{n-1}, \ldots a_0, \in A$, $y \neq 0$ in $x \perp y$ (to pomeni, da so vsi enolično določeni neobrnljivi elementi razcepa x na prafaktorje različni od tistih v razcepu y), taki, da velja $x^n/y^n + a_{n-1}x^{n-1}/y^{n-1} + \cdots + a_1 x/y + a_0 = 0$. Če zadnjo enačbo pomnožimo z y^n, nato x^n damo na drugo stran, dobimo $-y(a_{n-1}x^{n-1} + \cdots a_1 x y^{n-2} + a_0 y^{n-1}) = x^n$. V tem primeru vsak neobrnljiv faktor v razcepu y deli x^n in zato x, kar pa je zaradi $x \perp y$ mogoče le v primeru, ko je y obrnljiv in takih faktorjev ni. Sledi $x/y = xy^{-1} \in A$. □

Doslej smo uspeli pokazati, da je vsak diskreten valuacijski kolobar A Noetherski, normalen, lokalen z maksimalnim idealom $M \neq 0$ in da velja $\mathrm{Spec}A = \{\{0\}, M\}$. Pokazali bomo, da te lastnosti enolično določajo diskretne valuacijske kolobarje. Pred so bomo spomnili nekaj rezultatov iz komutativne algebre.

Trditev 2.27 ([8, trditev 7.2])**.** *Naj bo M A-modul, generiran z n elementi in $\phi : M \to M$ homomorfizem. Recimo, da obstaja tak ideal I v A, da velja $\phi(M) \subseteq IM$. Potem za ϕ velja $\phi^n + a_1\phi^{(n-1)} + , \ldots, + a_{n-1}\phi + a_n = 0$, kjer so $a_i \in I$.*

Dokaz. Naj bodo $m_1, \ldots, m_n$ generatorji M. Ker so $\phi(m_i) \in IM$, za vsak i velja $\phi(m_i) = \sum_{j=1}^n a_{i,j}m_j$ za neke $a_{i,j} \in I$. Povedano drugače: velja $\sum_{j=1}^n (\delta_{i,j}\phi - a_{i,j})m_j = 0$, kjer je $\delta_{i,j}$ Kroneckerjev δ, torej indikator $i = j$.

Definirajmo $n \times n$-matriko $\Delta := [(\delta_{i,j}\phi - a_{i,j})]_{i,j}$ s koeficienti v komutativnem kolobarju $A[\phi] \subseteq \mathrm{End}(M)$, generiranem z A-linearnim endomorfizmom ϕ in množenjem z elementi iz A:

$$\Delta = \begin{bmatrix} \phi - a_{1,1} & -a_{1,2} & -a_{1,3} & \ldots & -a_{1,n} \\ -a_{2,1} & \phi - a_{2,2} & -a_{2,3} & \ldots & -a_{2,n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ -a_{n,1} & -a_{n,2} & -a_{n,3} & \ldots & \phi - a_{n,n} \end{bmatrix}.$$

Pokazali bomo, da je determinanta Δ enaka nič. V razvoju Δ bomo tako dobili relacijo $\phi^n + a_1\phi^{(n-1)} + , \ldots, + a_{n-1}\phi + a_n = 0$, ki jo želimo dokazati. Naj bo $[c_{i,j}]_{i,j=1}^n := \widetilde{\Delta}$ adjungiranka Δ. Ker je $\widetilde{\Delta} \cdot \Delta = I_n \det(\Delta)$ in zato $\sum_{i=1}^n c_{k,i}(\delta_{i,j}\phi - a_{i,j}) = \delta_{k,j}\det(\Delta)$, potem za $k = 1, \ldots, n$ velja

$$\begin{aligned} \det(\Delta) \cdot m_k &= \sum_{j=1}^n \delta_{j,k}\det(\Delta) \cdot m_j = \sum_{j=1}^n (\sum_{i=1}^n c_{k,i}(\delta_{i,j}\phi - a_{i,j}))m_j \\ &= \sum_{i=1}^n c_{k,i} \sum_{j=1}^n (\delta_{i,j}\phi - a_{i,j})m_j = 0. \end{aligned}$$

Torej je $\det(\Delta)$ ničelni endomorfizem M. Trditev je dokazana. □

Posledica 2.28 ([11, posledica 2.8])**.** *(Lema Nakayama) Naj bo A lokalen kolobar z maksimalnim idealom M in N končno generiran A-modul. Potem iz $N = MN$ sledi $N = 0$.*

Dokaz. Ker je $N = \mathrm{id}_N(N) = MN$, po 2.27 obstajajo taki $a_0, a_1, \ldots, a_{n-1} \in M$, da velja $\mathrm{id}_N^n + a_1\mathrm{id}_n^{(n-1)} + , \ldots, + a_{n-1}\mathrm{id}_N + a_n = (1 + a_1 + \ldots a_n)\mathrm{id}_N = 0$. Torej obstaja $b \in M$, da je $(1 + b)\mathrm{id}_N = 0$, oz., povedano drugače, da velja $(1 + b)N = 0$. Toda ker je $1 + b \in 1 + M$, je $1 + b$ obrnljiv v A, iz česar sledi $N = 0$. □

Spomnimo se, da za A-modul M z $\mathrm{Ass}M = \{P \in \mathrm{Spec}A \mid Pm = 0 \text{ za nek } 0 \neq m \in M\}$ označujemo množico vseh praidealov A, ki slikajo nek neničeln element modula v nič. Takim idealom pravimo, da so *asociirani* M. Če za ideal $I \subseteq A$ obstaja tak $m \in M$, da je $Im = 0$, pravimo, da je I *anihilator* $m \in M$.

Trditev 2.29 ([11, trditev 8.4])**.** *Kolobar A je diskreten valuacijski kolobar natanko tedaj, ko je Noetherski, normalen, lokalen in velja $\mathrm{Spec}A = \{\{0\}, M\}$, kjer je $M \neq 0$.*

Dokaz. Pokazati moramo samo, da velja implikacija v desno smer. Najprej pokažimo, da je M glavni ideal A. Zato bomo najprej pokazali, da velja $M \neq M^2$. Ker je M kot vsak ideal A končno generiran kot A-modul, bi iz $M^2 = M$ sledilo

po lemi Nakayama $M = 0$, kar pa po predpostavki ne velja. Sedaj izberemo poljuben $x \in M \setminus M^2$ in pokažimo, da velja $M = (x)$. Če to ne velja, sledi, da je A-modul $N := M/(x) \neq 0$. Pokažimo, da je $\mathrm{Ass}N \subseteq \mathrm{Spec}A$ neprazna. Ker je $xN = 0$, je množica anihilatorjev elementov N neprazna, saj vsebuje denimo (x). Ker je A Noetherski, ima vsaka njegova množica idealov maksimalen element. Vsaka naraščajoča veriga idealov v A se namreč konča, zato obstoj maksimalnega ideala v množici obstaja po Zornovi lemi. Maksimalen element te množice je neničeln praideal A, torej je, ker je $\mathrm{Spec}A = \{\{0\}, M\}$, enak M. Zato obstaja tak $0 \neq y(x) \in N$, da je $My(x) = 0$ oz. $My \subseteq (x)$. Sedaj si oglejmo element $y/x \in K := \mathrm{Frac}A$. Ker je $x \in M$, ni obrnljiv, zato je $y/x \notin A$, toda $y/xM \subseteq A$, saj je $yM \subseteq (x)$. Če je $y/xM = A$, potem obstaja $y' \in M$, da je $yy'/x = 1$, kar pa ni mogoče, saj je x neobrnljiv v A. Zato je $y/mM \subseteq M$. V tem primeru je preslikava $\phi : M \to M$, $\phi(m) = y/xm$ dobro definiran homomorfizem M kot končno generiranega A-modula. Po 2.27 zato obstajajo $a_{n-1}, \ldots, a_0 \in A$, da velja $\phi^n + a_{n-1}\phi^{n-1} + \cdots + a_1\phi + a_0 = 0$. Sedaj v to enakost vstavimo poljuben $z \in M \setminus \{0\}$ in dobimo $((y/x)^n + a_{n-1}(y/x)^{n-1} + \cdots + a_1(y/x) + a_0)z = 0$, iz česar, ker je A cel kolobar ($\{0\}$ je namreč njegov praideal), sledi $(y/x)^n + a_{n-1}(y/x)^{n-1} + \cdots + a_1(y/x) + a_0 = 0$. Torej je, ker je A normalen, $y/x \in A$. Prišli smo do protislovja s predpostavko, da je $M/(x) \neq 0$, zato sklepamo, da velja $M = (x)$. Vidimo, da so, ker je A Noetherski in je po lemi 2.23 zato $\cap_{n=1}^{\infty}(x^n) = 0$, izpolnjene vse predpostavke leme 2.24. Torej je A diskreten valuacijski kolobar. □

2.2.3. *Absolutna vrednost na polju z valuacijo in napolnitev. Laurentove vrste in p-adična števila.* V tem razdelku bomo na polju z diskretno valuacijo definirali absolutno vrednost, ki bo odvisna od valuacije. Ta nam bo dala metriko, s katero bomo dobili definicijo polnega polja z diskretno valuacijo. Vsako polje z absolutno vrednostjo K lahko napolnimo oz. vložimo v enolično določeno polno polje $\widehat{K}$, v katerem je K gost. S pomočjo napolnitve bomo prišli do polj Laurentovih vrst in p-adičnih števil.

Naj bo K polje z valuacijo v ranga 1. Na K definiramo preslikavo $|\ |_v : K \to \mathbb{R}$ s predpisom $|0|_v := 0$ in $|x|_v := e^{-v(x)}$ za $x \in K^\times$. Hitro se prepričamo, da $|\ |_v$ zadošča naslednjim pravilom za vsaka $x, y \in K$:

(1) $|x|_v \geq 0$ in $|x|_v = 0 \Leftrightarrow x = 0$,
(2) $|xy|_v = |x|_v|y|_v$,
(3) $|x + y|_v \leq |x|_v + |y|_v$.

Preslikava iz polja v $\mathbb{R}$, ki zadošča zgornjim lastnostim, je *absolutna vrednost na polju*. Veljavnost prvih dveh pravil takoj sledi iz definicje $|\ |_v$, preverimo še (3). V resnici za $|\ |_v$ velja še močnejše pravilo kot (3), in sicer $|x + y|_v \leq \max\{|x|_v, |y|_v\}$, saj je $|x + y|_v = e^{-v(x+y)} \leq e^{-\min\{v(x),v(y)\}} = \max\{e^{-v(x)}, e^{-v(y)}\} = \max\{|x|_v, |y|_v\}$. Zaradi slednje lastnosti $|\ |_v$ pravimo, da je $|\ |_v$ *nearhimedska absolutna vrednost* na polju K.

Obratno se ni težko prepričati, da če je $|\ | : K \to \mathbb{R}$ nearhimedska absolutna vrednost, potem je $v_{|\ |} : K \to \mathbb{R}$, $v_{|\ |}(0) := \infty$ in $v_{|\ |}(x) := -\ln|x|$ za $x \in K$ valuacija ranga 1 na K, kar pa prepuščamo bralcu. Prav tako je stvar rutine preveriti, da je $v_{|\ |_v} = v$ za vsako valuacijo v ranga 1 na K in $|\ |_{v_{|\ |}} = |\ |$ za vsako nearhimedsko absolutno vrednost $|\ |$ na K, iz česar sledi, da so nearhimedske absolutne vrednosti in valuacije ranga 1 na polju K v bijektivni korespondenci.

Primer 2.30. Naj bo p praštevilo, $K = \mathbb{Q}$ in v_p valuacija iz primera 2.18. Potem za vsak $m/n \in \mathbb{Q} \setminus \{0\}$ velja $|m/n|_{v_p} = e^{\beta-\alpha}$, kjer je $m = p^\alpha m', n = p^\beta n', \alpha, \beta \in \mathbb{Z}$ in $p \perp m', n'$. Iz 2.21 sledi, da so to edine nearhimedske absolutne vrednosti na $\mathbb{Q}$, saj so te v bijekciji z valuacijami na $\mathbb{Q}$. Primer arhimedske absolutne vrednosti na $\mathbb{Q}$ pa je običajna absolutna vrednost, podedovana od $\mathbb{R}$. $\diamondsuit$

Ni se težko prepričati, da je preslikava $d : K \times K \to \mathbb{R}$, $d(x, y) := |x - y|_v$ metrika na K. Očitno je namreč, da je $d(x, y) = d(y, x) \geq 0$ za vsa $x, y \in K$ in da je $d(x, y) = 0 \Leftrightarrow x = y$. Preverimo še trikotniško neenakost: $d(x, z) = |x - z|_v = |x - y + y - z|_v \leq |x - y|_v + |y - z|_v = d(x, y) + d(y, z)$. Ugotovili smo, da je s tako definirano metriko polje K metrični prostor z metriko d.

Zaporedje $(x_n)_{n\in\mathbb{N}}$ v polju K z absolutno vrednostjo je *Cauchyjevo*, če za vsak $\epsilon > 0$ obstaja $N \in \mathbb{N}$, da za vsaka $m, n \geq N$ velja $|x_m - x_n| < \epsilon$, in *konvergira* proti $x \in K$, če za vsak $\epsilon > 0$ obstaja $N \in \mathbb{N}$, da za vsak $n \geq N$ velja $|x - x_n| < \epsilon$. V tem primeru pravimo, da je x *limita* zaporedja $(x_n)_{n\in\mathbb{N}}$. V primeru $|\ | = |\ |_v$ za neko valuacijo v je $(x_n)_{n\in\mathbb{N}}$ Cauchyjevo oz. konvergira proti $x \in K$ natanko tedaj, ko za vsak $M \in \mathbb{N}$ obstaja tak N, da je za vse $m, n \geq N$ $v(x_m - x_n) > M$ oz. $v(x - x_n) > M$. Vsako konvergentno zaporedje v K je Cauchyjevo, v kar se lahko prepričamo z enakim postopkom kot v primeru realnih števil s standardno absolutno vrednostjo, če pa velja tudi, da je vsako Caucyjevo zaporedje v K tudi konvergentno, pravimo, da je K *poln* metrični prostor. Na enak način, kot se to dokaže v primeru realnih števil, ni težko videti, da je limita vsote oz. produkta konvergentnih zaporedij enaka vsoti oz. produktu limit. Podobno bomo spodaj pokazali, da je limita inverza enaka inverzu limit.

Izrek 2.31 ([5, izrek 13])**.** *a) Naj zaporedje $(x_n)_{n\in\mathbb{N}} \subseteq K$ konvergira k $0 \neq x \in K$. Potem zaporedje $(x^{-1})_{n\in\mathbb{N}}$ konvergira k $x^{-1} \in K$.*

b) Naj bo zaporedje $(x_n)_{n\in\mathbb{N}} \subseteq K \setminus \{0\}$ Cauchyjevo in naj obstajata taka $\epsilon > 0$ in $N \in \mathbb{N}$, da je $|x_n| \geq \nu$ za vsak $n \geq N$. Potem je tudi zaporedje $(x_n^{-1})_{n\in\mathbb{N}}$ Cauchyjevo.

Dokaz. a) Ker je $x \neq 0$, je $|x| > 0$, zato za vsak $0 < \nu < |x|$, obstaja tak $N \in \mathbb{N}$, da je $|x_n| \geq \nu$ za vsak $n \geq N$. Potem je $|x^{-1} - x_n^1| = |x - x_n|/|xx_n| \leq |x - x_n|/|x|\nu$, iz česar sledi, da zaporedje $(x^{-1})_{n\in\mathbb{N}}$ konvergira k x^{-1}.

b) Dokaz te točke poteka podobno, saj za $m, n \geq N$ velja $|x_m^{-1} - x_n^1| = |x_m - x_n|/|x_m x_n| \leq |x_m - x_n|/\nu^2$. $\square$

Iz funkcionalne analize vemo, da lahko vsak normiran prostor V vložimo v prostor vseh Cauchyjevih zaporedij v V, na katerem, potem ko ga kvocientiramo po podprostoru zaporedij z limito 0, definiramo metriko in dobimo poln normiran prostor, v katerem je vložitev V poln podprostor. Temu prostoru pravimo *napolnitev* V. Zelo podoben postopek bomo uporabili pri napolnitvi polja K z absolutno vrednostjo.

Izrek 2.32 ([1, izrek 9.4.2])**.** *Naj bo K polje z absolutno vrednostjo. Potem obstaja polje $\hat{K}$ z absolutno vrednostjo, glede na katero je polno, K pa lahko vložimo v $\hat{K}$ tako, da je njegova slika gosta.*

Dokaz. S C označimo množico $\{(x_1, x_2, \ldots) \mid x_i \in K, (x_n)_{n\in\mathbb{N}}$ je Cauchyjevo$\}$ vseh Cauchyjevih zaporedij v K. Na C definiramo seštevanje in množenje po komponentah, s čimer C postane komutativen kolobar z ničlo $\overline{0}$ in enico $\overline{1}$ (aksiome za kolobar se da hitro preveriti po komponentah), pri čemer z $\overline{x}$ za $x \in K$ označimo konstantno zaporedje $(x, x, \ldots)$. Ta kolobar ni cel, kot kaže primer $(1, 0, 0, \ldots) \cdot (0, 1, 0, 0, \ldots) = \overline{0}$.

Množica $N := \{(x_1, x_2, \ldots) \mid (x_n)_{n\in\mathbb{N}} \in C, \lim_{n\to\infty} x_n = 0\}$ je ideal v C. Res: zaprtost za seštevanje sledi iz dejstva, da je limita vsote konvergentnih zaporedij enaka vsoti njihovih limit. Če vzamemo poljuben $(z_n)_{n\in\mathbb{N}} \in C$, potem za vse $m, n \in \mathbb{N}$ velja $|x_n z_n| = |x_n z_m + x_n(z_n - z_m)| \leq |x_n z_n| + |x_n||z_n - z_m|$, in ker lahko drugi člen $|z_n - z_m|$ omejimo navzgor za dovolj velike m in n, saj je $(z_n)_{n\in\mathbb{N}}$ Cauchyjevo, gre desna stran neenakosti proti nič in zato je $(x_n z_n)_{n\in\mathbb{N}} \in N$. Pokazali smo, da je N ideal v C.

S $\widehat{K}$ označimo kolobar C/N, v katerem sta elementa $(x_n)_{n\in\mathbb{N}} + N$ in $(y_n)_{n\in\mathbb{N}} + N$ enaka natanko tedaj, ko je $\lim_{n\to\infty} x_n = \lim_{n\to\infty} y_n$. Pokažimo, da je $\hat{K}$ polje. Naj bo $(x_n)_{n\in\mathbb{N}} + N \neq N$, kar pomeni, da $(x_n)_{n\in\mathbb{N}}$ ne konvergira proti nič. Ker je Cauchyjevo, hkrati pa ne konvergira proti nič, obstajata taka $\epsilon > 0$ in $N \in \mathbb{N}$, da je $|x_n| \geq \epsilon$ za vsak $n \geq N$. Pa recimo, da to ni res. Naj bo $\epsilon_1 > 0$ poljuben in $N_1 \in \mathbb{N}$ tak, da je $|x_m - x_n| < \epsilon_1/2$ za vsaka $m, n \geq N_1$. Obstaja tak $M \geq N_1$, da je $|x_M| \leq \epsilon_1/2$, iz česar sledi, da za vsak $n \geq M$ velja $|x_n| \leq |x_n - x_M| + |x_M| < \epsilon_1$. Ker je bil $\epsilon_1 > 0$ poljuben, smo pokazali, da je $(x_n)_{n\in\mathbb{N}} \in N$, kar pa ni mogoče. Pokazali smo, da obstajata taka $\epsilon > 0$ in $N \in \mathbb{N}$, da je $|x_n| \geq \epsilon$ za vsak $n \geq N$. Definiramo zaporedje $(x'_n)_{n\in\mathbb{N}}$ s predpisom $x'_n = 1$ za $n < N$ in $x'_n = x_n$ za $n \geq N$. Iz izreka 2.31 sledi, da je zaporedje $({x'_n}^{-1})_{n\in\mathbb{N}}$ Cauchyjevo. Ker je jasno, da velja $(x'_n)_{n\in\mathbb{N}} + N = (x_n)_{n\in\mathbb{N}} + N$, smo našli inverz za $(x_n)_{n\in\mathbb{N}} + N$ v $\widehat{K}$.

Na $\widehat{K}$ definiramo absolutno vrednost:

$$|(x_n)_{n\in\mathbb{N}} + N| := \lim_{n\to\infty} |x_n|.$$

$(|x_n|)_{n\in\mathbb{N}}$ je namreč Cauchyjevo zaporedje realnih števil, saj je $||x_n| - |x_m|| \leq |x_n - x_m|$, zato ima limito v $\mathbb{R}$. Če je $(x_n)_{n\in\mathbb{N}} + N = (y_n)_{n\in\mathbb{N}} + N$, potem je za vsako naravno število n $||x_n| - |y_n|| \leq |x_n - y_n|$, zato sta $\lim_{n\to\infty} |x_n|$ in $\lim_{n\to\infty} |y_n|$ enaki, s čimer smo pokazali, da je $|\ |$ dobro definirana preslikava na $\hat{K}$ in ni težko videti, da je tudi absolutna vrednost.

K vložimo v $\widehat{K}$ na naraven način: če vsak $x \in K$ pošljemo v $\overline{x} + N$, je jasno, da dobimo homomorfizem polj. Sedaj pokažimo, da je vložitev K gosta v $\widehat{K}$. Naj bo $(x_n)_{n\in\mathbb{N}} + N \in \hat{K}$, $\epsilon > 0$ in $N \in \mathbb{N}$ tak, da je $|x_m - x_n| \leq \epsilon$ za vse $m, n \geq N$. Potem velja $|(x_n)_{n\in\mathbb{N}} - \overline{x}_N + N| < \epsilon$. Ker je bil izbran ϵ poljuben, smo pokazali, da je K gost v $\hat{K}$.

Pokažimo še, da je $\widehat{K}$ poln. Naj bo $(\alpha_n + N)_{n\in\mathbb{N}}$ Cauchyjevo zaporedje v $\widehat{K}$. Zaradi gostosti K za vsak $n \in \mathbb{N}$ obstaja tak $x_n \in K$, da je $|(\overline{x}_n - \alpha_n) + N| < 1/n$. Ker je $|(\overline{x}_n - \overline{x}_m) + N| \leq |(\overline{x}_n - \alpha_n) + N| + |(\alpha_n - \alpha_m) + N| + |(\overline{x}_m - \alpha_m) + N|$ in ker je za dovolj velike m in n desna stran neenakosti poljubno majhna, je $(x_n + N)_{n\in\mathbb{N}}$ Cauchyjevo v $\hat{K}$, iz česar sledi, da je $\alpha := (x_n)_{n\in\mathbb{N}}$ Cauchyjevo zaporedje v K in zato je $\alpha + N$ vsebovan v $\hat{K}$. Iz $|(\alpha - \alpha_n) + N| \leq |(\alpha - \bar{x}_n) + N| + |(\bar{x}_n - \alpha_n) + N|$ pa sledi, da $(\alpha_n + N)_{n\in\mathbb{N}}$ konvergira proti $\alpha + N$ v $\widehat{K}$. □

Ker je $|\bar{x} + N| = |x|$ za vsak $x \in K$, vidimo, da je absolutna vrednost na $\widehat{K}$, definirana v dokazu izreka, razširitev absolutne vrednosti na K. Spodnji izrek pokaže, da je s tem dodatnim pogojem napolnitev K do izomorfizma enolično določena.

Trditev 2.33 ([1, izrek 9.4.3])**.** *Naj bo K polje z absolutno vrednostjo in $\hat{K}$ kot v dokazu 2.32. Če lahko K gosto vložimo v polno polje L, katerega absolutna vrednost je razširitev tiste od K, potem je L izomorfen $\hat{K}$. Izomorfizem med njima je konstanten na K.*

Dokaz. Naj bo $i : K \to L$ vložitev. Za $(x_n)_{n\in\mathbb{N}} + N \in \hat{K}$ je $(x_n)_{n\in\mathbb{N}}$ Cauchyjevo v K, zato je tudi $(i(x_n))_{n\in\mathbb{N}}$ Cauchyjevo v L. Ker je L poln, ima natanko določeno limito $y \in L$. Definirajmo preslikavo $f : \hat{K} \to L$, kjer vsakemu $(x_n)_{n\in\mathbb{N}} + N \in \hat{K}$ priredimo limito $(i(x_n))_{n\in\mathbb{N}}$ v L. Ker je v vsakem polju vsota limit oz. produkta enaka limiti vsote oz. produkta, je f homomorfizem polj. $f((x_n)_{n\in\mathbb{N}} + N) = 0$ velja natanko tedaj, ko je $\lim_{n\to\infty} x_n = \lim_{n\to\infty} i(x_n) = 0$, zato je f monomorfizem. Ker je zaradi gostosti K v L vsak $y \in L$ limita Cauchyjevega zaporedja $(x_n)_{n\in\mathbb{N}}$ v K, je $y = f((x_n)_{n\in\mathbb{N}} + N)$, torej je f tudi surjektiven in zato izomorfizem polj. Konstantnost f na K je očitna. □

Sedaj se vrnimo na valuacije. Najprej premislimo, da je napolnitev $\widehat{K}$ polja z valuacijo K tudi sama polje z valuacijo. Za to zadošča premisliti, da je absolutna vrednost, definirana na $\widehat{K}$, arhimedska. Če bi za $x, y \in \widehat{K}$ veljalo $|x + y| > \max\{|x|, |y|\}$, bi zaradi gostosti K v $\widehat{K}$ lahko našli $x', y' \in K'$, za kateri bi veljalo $|x' + y'|_v > \max\{|x'|_v, |y'|_v\}$. Tako bi prišli do protislovja z dejstvom, da je $|\ |_v$ arhimedska.

Zdaj bomo pokazali, da lahko napolnitev polja z diskretno valuacijo (glede na prirejeno nearhimedsko absolutno vrednost) predstavimo še na drug način - v obliki potenčnih vrst. Za to bomo najprej potrebovali kratko lemo:

Lema 2.34. *Naj bo K polje z diskretno valuacijo v in $\mathcal{O}$ pripadajoč valuacijski kolobar. Potem so vsi ideali $\mathcal{O}$ v K. V posebnem to pomeni, da je $\mathcal{O}$ zaprt v K.*

Dokaz. Naj bo I ideal $\mathcal{O}$. Potem je $I = (t^n)$ za nek $t \in K, v(t) = 1$, $n \in \mathbb{N}$. Pa recimo, da obstaja tako zaporedje $(x_n)_{n\in\mathbb{N}}$ v I, ki konvergira k nekemu $x \in K \setminus I$. Ker je $v(x) < n$, je $v(x - y) = v(x)$ za vsak $y \in I$, saj je $v(y) \geq n$. Iz tega za vsak $n \in \mathbb{N}$ sledi $|x - x_n|_v = e^{-v(x-x_n)} = e^{-v(x)} = |x|_v$. Zato zaporedje $(x_n)_{n\in\mathbb{N}}$ ne more konvergirati k x. □

Naj bo K polje z diskretno valuacijo v, $\mathcal{O}$ in $\mathcal{M}$ pa pripadajoč valuacijski kolobar in njegov maksimalen ideal. Spomnimo se, da za vsak $t \in A, v(t) = 1$ velja $\mathcal{M} = (t)$ in da je poljuben ideal $I \subseteq \mathcal{O}$ oblike (t^n) za naravno število n. S $\overline{K} := \mathcal{O}/\mathcal{M}$ označimo polje ostankov v. Za vsak $x + \mathcal{M} \in \overline{K}$ izberemo en predstavnik $a \in \mathcal{O}$. Naj bo $S \subset \mathcal{O}$ množica izbranih predstavnikov odsekov $\overline{K}$, pri čemer za predstavnika $0 + \mathcal{M}$ vzamemo kar 0. Za ostale predstavnike $a \in S$ velja, da so obrnljivi v $\mathcal{O}$, sicer bi bili vsebovani v $\mathcal{O}$, iz česar bi sledilo $a + \mathcal{M} = \mathcal{M}$. Za vsak $u \in A$ tako obstaja natanko določen $a_0 \in S$, da je $u + \mathcal{M} = a_0 + \mathcal{M}$ in zato $u - a_0 \in \mathcal{M} = (t)$. Torej je $u = a_0 + tu'$ za nek $u' \in A$. Če postopek ponovimo za u', najdemo natanko določen $a_1 \in S$, da je $u' + \mathcal{M} = a_1 + \mathcal{M}$. Sledi $u' = a_1 + tu''$ za nek $u'' \in \mathcal{O}$. Če postopek ponavljamo, vidimo, da velja

$$u = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n + \cdots ,$$

kjer so $a_i \in S$ enolično določeni. Pokažimo, da je zaporedje $(\sum_{i=0}^{n} a_i t^i)_{n\in\mathbb{N}}$ Cauchyjevo v $\mathcal{O}$ za poljuben nabor $a_i \in S$. Naj bo $\epsilon > 0$ in $N \in \mathbb{N}$. Potem za poljubna $m \geq n \geq N$ velja $\sum_{i=0}^{m} a_i t^i - \sum_{i=0}^{n} a_i t^i = \sum_{i=n}^{m} a_i t^i$ in zato je $v(\sum_{i=0}^{m} a_i t^i - \sum_{i=0}^{n} a_i t^i) \geq n \geq N$. Iz tega sledi, da je zgornje zaporedje res Cauchyjevo, in če ima limito v K, to limito označimo z $\sum_{i=0}^{\infty} a_i t^i$. Iz 2.34 sledi, da je v tem primeru $\sum_{i=0}^{\infty} a_i t^i \in \mathcal{O}$.

Lema 2.35. *u je obrnljiv v $\mathcal{O}$ natanko tedaj, ko je $a_0 \neq 0$.*

Dokaz. Če u ni obrnljiv v $\mathcal{O}$, je $u \in \mathcal{M}$ in zato $u + \mathcal{M} = a_0 + \mathcal{M} = \mathcal{M}$. Zaradi naše izbire predstavnika $\mathcal{M}$ v S sledi $a_0 = 0$. Če pa velja, obratno, $a_0 = 0$, je $u = a_1 t + a_2 t^2 + \cdots + = t(a_1 + a_2 t + \ldots)$, kjer je $(a_1 + a_2 t + \ldots) = \lim_{n\to\infty}(a_1 + a_2 t + \ldots + a_n t^{n-1}) \in A$, saj je po lemi 2.34 A zaprt za limite. Sledi $u \in (t) = M$, torej je u neobrnljiv v A. □

Sedaj pokažimo, da lahko vsak $u/v \in K$ zapišemo v obliki vrste

$$c_m t^m + \cdots c_0 + c_1 t + c_2 t^2 + \cdots, m \in \mathbb{Z}, c_i \in S.$$

Naj bo $u = a_0 + a_1 t + a_2 t^2 + \cdots$ in $v = b_0 + b_1 t + b_2 t^2 + \cdots$. Naj bo m najmanjši tak, da je $b_m \neq 0$. Potem je $v = t^m(b_m + b_{m+1} t + \cdots)$. Element $v' := b_m + b_{m+1} t + \cdots \in \mathcal{O}$ je obrnljiv. Torej je $u/v = t^{-m} u v'^{-1}$. Ker je $uv'^{-1} \in \mathcal{O}$, obstajajo $d_i \in S$, da je $uv'^{-1} = d_0 + d_1 t + d_2 t^2 + \cdots$. Če za $n \geq -m$ definiramo $c_n = d_{n+m}$, sledi $u/v = t^{-m} u v'^{-1} = t^{-i} c_{-m} + t^{-m+1} c_{-m+1} + \cdots + c_o + c_1 t + \cdots$.

Naj bo $(x_n)_{n\in\mathbb{N}}$ Cauchyjevo zaporedje v K (glede na $|\ |_v$) in $\epsilon > 0$. Potem obstaja najmanjši $n \in \mathbb{Z}$, da je $e^{-n} < \epsilon$ in tak $N \in \mathbb{N}$, da je za vse $m, k \geq N$ $|x_m - x_k|_v < \epsilon$. Iz $e^{-v(x_m - x_k)} = |x_m - x_k|_v < \epsilon$ in dejstva, da je $v(x_m - x_k) \in \mathbb{Z}$, sledi $-v(x_m - x_k) \geq -n$ oziroma $v(x_m - x_k) = n$. Torej je $x_m - x_k \in (t^n)$. Po zgornjem postopku x_m in x_t razvijemo po potencah t: $x_m = a_{-l} t^{-l} + \cdots a_0 + a_1 t + \cdots$, $x_k = b_{-l'} t^{-l'} + \cdots b_0 + b_1 t + \cdots$. Brez škode za splošnost lahko predpostavimo, da je $l' = l$, sicer dopolnimo vrsto s členi, za katere je a_i oz. $b_i = 0$. Za vse $i \leq n$ velja $a_i = b_i$. Res: sicer naj bo $j < n$ najmanjši tak, da je $a_j \neq b_j$. Ker je $a_j + M \neq b_j + M$, je $a_j - b_j \notin M$. Zato je $x_m - x_n = c_j t^j + c_j t^{j+1} + \cdots, c_j \neq 0$, kar je v nasprotju s predpostavko, da je $x_m - x_n \in (t^n)$. Ugotovili smo: če je $(x_n)_{n\in\mathbb{N}}$ Cauchyjevo zaporedje v K in $\epsilon > 0$, potem obstaja tak $n \in \mathbb{Z}$, da so od nekega $N \in \mathbb{N}$ naprej vsi koeficienti $a_i \in S$ pri razvoju x_j po potencah t enaki za vse $i < n$ in vse $j \geq N$. Še več: ko ϵ pošljemo proti nič, potem gre vrednost najmanjšega $n \in \mathbb{Z}$, da je $e^{-n} < \epsilon$, proti neskončnosti, zato bodo za vse m od nekega N naprej koeficienti $a_i, \in Si < n$ enaki.

Definiramo množico $\widetilde{K} = \{\sum_{i=m}^{\infty} a_i t^i \mid a_i \in S, m \in \mathbb{Z}\}$ s preslikavo $|\sum_{i=m}^{\infty} a_i t^i| = e^{-m}$, kjer je m najmanjši tak, da je $a_m \neq 0$. Na $\widetilde{K}$ definiramo operaciji množenja in seštevanja s prenosom. Za $\sum_{i=m}^{\infty} a_i t^i$ in $\sum_{j=n}^{\infty} b_j t^j$, če naprej brez škode za splošnost predpostavimo, da je $m = n$ (sicer definiramo manjkajoče a_i oz. b_j z nič), definiramo $\sum_{i=m}^{\infty} a_i t^i + \sum_{j=m}^{\infty} b_j t^j = \sum_{i=m}^{\infty} c_i t^i$, kjer je :

- $c_m + x_m = a_m + b_m$, kjer sta c_m in x_m enolično določena, tako da velja $c_m \in S$, $x_m \in \mathcal{M}$.
- $c_k + x_k = a_k + b_k + x_{k-1}$, kjer sta c_k in x_k enolično določena, tako da velja $c_k \in S$, $x_k \in \mathcal{M}$.

Množenje definiramo z $\sum_{i=m}^{\infty} a_i t^i \cdot \sum_{j=m}^{\infty} b_j t^j = \sum_{i=2m}^{\infty} d_i t^i$, kjer je :

- $d_{2m} + x_{2m} = a_m b_m$ in
- $d_l + x_l = \sum_{j=m}^{l+m} a_j b_{l-j} + x_{l-1}$,

kjer definiramo d_l in x_l tako kot pri seštevanju. S temi operacijami je, $\widetilde{K}$ polje. Z lahkoto namreč preverimo, da je komutativen kolobar, poiščimo še inverz: za $\sum_{i=m}^{\infty} a_i t^i$, kjer je $a_m \neq 0$, je $\sum_{i=-m}^{\infty} b_i t^i$, kjer za $b_i \in S$ velja:

- $a_m b_{-m} + \mathcal{M} = 1 + \mathcal{M}$,
- $\sum_{j=m}^{l+m} a_j b_{l-j} + \mathcal{M} = \mathcal{M}$.

$\widehat{K}$ je torej polje. Ni težko videti, da $|\ |$ na $\widehat{K}$ zadošča aksiomom absolutne vrednosti. Pokazali bomo, da je $\widetilde{K}$ (enolično določena) napolnitev K. Najprej bomo

pokazali, da lahko K vložimo v $\widetilde{K}$ in da je absolutna vrednost, ki smo jo definirali na $\widetilde{K}$, razširitev absolutne vrednosti $|\ |_v$ na K. Kot smo pokazali zgoraj, se vsak $x \in K$ da zapisati v obliki $\sum_{i=m}^{\infty} a_i t^i$, in ker se dva elementa $x, y \in K$, zapisana v taki obliki, seštevata in množita s prenosom, iz tega sledi, da lahko K homomorfno vložimo v $\widetilde{K}$. Če je $x = \sum_{i=m}^{\infty} a_i t^i \in K$, kjer je $a_m \neq 0$, potem je $x = \lim_{N\to\infty} \sum_{i=m}^{N} a_i t^i = t^m \lim_{N\to\infty} \sum_{i=0}^{N-m} a_{i+m} t^i$, in ker je $\sum_{i=0}^{N-m} a_{i+m} t^i \in \mathcal{O}^\times$ za vsak $N \in \mathbb{Z}$, zaradi zaprtosti $\mathcal{O}^\times$ to velja tudi za $\sum_{i=0}^{\infty} a_{i+m} t^i$. Zato je $v(x) = v(t^m) = m$ in posledično $|x|_v = e^{-m} = |\sum_{i=m}^{\infty} a_i t^i|$, kjer je $|\ |$ absolutna vrednost na $\widetilde{K}$. Torej je absolutna vrednost, definirana na $\widetilde{K}$, res razširitev $|\ |_v$. Ostane nam še, da pokažemo, da je K gost v $\widetilde{K}$. To pa sledi iz dejstva, da je $\sum_{i=m}^{\infty} a_i t^i = \lim_{N\to\infty} \sum_{i=m}^{N} a_i t^i$ za vsako tako vsoto iz $\widetilde{K}$, in ker so vse končne vsote v limiti elementi K, sledi gostost K v $\widetilde{K}$. Zaradi enoličnosti napolnitve, dokazane v 2.33, vela $\widetilde{K} = \widehat{K}$. V spodnjih primerih bomo delno zaradi konvencij, delno zaradi večje jasnosti take predstavitve napolnitve zgoraj obravnavanih polj z diskretno valuacijo uporabili definirali kot polja potenčnih vrst, ki jih včasih imenujemo *Laurentove vrste* (mi bomo to ime sicer ohranili za polje potenčnih vrst nad poljem v eni spremenljivki, ki je, kot bomo videli, prav tako napolnitev polja z diskretno valuacijo).

Primer 2.36. Najprej si bomo ogledali napolnitve $\mathbb{Q}$ glede na nearhimedske absolutne vrednosti, ki pripadajo valuacijam v_p iz 2.18. Naj bo za praštevilo p $\mathcal{O}_p$ valucijski kolobar, ki pripada v_p, $\mathcal{O}_p$ pa njegov maksimalen ideal, ki sta, spomnimo, enaka kolobarju $\mathbb{Z}_{(p)}$ in njegovemu maksimalnem idealu $(p) = (p)\mathbb{Z}_{(p)}$. Prav tako smo že pokazali, da je polje ostankov $\overline{K_p} := \mathcal{O}_p/\mathcal{M}_p$ izomorfno $\mathbb{Z}_p$. Pokažimo še, da so $0+\mathcal{M}_p, 1+\mathcal{M}_p, \ldots, p-1+\mathcal{M}_p$ različni predstavniki $\overline{K_p}$. Res: za različni celi števili $0 \leq n, m \leq p-1$ je $n-m \in \mathcal{O}_p \setminus \mathcal{M}_p$, saj je $v(n-m) = 0$, zato je $n+\mathcal{M}_p \neq m+\mathcal{M}_p$. Iz povedanega sledi, da lahko vsak $m/n \in \mathbb{Q}$ predstavimo kot vsoto $\sum_{i=n}^{\infty} a_i p^i$, kjer so $a_i \in S := \{0, 1, \ldots, p-1\}$, množica $\mathbb{Q}_p := \{\sum_{i=m}^{\infty} a_i p^i \mid m \in \mathbb{Z}, 0 \leq a_i \leq p-1\}$. To polje imenujemo *polje p-adičnih števil*. $\mathbb{Q}$ lahko gosto vložimo v $\mathbb{Q}_p$, ker pa je kardinalnost $\mathbb{Q}$ enaka $\aleph_0$, kardinalnost $\mathbb{Q}_p$ pa $2^{\aleph_0}$, je ta vložitev prava, torej velja $\mathbb{Q} \subsetneq \mathbb{Q}_p$. ♢

Primer 2.37. Drug primer napolnitve je po konstrukciji analogen. Polje racionalnih funkcij v eni spremenljivki $k(x)$ napolnimo glede na valuacijo v_p, kjer za p vzamemo monom $p(x) = x$, in valuacijo označimo z v_x. Pripadajoč valuacijski kolobar $\mathcal{O}_x$ je oblike $\{p/g \mid x \nmid q\}$, ki je enak $k[x]_{(x)}$, lokalizaciji $k[x]$ pri maksimalnemu idealu (x). $\mathcal{M}_x$ je, kot sledi, enak $(x)\mathcal{O}_x = (x)k[x]_{(x)}$, polje ostankov $\overline{K_x}$ pa je $k[x]_{(x)}/(x)k[x]_{(x)} \cong k$. Enako kot zgoraj se prepričamo, da različni elementi $a + \mathcal{M}_x, a \in k$ tvorijo sistem predstavnikov polja $\overline{K_x}$. Iz tega sledi, da lahko vsak $p/q \in k(x)$ zapišemo v obliki $\sum_{i=n}^{\infty} a_i x^i$ za nek $n \in \mathbb{Z}$, $a_i \in k$, polje Laurentovih vrst nad poljem k, ki ga označimo s $k((x)) := \{\sum_{i=n}^{\infty} a_i x^i \mid n \in \mathbb{Z}, a_i \in k\}$ pa je napolnitev $k(x)$ glede na valuacijo v_x. ♢

Posebej si oglejmo primer Laurentovih vrst nad poljem praštevilske moči $\mathbb{Z}_p((x))$. Njegove elemente lahko predstavimo v obliki neskončnih vsot $\sum_{i=n}^{\infty} a_i x^i$ s koeficienti v $\mathbb{Z}_p$. Ti elementi so na videz podobni elementom $\mathbb{Q}_p$, zapisanih v obliki $\sum_{i=n}^{\infty} a_i p^i$. Kljub temu, da polji $\mathbb{Z}_p((x))$ in $\mathbb{Q}_p$ nista izomorfni, saj ima prvo karakteristiko p, drugo pa ima zaradi prenosa pri seštevanju karateristiko 0, so ju pogosto primerjali med seboj, kar je privedlo do včasih napačnih domnev, pa tudi do presenetljivih podobnosti. Preden bomo povedali nekaj o slednjih, bomo obravnavali razširitve

valuacij v odvisnosti od razširivev polj in pokazali, da so v primeru algebraičnih razširitev polnih polj z diskretno valuacijo te enolično določene.

2.3. **Razširitve valuacij.**

Definicija 2.38. Naj bosta K_1 in K_2 polji z valuacijami, kjer je $K_2 \mid K_1$ razširitev, $\mathcal{O}_1 \subseteq K_1$ in $\mathcal{O}_2 \subseteq K_2$ pa pripadajoča valuacijska kolobarja. Pravimo, da je $\mathcal{O}_2$ *razširitev* $\mathcal{O}_1$, če je $\mathcal{O}_2 \cap K_1 = \mathcal{O}_1$. V tem primeru pišemo $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$.

2.3.1. *Chevalleyev razširitveni izrek.* Če velja $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$, potem velja $\mathcal{M}_2 \cap K_1 = \mathcal{M}_2 \cap \mathcal{O}_1 = \mathcal{M}_1$ za pripadajoča maksimalna ideala $\mathcal{M}_1$ in $\mathcal{M}_2$ ter $\mathcal{O}_2^\times \cap K_1 = \mathcal{O}_2^\times \cap \mathcal{O}_1 = \mathcal{O}_1^\times$. Prepričajmo se samo v prvi dve enakosti, saj iz nje neposredno sledita drugi dve, brž ko si ogledamo komplemente glede na $\mathcal{M}_1$. Očitno velja $\mathcal{M}_2 \cap \mathcal{O}_1 \subseteq \mathcal{M}_2 \cap K_1$, obratna neenakost pa sledi iz dejstva, da je $\mathcal{M}_2 \subseteq \mathcal{O}_2$ in $\mathcal{O}_2 \cap K_1 = \mathcal{O}_1$. Če bi bil $x \in \mathcal{M}_2 \cap \mathcal{O}_1 = \mathcal{M}_2 \cap K_1$ obrnljiv $\mathcal{O}_1$, bi bil obrnljiv tudi v $\mathcal{O}_2$, kar pa ne velja. Zato je $\mathcal{M}_2 \cap \mathcal{O}_1 = \mathcal{M}_2 \cap K_1 \subseteq \mathcal{M}_1$, sedaj pa pokažimo še drugo smer zadnje neenakosti. Za $0 \neq x \in \mathcal{M}_1 \subseteq \mathcal{O}_1 \subseteq K_1$ velja $x^{-1} \notin \mathcal{O}_1 = \mathcal{O}_2 \cap K_1$, iz česar sledi $x^{-1} \notin \mathcal{O}_2$, saj je K_1 zaprt za inverze.

Tako smo dokazali zgornje enakosti. Sedaj bomo pokazali, da za vsako razširitev polj $K_2 \mid K_1$, kjer je K_1 polje, $\mathcal{O}_1$ pa njegov valuacijski podkolobar, obstaja razširitev $\mathcal{O}_2 \subseteq K_2$, ki je razširitev $\mathcal{O}_1$. Za to si bomo pomagali s spodnjim izrekom.

Izrek 2.39 ([4, izrek 3.1.1])**.** *(Chevalley) Naj bo K polje, $R \subseteq K$ kolobar in $P \subseteq R$ praideal R. Potem obstaja valuacijski kolobar $\mathcal{O}$, da velja $R \subseteq \mathcal{O}$ in $\mathcal{M} \cap R = P$, kjer je $\mathcal{M}$ maksimalni ideal $\mathcal{O}$.*

Dokaz. Definirajmo množico

$$\Sigma := \{(A, I) \mid R_P \subseteq A \subseteq K, PR_P \subseteq I \subseteq A, A \text{ kolobar}, I \text{ pravi ideal } A\},$$

kjer je R_P lokalizacija kolobarja R pri praidealu P. Množica Σ ni prazna, saj vsebuje par (R_P, PR_P). Na njej definiramo delno ureditev $\leq : (A_1, I_1) \leq (A_2, I_2)$ natanko tedaj, ko je $A_1 \subseteq A_2$ in $I_1 \subseteq I_2$. Ni težko videti, da je za vsako naraščajočo verigo parov $\{(A_i, I_i) \mid i \in I\} \subseteq \Sigma$, kjer je I neprazna, $\cup_{i\in I} A_i$ podkolobar K, $\cup_{i\in I} I_i$ pa njegov pravi ideal (kar sledi iz dejstva, da ne vsebuje 1). Iz definicije je očitno, da je par $(\cup_{i\in I} A_i, \cup_{i\in I} I_i) \in \Sigma$ zgornja meja za $\{(A_i, I_i) \mid i \in I\}$. Iz Zornove leme sledi, da ima Σ maksimalen element, ki ga označimo z $(\mathcal{O}, \mathcal{M})$. Zaradi maksimalnosti para je očitno, da je $\mathcal{M}$ maksimalen ideal $\mathcal{O}$, sicer bi lahko $\mathcal{M}$ povečali z upoštevanjem dejstva, da je v komutativnem kolobarju z enoto vsak ideal vsebovan v maksimalnem idealu. Prav tako zaradi maksimalnosti velja, da je $(\mathcal{O}, \mathcal{M})$ lokalen kolobar, sicer bi ga lahko povečali z lokalizacijo pri $\mathcal{M}$.

Pokažimo, da je $\mathcal{O}$ valuacijski kolobar. Pa recimo, da ni. Potem obstaja $x \in K^\times$, za katerega velja $x, x^{-1} \notin \mathcal{O}$. Iz maksimalnosti sledi, da je $\mathcal{M}\mathcal{O}[x] = \mathcal{O}[x]$, saj bi v nasprotnem primeru veljalo $(\mathcal{O}, \mathcal{M}) \subsetneq (\mathcal{O}[x], \mathcal{N}) \in \Sigma$, kjer bi bil $\mathcal{N}$ maksimalen ideal $\mathcal{O}[x]$, ki bi vseboval $\mathcal{M}\mathcal{O}[x]$. Zaradi enakega razloga velja tudi $\mathcal{M}\mathcal{O}[x^{-1}] = \mathcal{O}[x^{-1}]$. Ker je zato $1 \in \mathcal{M}\mathcal{O}[x] = \mathcal{M}\mathcal{O}[x^{-1}]$, obstajajo taki $a_0, a_1, \ldots, a_n \in \mathcal{M}$ ter $b_0, b_1, \ldots, b_m \in \mathcal{M}$, da je $1 = \sum_{i=0}^n a_i x^i = \sum_{i=0}^m b_i x^{-i}$. Izberimo najmanjša taka $m, n \in \mathbb{N}$, za katera obstajo taki koeficienti. Brez škode za splošnost lahko predpostavimo, da je $m \leq n$, sicer zamenjamo vlogi x in x^{-1}. Ker je $b_0 \in \mathcal{M}$, je $1 - b_0 \in \mathcal{O}^\times$, saj je $\mathcal{O}$ lokalen kolobar. Zato je tudi $1 - b_0 = \sum_{i=1}^m b_i x^{-i} \in \mathcal{O}^\times$. Če enakost delimo z $b_0 - 1$ dobimo $1 = \sum_{i=1}^m c_i x^{-i}$, kjer je $c_i = b_i/(1 - b_0)$, iz česar po množenju obeh strani z x^n sledi $x^n = \sum_{i=1}^m c_i x^{n-i}$. Dobimo $1 = \sum_{i=0}^n a_i x^i = \sum_{i=0}^{n-1} a_i x^i + a_n x^n = \sum_{i=0}^{n-1} a_i x^i + \sum_{i=1}^m a_n c_i x^{n-i}$. Ker v tej vsoti ne nastopa potenca

x^n, smo 1 zapisali kot vsoto $\sum_{i=0}^{n-1} d_i x^i$ (ker je $m \leq n$, negativnih potenc x v vsoti ni). To pa je v nasprotju z minimalnostjo takšnega n.

Pokazali smo, da je $(\mathcal{O}, \mathcal{M})$ valuacijski kolobar, za katerega po konstrukciji velja $R \subseteq R_P \subseteq \mathcal{O}$. Za konec dokaza moramo pokazati še, da je $\mathcal{M} \cap R = P$. To pa sledi iz dejstva, da je $\mathcal{M} \cap R_P = PR_P$, saj je PR_P maksimalen ideal R_P in velja $PR_P \cap R = P$. □

Posledica 2.40 ([4, posledica 3.1.2])**.** *Naj bo polje K_2 razširitev K_1, $\mathcal{O}_1 \subseteq K_1$ pa valuacijski kolobar. Potem obstaja valuacijski kolobar $\mathcal{O}_2 \subseteq K_2$, ki je razširitev $\mathcal{O}_1$.*

Dokaz. Po Chevalleyevem izreku obstaja tak valuacijski kolobar $\mathcal{O}_2 \subseteq K_2$ z maksimalnim idealom $\mathcal{M}_2$, da je $\mathcal{O}_1 \subseteq \mathcal{O}_2$ in $\mathcal{M}_2 \cap \mathcal{O}_1 = \mathcal{M}_1$. $\mathcal{M}_2 \cap \mathcal{O}_1$ je obenem tudi maksimalen ideal $\mathcal{O}_2 \cap K_1$, ki je valuacijski kolobar nad K_1. Torej sta $\mathcal{O}_1$ in $\mathcal{O}_2 \cap K_1$ valuacijska kolobarja na K_1, in ker sta njuna maksimalna ideala enaka, sledi $\mathcal{O}_1 = \mathcal{O}_2 \cap K_1$. □

Sedaj povejmo še nekaj lastnosti valuacijskih grup in polj ostankov razširitev. Naj bo $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$ razširitev polj z valuacijo in $v_i : K_i \to \Gamma_i \cup \{\infty\}$ za $i = 1, 2$ pripadajoči valuaciji in valuacijski grupi. Spomnimo se, da je $\Gamma_i \cong K_i^\times / \mathcal{O}_i^\times$. Preslikava $K_1^\times \to K_2^\times \to K_2^\times / \mathcal{O}_2^\times \cong \Gamma_2$ ima jedro $\mathcal{O}_2^\times \cap K_1^\times = \mathcal{O}_1^\times$. Zato obstaja vložitev $\Gamma_1 \cong K_1^\times / \mathcal{O}_1^\times \to \Gamma_2$. Zato lahko brez škode za splošnost grupo Γ_1 obravnavano kot podgrupo Γ_2. Indeks $e = e(\mathcal{O}_2/\mathcal{O}_1) := [\Gamma_2 : \Gamma_1]$ imenujemo *razvejitveni indeks* razširitve valuacije. Na podoben način vidimo, da je jedro preslikave $\mathcal{O}_1 \to \mathcal{O}_2 \to \mathcal{O}_2/\mathcal{M}_2 = \overline{K_2}$ enako $\mathcal{M}_2 \cap \mathcal{O}_1 = \mathcal{O}_2$, zato obstaja vložitev $\overline{K_1} = \mathcal{O}_1/\mathcal{M}_1 \to \overline{K_2}$ in na $\overline{K_1}$ spet brez škode za splošnost gledamo kot na podpolje $\overline{K_2}$. Indeks $f = f(\mathcal{O}_2/\mathcal{O}_1) := [\overline{K}_2 : \overline{K}_1]$ imenujemo *stopnja ostankov* razširitve valuacije. V primeru, ko je $e(\mathcal{O}_2/\mathcal{O}_1) = f(\mathcal{O}_2/\mathcal{O}_1) = 1$, pravimo, da je razširitev $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$ *neposredna*. Primer neposredne razširitve je denimo napolnitev polja z diskretno valuacijo. V primeru $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2) \subseteq (K_3, \mathcal{O}_3)$ seveda velja $e(\mathcal{O}_3/\mathcal{O}_1) = e(\mathcal{O}_3/\mathcal{O}_2)e(\mathcal{O}_2/\mathcal{O}_1)$ in $f(\mathcal{O}_3/\mathcal{O}_1) = f(\mathcal{O}_3/\mathcal{O}_2)f(\mathcal{O}_2/\mathcal{O}_1)$.

2.3.2. *Algebraične razširitve polj z valuacijo.* Spoznali smo, da za vsako razširitev polja z valuacijo obstaja tudi razširitev valuacije. Osredotočili se bomo na primer, ko je K_2 algebraična razširitev K_1 in ugotovili, kaj v tem primeru velja za kvocient Γ_2/Γ_1 in razširitev $\overline{K_1} \mid \overline{K_2}$.

Lema 2.41 ([4, izrek 3.2.2])**.** *Naj bo $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$ razširitev ter $v_i : K_1 \to \Gamma_i \cup \{\infty\}$ pripadajoči valuaciji za $i = 1, 2$. Naj bo $e = [\Gamma_2 : \Gamma_1]$ in $f = [\overline{K_2} : \overline{K_1}]$ in naj bodo $x_1, \ldots, x_f \in \mathcal{O}_2$ in $y_1, \ldots y_e \in K_2^\times$ taki, da velja:*

(1) *$\overline{x_1}, \ldots, \overline{x_f}$ so $\overline{K_1}$-linearno neodvisni elementi $\overline{K_2}$,*
(2) *$v_2(y_1), \ldots, v_2(y_e)$ so predstavniki različnih odsekov grupe Γ_2/Γ_1.*

Potem velja $v_2(\sum_{i=1}^f \sum_{j=1}^e a_{i,j} x_i y_j) = \min\{v_2(a_{i,j} x_i y_j) \mid 1 \leq i \leq f, 1 \leq j \leq e\}$ za vse $a_{i,j} \in K_1$.

Dokaz. Naj bodo $a_{i,j} \in K_1$ poljubni. Izberemo taka $1 \leq I \leq f$ in $1 \leq J \leq e$, da velja $v_2(a_{I,J} y_J) = \min\{v_2(a_{i,j} y_j) \mid 1 \leq i \leq f, 1 \leq j \leq e\}$. Najprej opazimo, da za $j \neq J$ in poljuben i velja $v_2(a_{i,j} y_j) > v_2(a_{I,J} y_J)$. V primeru enakosti $v_2(a_{i,j} y_j) = v_2(a_{I,J} y_J)$ bi namreč veljalo $v_2(y_J) - v_2(y_j) = v_2(a_{i,j}) - v_2(a_{I,J}) \in \Gamma_1$, kar je v nasprotju z predpostavko (2), po kateri sta $v_2(y_j)$ in $v_2(y_J)$ različna predstavnika Γ_2/Γ_1. Zato velja $v_2(a_{i,j} y_j (a_{I,J} y_J)^{-1}) > 0$ in torej tudi $a_{i,j} y_j (a_{I,J} y_J)^{-1} \in \mathcal{M}_2$ za vsak $j \neq J$.

Naj bo $z = \sum_{i=1}^f \sum_{j=1}^e a_{i,j} x_i y_j \in K_2$ in recimo, da velja $v_2(z) > \min\{v_2(a_{i,j} x_i y_j) \mid 1 \leq i \leq f, 1 \leq j \leq e\}$. Ker je $x_i \in \mathcal{O}_2$ za vsak i, je $\min\{v_2(a_{i,j} x_i y_j) \mid 1 \leq i \leq$

$f, 1 \leq j \leq e\} \geq \min\{v_2(a_{i,j}y_j) \mid 1 \leq i \leq f, 1 \leq j \leq e\} = v_2(a_{I,J}y_J)$. Zato je $v_2(z(a_{I,J}y_j)^{-1}) > 0$ in $z(a_{I,J}y_J)^{-1} \in \mathcal{M}_2$. Zapišimo

$$z = \sum_{i=1}^{f}\sum_{j=1}^{e} a_{i,j}x_iy_j = \sum_{i=1}^{f}\sum_{j=1,j\neq J}^{e} a_{i,j}x_iy_j + \sum_{i=1}^{f} a_{i,J}x_iy_J \in K_2$$

in potem obe strani delimo z $a_{I,J}y_J$. Dobimo

$$z(a_{I,J}y_J)^{-1} = \sum_{i=1}^{f}\sum_{j=1,j\neq J}^{e} a_{i,j}y_j(a_{I,J}y_J)^{-1}x_i + \sum_{i=1}^{f} a_{i,J}a_{I,J}^{-1}x_i.$$

Dobljeno enačbo kvocientiramo po $\mathcal{M}_2$ in dobimo $\sum_{i=1}^{f} \overline{a_{i,J}a_{I,J}^{-1}x_i} = 0$. Ker v tej vsoti vsi koeficienti $\overline{a_{i,J}a_{I,J}^{-1}}$ niso enaki nič (vzemimo npr. $i = I$), smo prišli do protislovja s predpostavko (1). □

Iz leme sledi, da so pari x_iy_j za $1 \leq i \leq f$, $1 \leq j \leq e$ med seboj K_1-linearno neodvisni, saj iz $\sum_{i=1}^{f}\sum_{j=1}^{e} a_{i,j}x_iy_j = 0$ sledi

$$v_2(\sum_{i=1}^{f}\sum_{j=1}^{e} a_{i,j}x_iy_j) = \min\{v_2(a_{i,j}x_iy_j) \mid 1 \leq i \leq f, 1 \leq j \leq e\} = \infty,$$

torej so vsi $a_{i,j} = 0$. Iz povedanega takoj sledi spodnja posledica.

Posledica 2.42 ([4, posledica 3.2.3])**.** *Naj bo $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$ razširitev, $n := [K_2 : K_1], e := [\Gamma_2 : \Gamma_1]$ in $f := [\overline{K_2} : \overline{K_1}]$. Potem velja $ef \leq n$.*

Iz te posledive sledita spodnji pomembni lastnosti valuacijskih grup in polj ostankov pri algebraičnih razširitvah polj z valuacijo, ki ju bomo pri dokazovanju izreku Ax-Kochen-Jeršov pogosto potrebovali.

Izrek 2.43 ([4, posledica 3.2.4])**.** *Naj bo $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$ razširitev, kjer je K_2 algebraičen nad K_1. Potem velja:*

(1) *Vsak element Γ_2/Γ_1 ima končen red,*
(2) *$\overline{K_2}$ je algebraična razširitev $\overline{K_1}$.*

Dokaz. Za dokaz prve točke izberemo poljuben $\gamma \in \Gamma_2$ in pokažemo, da je $n\gamma \in \Gamma_1$ za nek $n \in \mathbb{Z} \setminus \{0\}$. Izberimo tak $x \in K_2$, da je $v_2(x) = \gamma$. Naj bo $L := K_1(x), \mathcal{O} := \mathcal{O}_2 \cap L$, v valuacija na L, ki pripada $\mathcal{O}$, Γ pa pripadajoča valuacijska grupa, za katero lahko brez škode za splošnost predpostavimo, da je vsebovana v Γ_2. Po 2.42 je Γ/Γ_1 končna grupa, saj je $e(\mathcal{O}/\mathcal{O}_1) \leq [L : K_1]$, zato obstaja tako neničelno celo število n, da je $n\gamma \in \Gamma_1$.

Točko (2) dokažemo podobno kot prvo. Vzemimo poljuben $x \in K_2$ in naj bo spet $L = K_1(x)$. Potem iz 2.42 sledi $[\overline{L} : \overline{K_1}] \leq [L : K_1]$, zato je $\overline{x} \in \overline{L}$ algebraičen nad $\overline{K_1}$. □

Lema 2.44 ([4, posledica 3.2.6])**.** *Naj bodo $\mathcal{O}_1, \ldots, \mathcal{O}_n$ valuacijski kolobarji polja K, $\mathcal{M}_1, \ldots, \mathcal{M}_n$ pa pripadajoči maksimalni ideali. Naj bo $R := \cap_{i=1}^{n}\mathcal{O}_i$ in $P_i := R \cap \mathcal{M}_i$. Potem je $\mathcal{O}_i = R_{P_i}$ za $1 \leq i \leq n$.*

Dokaz. Vsak element R_{P_i} je oblike yx^{-1} za $y \in R \subseteq \mathcal{O}_i$ in $x \in R \setminus \mathcal{M}_i \subseteq \mathcal{O}_i \setminus \mathcal{M}_i$, zato je $R_{P_i} \subseteq \mathcal{O}_i$ za vsak i. Da dokažemo obratno inkluzijo, vzamemo poljuben $a \in \mathcal{O}_i$ in definiramo množico $I_a := \{j \mid a \in \mathcal{O}_j\}$. Naj bo $\overline{a_j} := a + \mathcal{M}_j \in \overline{K}_j$ za vsak $j \in I_a$. Naj bo p tako praštevilo, da za vsak $j \in I_a$ velja $p > \mathrm{char}(\overline{K}_j)$ in $\overline{a_j}^p \neq 1$, razen če je $\overline{a_j} = 1$, in $b := 1 + a + \cdots + a^{p-1}$. Če je $\overline{a_j} = 1$, je $\overline{b_j} = 1 + \ldots + 1 = p \neq 0$,

v nasprotnem primeru pa je $\overline{b_j} = (1-\overline{a_j}^p)/(1-\overline{a_j}) \neq 0$. S tem pridemo do zaključka, da je $b \in \mathcal{O}_j^\times$ za vsak $j \in I_a$. Če pa velja $j \in \{1, \ldots, n\} \setminus I_a$, velja $a \notin \mathcal{O}_j$ in zato $a^{-1} \in \mathcal{M}_1 \subseteq \mathcal{O}_j$. Potem je $1 + a^{-1} + \cdots + a^{-(p-1)} \in \mathcal{O}_j^\times$ in zato

$$b^{-1} = (1 + a + \cdots + a^{p-1})^{-1} = a^{-(p-1)}(1 + a^{-1} + \ldots + a^{-(p-1)})^{-1} \in \mathcal{O}_j,$$
$$ab^{-1} = a^{-(p-2)}(1 + a^{-1} + \ldots + a^{-(p-1)})^{-1} \in \mathcal{O}_j.$$

Ugotovili smo, da za vsak $1 \leq j \leq n$ velja $b^{-1}, ab^{-1} \in \mathcal{O}_j$, zato sta oba elementa tudi v R. Ker je $i \in I_a$, sledi $b, b^{-1} \in \mathcal{O}_i^\times$, zato je $b^{-1} \notin P_i = R \cap \mathcal{M}_i$. Pokazali smo, da je $a = ab^{-1}/b^{-1} \in R_{P_i}$. □

Izrek 2.45 ([4, izrek 3.2.7]). *Naj bodo $\mathcal{O}_i, \mathcal{M}_i, R$ in P_i za $1 \leq i \leq n$ kot v 2.44. Predpostavimo, da velja še $\mathcal{O}_i \not\subseteq \mathcal{O}_j$ za $i \neq j$. Potem velja:*

(1) *iz $i \neq j$ sledi $P_i \not\subseteq P_j$,*
(2) *$P_1, \ldots, P_n$ so vsi maksimalni ideali R,*
(3) *za vsak $(a_1, \ldots, a_n) \in \mathcal{O}_1 \times \cdots \times \mathcal{O}_n$ obstaja tak $a \in R$, da je $a - a_i \in \mathcal{M}_i$.*

Dokaz. (1) : Če je $P_i \subseteq P_j$, je po 2.44 $\mathcal{O}_j = R_{P_j} \subseteq R_{P_i} = \mathcal{O}_i$, kar je v nasprotju s predpostavko.

(2) : Pokazali bomo, da je vsak pravi ideal $I \subseteq R$ vsebovan v nekem P_i, $1 \leq i \leq n$. Pa recimo, da to ne drži, torej obstaja tak ideal I v R, da za vsak i obstaja $a_i \in I \setminus P_i$. Za vsak par $i \neq j$ izberimo $b_{i,j} \in P_i \setminus P_j$ (tak $b_{i,j}$ obstaja po (1)). Potem za $c_j := \Pi_{i \neq j} b_{i,j}$ velja $c_j \in P_i$ za $i \neq j$ in $c_j \notin P_j$, saj je P_j praideal. Enako velja za $a_j c_j$. Naj bo $d := \sum_{j=1}^n a_j c_j \in I$. Ker za vsak j velja, da natanko en člen vsote ni vsebovan v P_j, sledi $d \notin P_j = R \cap \mathcal{M}_j$ za vsak j. Torej je $d \notin \mathcal{M}_j$, zato je v $\mathcal{O}_j^\times$ za vsak $1 \leq j \leq n$. Potem je $d^{-1} \in R$, iz česar sledi, da je d obrnljiv v R, kar je v nasprotju z dejstvom, da je $d \in I$. Pokazali smo, da je vsak ideal R vsebovan v P_j za nek j, iz česar sledi, da so P_j vsi maksimalni ideali, saj po (1) noben ni vsebovan v drugem.

(3) : Iz (1) in (2) sledi, da je $P_i + P_j = R$ za $i \neq j$. Po kitajskem izreku o ostankih je zato kvocientna preslikava $R \to R/P_1 \times \cdots \times R/P_n$ surjekcija. Ker velja $R_{P_i}/P_i R_{P_i} \cong R/P_i$ in, po lemi 2.44, $R_{P_i} = \mathcal{O}_i$ ter $P_i R_{P_i} = \mathcal{M}_i$ za vsak i, zato obstaja surjekcija $R \to \mathcal{O}_1/\mathcal{M}_1 \times \cdots \times \mathcal{O}_n/\mathcal{M}_n$. Iskani $a \in R$ je praslika $(a_1 + \mathcal{M}_1, \ldots, a_n + \mathcal{M}_n)$ za to surjekcijo. □

Sedaj pokažimo še, da je predpostavka zgornjega izreka v primeru različnih razširitev valuacijskega kolobara pri algebraični razširitvi polja z valuacijo vedno izpolnjena.

Lema 2.46 ([4, lema 3.2.8]). *Naj bo $K_2 \mid K_1$ algebraična razširitev polj. Naj bo $\mathcal{O}$ valuacijski kolobar K_1, $\mathcal{O}'$ in $\mathcal{O}''$ pa dve različni razširitvi $\mathcal{O}$ na K_2. Če je $\mathcal{O}' \subseteq \mathcal{O}''$, potem velja $\mathcal{O}' = \mathcal{O}''$.*

Dokaz. Recimo, da velja $\mathcal{O}' \subseteq \mathcal{O}''$, iz česar sledi $\mathcal{M}'' \subseteq \mathcal{M}'$. Označimo $\overline{K}'' := \mathcal{O}''/\mathcal{M}''$. Naj bo $x \in K$ poljuben. Ker je eden izmed x in $x^{-1} \in \mathcal{O}''$ vsebovan v $\mathcal{O}'$, je eden izmed $x\mathcal{M}''$ in $x^{-1}\mathcal{M}''$ vsebovan v $\overline{\mathcal{O}'} := \mathcal{O}'/\mathcal{M}''$. Zato je $\overline{\mathcal{O}'}$ valuacijski kolobar $\overline{K}''$. Ker sta $\mathcal{O}'$ in $\mathcal{O}''$ razširitvi $\mathcal{O}$, velja $\mathcal{M}'' \cap \mathcal{O} = \mathcal{M}$ in $\mathcal{O} \subseteq \mathcal{O}'$, zato lahko $\overline{K} = \mathcal{O}/\mathcal{M}$ vložimo v $\overline{\mathcal{O}}'$. Brez škode za splošnost predpostavimo, da je v $\overline{\mathcal{O}}'$ tudi vsebovan. Po izreku 2.43 je $\overline{K}''$ algebraična razširitev $\overline{K}$. Ker je vsako polje z valuacijo enako polju ulomkov valuacijskega kolobarja, je $\overline{K}''$ polje ulomkov za $\overline{\mathcal{O}'}$. Potem je tudi $\overline{\mathcal{O}'}$ polje. Res: naj bo $0 \neq \overline{x} \in \overline{\mathcal{O}'}$ poljuben. Pokažimo, da ima inverz

v $\overline{\mathcal{O}'}$. Ker je $\overline{x^{-1}} \in \overline{K''}$, ki je algebraična razširitev $\overline{K} \subseteq \overline{\mathcal{O}'}$, obstajajo $\overline{a_i} \in \overline{\mathcal{O}'}$, da velja $\overline{x}^{-n} + \overline{a_{n-1}}\overline{x}^{-(n-1)} + \cdots + \overline{a_0} = 0$ oz., če enakost na obeh stranih pomnožimo z $\overline{x}^{(n-1)}$, $\overline{x}^{-1} + \overline{a_{n-1}} + \cdots + \overline{a_0}\overline{x}^{(n-1)} = 0$. Torej je $\overline{x}^{-1} \in \overline{\mathcal{O}'}$. Pokazali smo, da je $\overline{\mathcal{O}'}$ polje, in ker je tudi valuacijski podkolobar $\overline{K''}$, sledi $\mathcal{O}'/\mathcal{M}'' = \overline{\mathcal{O}'} = \overline{K''} = \mathcal{O}''/\mathcal{M}''$. Zato je tudi $\mathcal{O}' = \mathcal{O}''$. Iz $\mathcal{O}'/\mathcal{M}'' = \mathcal{O}''/\mathcal{M}''$ namreč sledi, da je $\mathcal{O}'/\mathcal{M}''$ polje, torej je $\mathcal{M}''$ maksimalni ideal $\mathcal{O}'$, iz česar sledi $\mathcal{M}'' = \mathcal{M}'$. □

V naslednjih izrekih bomo spoznali, da lahko za nekatere razširitve K_2 polja z valuacijo $(K_1, \mathcal{O}_1)$ število pripadajočih razširitev valuacije $\mathcal{O}_1 \subseteq \mathcal{O}_2$ omejimo navzgor. Pred tem se bomo spomnili relevantnih definicij in rezultatov iz teorije razširitev obsegov. Pravimo, da je polinom $p \in K_1[x]$ *separabilen*, če ima v svojem razpadnem obsegu same enostavne ničle oz., ekvivalentno, je tuj proti svojemu formalnemu odvodu. Element $a \in K_2$, kjer je $K_2 \mid K_1$ algebraična razširitev, je *separabilen*, če je separabilen njegov minimalni polinom. Sicer je *neseparabilen*. *Separabilna razširitev polja* K_1 je množica vseh separablinih elementov nad K_1. Vsaka separabilna razširitev je algebraična. Pravimo, da je obseg K_1 *perfekten*, če je vsak element, ki je algebraičen nad njim, tudi separabilen. Vsi obsegi s karakteristiko nič in vsi končni obsegi so perfektni. Če je K_1 polje s karakteristiko p, pravimo, da je $a \notin K_1$ *čisto neseparabilen* nad K_1, če ima njegov minimalni polinom obliko $x^{p^k} - b \in K_1[x]$, ali, ekvivalentno, velja $a^{p^k} \in K_1$ za neko naravno število k. Če je a algebraičen nad K_1, potem obstaja neko naravno število k, da je a^{p^k} separabilen nad K_1. Razširitev obsegov $K_2 \mid K_1$ je *normalna*, če je vsak polinom s koeficienti v K_1 bodisi nerazcepen v K_2 bodisi v K_2 razpade na same linearne faktorje. Če je razširitev normalna in separabilna, je *Galoisova*. Vsaka normalna razširitev perfektnega polja je Galoisova.

Naj bo $K_2 \cap K_1^s := \{x \in K_2 \mid x \text{ je separabilen nad } K_1\}$. $K_2 \cap K_1^s$ je separabilna razširitev polja K_1. S $[K_2 : K_1]^s := [K_2 \cap K_1^s : K_1]$ označimo *stopnjo separabilnosti* K_2 nad K_q, s $[K_2 : K_1]^i := [K_2 : K_2 \cap K_1^s]^i$ pa *stopnjo neseparabilnosti* K_2 nad K_1. Če je K_1 perfekten, je $[K_2 : K_1]^s = [K_2 : K_1]$ in $[K_2 : K_1]^i = 1$. Vsak element $x \in K_2 \setminus K_2 \cap K_1^s$ je čisto neseparabilen nad $K_2 \cap K_1^s$. Sedaj lahko povemo nekaj o številu razširitev valuacij v primeru, ko je stopnja separabilnosti razširitve končna.

Izrek 2.47 ([4, lema 3.2.8])**.** *Naj bo K_2 algebraičen nad K_1, kjer velja $[K_2 : K_1]^s < \infty$, in naj bo $\mathcal{O}$ valuacijski kolobar K_1. Če z n označimo število različnih razširitev $\mathcal{O}$ na K_2, velja $n \leq [K_2 : K_1]^s$. V posebnem to pomeni, da je takih različnih razširitev končno mnogo.*

Dokaz. Naj bodo $\mathcal{O}_1, \ldots, \mathcal{O}_m$ različne razširitve $\mathcal{O}$ na K_2 z maksimalnimi ideali $\mathcal{M}_1, \ldots, \mathcal{M}_m$. Iz leme 2.46 sledi, da so različni $\mathcal{O}_i$ medsebojno neprimerljivi glede na relacijo vsebovanosti. Zato, če se skličemo na točko (3) izreka 2.45, obstajajo taki $c_1, \ldots, c_m \in K_2$, da velja $c_j - 1 \in \mathcal{M}_j$ in $c_j \in \mathcal{M}_i$ za $i \neq j$. Če je karakteristika K_1 enaka $p > 0$, izberemo dovolj velik k, da so $c_1^{p^k}, \ldots, c_m^{p^k}$ vsi separabilni nad K_1, sicer za k vzamemo nič.

Pokažimo, da so izbrani elementi $c_1^{p^k}, \ldots, c_m^{p^k}$ K_1-linearno neodvisni. Pa recimo, da to ne velja, torej obstajajo $a_1, \ldots, a_n$, ne vsi enaki nič, da je $\sum_{i=1}^m a_i c_i^{p^k} = 0$. Naj bo $1 \leq j \leq m$ tak, da je $v(a_j) = \min\{v(a_1), \ldots, v(a_m)\}$. Potem je $a_j \neq 0$, zato lahko z njim delimo enakost in dobimo $c_j^{p^k} = -\sum_{i=1, i\neq j}^m a_j^{-1} a_i c_i^{p^k} \in \mathcal{M}_j$, kar je zato, ker so $\mathcal{M}_i$ praideali, v nasprotju z dejstvom, da je $c_j \in M_i$ natanko tedaj, ko velja $i \neq j$.

Torej so $c_i^{p^k} \in K_2 \cap K_1^s$ medsebojno K_1-linearno neodvisni, iz česar sledi $m \leq [K_2 : K_1]^s$. Izrek je tako dokazan. □

Izrek ima za čisto neseparabilne razširitve takojšnjo posledico, saj za čisto neseparabilno razširitev velja $[K_2 : K_1]^s = 1$.

Posledica 2.48 ([4, lema 3.2.8])**.** *Naj bo K_2 čisto neseparabilna razširitev polja z valuacijo $(K_1, \mathcal{O}_1)$. Potem je razširitev $\mathcal{O}_1 \subseteq \mathcal{O}_2$ enolično določena.*

Sedaj si lahko odnos med različnimi razširitvami valuacijskih kolobarjev, ki pripadajo normalnim razširitvam polj.

Izrek 2.49 ([4, lema 3.2.13])**.** *Naj bo $L \mid K$ končna normalna razširitev polj in $G = Aut(L \mid K)$. Naj bo $\mathcal{O}$ valuacijski kolobar na K, $\mathcal{O}'$ in $\mathcal{O}''$ pa njegovi razširitvi na L. Potem obstaja tak $\sigma \in G$, da $\sigma(\mathcal{O}') = \mathcal{O}''$.*

Dokaz. Najprej se prepričajmo, da se lahko omejimo na primer, ko je $L \mid K$ separabilna, torej tudi Galoisova razširitev. Če je $\mathcal{O}'$ razšitev $\mathcal{O}$ na $L \cap K^s$, jo lahko po posledici 2.48 razširimo na L na en sam način. Torej so razširitve $\mathcal{O}$ na $L \cap K^s$ v bijektivni korespondenci z razširitvami $\mathcal{O}$ na L. Prav tako lahko vsak $\sigma \in \mathrm{Aut}(L \cap K^s \mid K)$ razširimo do $\sigma' \in G$. Zato se lahko omejimo na razširitve σ na $L \cap K^s$, oz. brez škode za splošnost predpostavimo, da je $L \mid K$ separabilna razširitev.

Predpostavimo torej, da je L končna Galoisova razširitev K. Naj bosta $\mathcal{O}'$ in $\mathcal{O}''$ razširitvi $\mathcal{O}$ na L. Definiramo $H' := \{\sigma \in G \mid \sigma(\mathcal{O}') = \mathcal{O}'\}$ ter $H'' := \{\tau \in G \mid \tau(\mathcal{O}'') = \mathcal{O}''\}$. Ker je $\sigma(\mathcal{M}')$ maksimalen ideal $\sigma(\mathcal{O}') = \mathcal{O}'$, iz lokalnosti $\mathcal{O}'$ sledi $\sigma(\mathcal{M}') = \mathcal{M}'$ za vsak $\sigma \in H'$. Podobno sklepamo, da je $\tau(\mathcal{M}'') = \mathcal{M}''$ za vsak $\tau \in H''$. Sedaj zapišimo G kot unijo odsekov po H' oz. H'': $G = \cup_{i=1}^{n} H'\sigma_i^{-1} = \cup_{j=1}^{m} H''\tau_j^{-1}$ za primerne $\sigma_i, \tau_j \in G$. Ker sta za $1 \leq i < j \leq n$ σ_i^{-1} in σ_j^{-1} predstavnika različnih odsekov G po H', velja $\sigma_i(\mathcal{O}') \neq \sigma_j(\mathcal{O}')$. V nasprotnem primeru bi sledilo $\sigma_j^{-1}\sigma_i(\mathcal{O}') = \mathcal{O}'$, kar pa je v nasprotju z $H'\sigma_i^{-1} \neq H'\sigma_j^{-1}$. Po lemi 2.46 sledi $\sigma_i(\mathcal{O}') \not\subseteq \sigma_j(\mathcal{O}')$. Analogno se prepričamo, da za $1 \leq i < j \leq m$ velja $\tau_i(\mathcal{O}'') \not\subseteq \tau_j(\mathcal{O}'')$. Predpostavimo še, da velja $\sigma_i(\mathcal{O}') \not\subseteq \tau_j(\mathcal{O}'')$ in $\tau_j(\mathcal{O}'') \not\subseteq \sigma_i(\mathcal{O}')$ za vse $1 \leq i \leq n$ in $1 \leq j \leq m$. To nas bo vodilo do protislovja.

Naj bo $R := \cap_{i=1}^{n} \sigma_i(\mathcal{O}') \cap \cap_{j=1}^{m} \tau_j(\mathcal{O}')$. Po tretji točki izreka 2.45 obstaja $a \in R$, za katerega velja $a - 1 \in \sigma_i(\mathcal{M}')$ za $1 \leq i \leq n$ in $a \in \tau_j(\mathcal{M}'')$ za $1 \leq j \leq m$. Za poljuben $\sigma \in G$ obstajata tak i in tak $\rho \in H'$, da je $\sigma = \rho\sigma_i^{-1}$. Po drugi strani obstajata tak j in $\rho' \in H''$, da je $\sigma = \rho'\tau_j^{-1}$. Za vsak $\sigma \in G$ in a, kot smo ga definirali zgoraj, potem po eni strani velja $\sigma(a-1) = \rho\sigma_i^{-1}(a-1)$. Ker je $a - 1 \in \sigma_i(\mathcal{M}')$, je $\sigma(a-1) = \rho\sigma_i^{-1}(a-1) \in \rho\sigma_1^{-1}(\sigma_1(\mathcal{M}')) = \mathcal{M}'$, saj je $\rho \in H'$. Enako sklepamo, da je $\sigma(a) \in \mathcal{M}''$ za vsak $\sigma \in G$. $\Pi_{\sigma \in G}\sigma(a)$ je enak konstantnemu členu minimalnega polinoma za a v K, zato je vsebovan K. Kot smo premislili, je, ker je $\sigma(a) \in 1 + \mathcal{M}'$ za vsak $\sigma \in G$, tudi $\Pi_{\sigma \in G}\sigma(a) \in \mathcal{M}' + 1$. Po drugi strani je, kot premislimo na enak način, $\Pi_{\sigma \in G}\sigma(a) \in \mathcal{M}''$. Ker je $\mathcal{M}' \cap K = \mathcal{M}'' \cap K = \mathcal{M}$, je $\Pi_{\sigma \in G}\sigma(a) \in \mathcal{M} \cap (1 + \mathcal{M})$, kar pa ni mogoče.

Prišli smo do protislovja s predpostavko, da velja $\sigma_i(\mathcal{O}') \not\subseteq \tau_j(\mathcal{O}'')$ in $\tau_j(\mathcal{O}'') \not\subseteq \sigma_i(\mathcal{O}')$ za vse $1 \leq i \leq n$ in $1 \leq j \leq m$. Torej obstajata taka i, j, da je $\sigma_i(\mathcal{O}') \subseteq \tau_j(\mathcal{O}'')$ ali obratno. V obeh primerih po 2.46 sledi $\sigma_i(\mathcal{O}') = \tau_j(\mathcal{O}'')$ in zato $\tau_j^{-1}\sigma_i(\mathcal{O}') = \mathcal{O}''$. S tem je izrek dokazan. □

2.3.3. *Razširitev valuacije na polje racionalnih funkcij.* Pri dokazovanju izreka Ax-Kochen - Jeršov nam bosta v pomoč tudi naslednji trditvi o razširitvah valuacij na polje racionalnih funkcij. Takšne razširitve smo v primeru, ko je valuacija na polju trivialna, že spoznali.

Lema 2.50. [3] *Naj bo K polje z valuacijo v in Γ pripadajoča valuacijska grupa. Naj bo Γ' urejena abelova grupa, ki vsebuje Γ in $\gamma \in \Gamma'$ poljuben. Potem obstaja enoličnо določena valuacija na polju racionalnih funkcij $w : K(X) \to \Gamma \oplus \mathbb{Z}\gamma$ na polju racionalnih funkcij $K(x)$, za katero velja $w(\sum_{j=0}^{n} a_j x^j) = \min_{0\leq j\leq n}(v(a_j)+j\gamma)$ za vsak polinom $p = \sum_{j=0}^{n} a_j x^j$.*

Dokaz. Najprej bomo definirali w na kolobarju poliomov $K[x]$. Za $p(x) = \sum_{j=0}^{n} a_j x^j$ definiramo $w(p(x)) := \min_{0\leq j\leq n}(v(a_j) + j\gamma), w(0) := \infty$. Pokažimo, da w na $K[x]$ zadošča aksiomom valuacije. Prvi velja po definiciji. Za polinoma $p(x) = \sum_{j=0}^{n} a_j x^j$ in $q(x) = \sum_{j=0}^{m} b_j x^j$ je (brez škode za splošnost predpostavimo, da je $m = n$, sicer dodamo monome z ničelnimi koeficienti) $w(p(x)+q(x)) = \min_{0\leq j\leq n}\{v(a_j+b_j)+j\gamma\}$. Ker je za vsak $0 \leq j \leq n$

$$v(a_j + b_j) + j\gamma \geq \min\{v(a_j), v(b_j)\} + j\gamma = \min\{v(a_j) + j\gamma, v(b_j) + j\gamma\}, \text{ je}$$
$$w(p(x) + q(x)) \geq \min_{0\leq j\leq n}\{\min\{v(a_j) + j\gamma, v(b_j) + j\gamma\}\} = \min\{w(p(x), w(g(x))\}.$$

Sedaj dokažimo še, da velja $w(pq) = w(p)w(q)$. Naj bo i_1 najmanjši j, da je $\alpha := w(p(x)) = v(a_j) + j\gamma$ in i_2 najmanjši j, da je $\beta := w(q(x)) = v(b_j) + j\gamma$. Za $0 \leq j, j' \leq n$ velja $w(a_j b_{j'} x^{j+j'}) = (v(a_j) + členov) + (v(b_{j'}) + j'\gamma) \geq \alpha + \beta$, iz česar sledi $w(pq) \geq \alpha+\beta$, saj je $p(x)q(x)$ vsota koeficientov zgornje oblike $a_j b_{j'} x^{j+j'}$. Pokazati moramo še neenakost v obratni smeri. Zapišimo $p(x)q(x) = \sum_{j=0}^{n^2} c_j x^j$. Ker je $c_j = \sum_{l=0}^{j} a_l b_{j-l}$ (za $i > n$ definiramo $a_i = b_i = 0$), je $w(c_j x^j) = \min_{0\leq l\leq j}\{v(a_l) + v(b_{j-l}) + j\gamma\}$. Ta minimum je pri $j = i_1 + i_2$ dosežen, ko je $l = i_1$, kjer je enak $v(a_{i_1}) + v(b_{i_2}) + (i_1 + i_2)\gamma = \alpha + \beta$. Ker je

$$w(p(x)q(x)) = \min_{0\leq j\leq n^2}\{v(c_j)x^j + j\gamma\} = \min_{0\leq j\leq n^2}\min_{0\leq l\leq j}\{v(a_l) + v(b_{j-l}) + j\gamma\},$$

je zato $w(p(x)q(x)) \leq \alpha + \beta$.

Pokazali smo, da w na $K[x]$ zadošča aksiomom valuacije. Kot smo to naredili velikokrat prej v nalogi, se ni težko prepričati, da lahko to valuacijo s predpisom $w(p/q) := w(p) - w(q)$ enoličnо razširimo še na $K(x)$. S tem je lema dokazana. □

Trditev 2.51. [3] *Naj bo K polje z valuacijo v in Γ pripadajoča valuacijska grupa. Naj bo Γ' urejena abelova grupa, ki vsebuje Γ in $\gamma \in \Gamma' \setminus \Gamma$ tak, da je urejena abelova podgrupa $\Gamma \oplus \mathbb{Z}\gamma \subseteq \Gamma'$ direktna vsota oz. da iz $n\gamma \in \Gamma$ sledi $n = 0$ za vsako celo število n. Potem obstaja enoličnо določena valuacija $w : K(x) \to \Gamma \oplus \mathbb{Z}\gamma$, da velja $w(x) = \gamma$ in $w(a) = v(a)$ za $a \in K$. V tem primeru je pripadajoče polje ostankov $\overline{K(x)}$ enako $\overline{K}$.*

Dokaz. Najprej pokažemo, da je w enoličnо določena. Naj bo $p(x) = \sum_{j=0}^{m} a_j x^j$. Videti želimo, da je $w(p(x)) = \min_{0\leq j\leq m} w(a_j x^j) = \min_{0\leq j\leq m}(v(a_j) + j\gamma)$. Vsi monomi $a_j x^j$ v vsoti imajo različno vrednost za w. V nasprotnem bi za $j \neq j'$ veljalo $w(a_j x^j) = w(a_{j'} x^{j'})$ in zato $v(a_j) - v(a_{j'}) = (j - j')\gamma$, kar pa zaradi predpostaljene direktnosti vsote $\Gamma \oplus \mathbb{Z}\gamma$ ni mogoče. Zato je $w(p(x)) = \min_{0\leq j\leq n}(v(a_j) + j\gamma)$, iz česar po 2.50 sledi, da w obstaja in je enoličnо določena. Prav tako je očitno, da je $\Gamma \oplus \mathbb{Z}\gamma$ pripadajoča valuacijska grupa.

Vsak polinom $p(x) \neq 0$ lahko zapišemo v obliki $p = ax^n(1 + q(x))$ za $a \in K \setminus \{0\}$, $n \in \mathbb{N}_0$ in $q \in K(x)$, $w(q(x)) > 0$. Res: naj bo $0 \leq k \leq n$ takšen, da je $w(a_k x^k) =$

$\min_{0\le j\le n} w(a_jx^j)$. Potem je

$$\begin{aligned} p(x) &= a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \\ &= a_kx^k(a_n/a_kx^{n-k} + \cdots + a_{k+1}/a_kx + 1 + a_{k-1}/a_kx^{-1} + \cdots a_0/a_kx^{-k}). \end{aligned}$$

Ker je za $j \neq k$ $w(a_jx^j) > w(a_kx^k)$ (enakosti po zgornjem razmisleku ne more biti), je $w(a_n/a_kx^{n-k} + \cdots + a_{k+1}/a_kx + a_{k-1}/a_kx^{-1} + \cdots a_0/a_kx^{-k}) > 0$. Če označimo s $q(x) := a_n/a_kx^{n-k} + \cdots + a_{k+1}/a_kx + a_{k-1}/a_kx^{-1} + \cdots a_0/a_kx^{-k}$, smo p zapisali na želen način. Zato lahko vsako neničelno racionalno funkcijo $r(x)$ zapišemo v obliki $r(x) = ax^n(1 + q(x))$ za $a \in K \setminus \{0\}$, $n \in \mathbb{Z}$ in $q \in K(x)$, $w(q(x)) > 0$ (postopek pretvorbe je isti, samo da pred tem izpostavimo najnižjo potenco x). Zato je $w(r(x)) = w(ax^n) + w(1 + q(x)) = v(a) + n\gamma$. Sledi, da je $w(r(x)) = 0$ če in samo če velja $v(a) = 0$ in $n = 0$. Če torej velja $w(r) = 0$, je $\overline{r} = \overline{a}$, saj je v tem primeru $p(x) = a_0 + a_ix + \ldots a_nx^n$, kjer je $w(a_0) = 0$ in $w(a_ix^i) > 0$ za $i \geq 1$. Iz tega sledi, da je polje ostankov $\overline{K(x)}$ enako $\overline{K}$. □

Trditev 2.52. [3] *Naj bo K polje z valuacijo v, Γ in $\overline{K}$ pa pripadajoča valuacijska grupa in polje ostankov. Potem obstaja enolično določena valuacija w na $K(x)$, da je $w(x) = 0$, $w(a) = v(a)$ za $a \in K$, $\overline{x}$ pa transcendenten nad $\overline{K}$. Pripadajoča valuacijska grupa je pri tem enaka Γ, polje ostankov pa $\overline{K}(\overline{x})$.*

Dokaz. Po 2.50 bo za enoličnost w zadoščalo pokazati, da za vsak neničeln polinom $p(x) = \sum_{j=0}^n a_jx^j \in K[x]$ velja $w(p(x)) = \min_{0\le j\le n} v(a_j)$. Brez škode za splošnost lahko predpostavimo, da za vsak j velja $v(a_j) \geq 0$ in da za nek j velja $v(a_j) = 0$, sicer p pomnožimo s takim $a \in K$, da velja $v(a) = -\min_{0\le j\le n} v(a_j)$. Ker je po predpostavki $w(x) = 0$, je $w(p(x)) \geq 0$ in zato $p(x) \in \mathcal{O}$. Potem je $\overline{p(x)} = \sum_{j=0}^n \overline{a_jx^j}$. Ker je po predpostavki $\overline{x}$ transcendenten nad $\overline{K}$, je $\overline{p(x)} \neq 0$. Zato je $w(p(x)) = 0 = \min_{0\le j\le n} w(a_j) = \min_{0\le j\le n} v(a_j)$.

Sedaj dokažimo še obstoj w. Če za polinom $p(x) = \sum_{j=0}^n a_jx^j$ definiramo $w(p) = \min_{0\le j\le n} v(a_j)$, smo definirali valuacijo na $K[x]$, ki jo lahko razširimo na $K(x)$. Dokaz za to je identičen dokazu 2.50. Iz definicije sledi $w(x) = 0$. Sedaj bomo pokazali, da je $\overline{x}$ transcendenten nad $\overline{K}$. Pa recimo, da to ne drži in je $\sum_{j=0}^n \overline{a_jx^j} = 0$ za neke $a_j \in \mathcal{O}$, kjer je $v(a_n) = 0$. Potem je $w(\sum_{j=0}^n a_jx^j) > 0$, zato je $v(a_j) > 0$, iz česar sledi $\overline{a_j} = 0$ za vsak j, s čimer smo prišli do protislovja. Torej je $\overline{x}$ res transcendenten nad $\overline{K}$.

Ostane nam še, da pokažemo, da je polje ostankov, ki pripada w in ga označimo s $\overline{K(x)}$, enako $\overline{K}(\overline{x})$. Naj bo $r \in K(x)$ poljuben. Potem ga lahko zapišemo v obliki $c(\sum_{j=0}^n a_jx^j)/(\sum_{l=0}^m b_lx^l)$, kjer so $c, a_j, b_l \in K$, $v(a_j) \geq 0$ in $v(b_l) \geq 0$ za vse j, l, kjer je enakost dosežena vsaj pri enem j in vsak pri enem l. Potem, ker je $w(\sum_{j=0}^n a_jx^j) = w(\sum_{l=0}^m b_lx^l) = 0$, velja $w(r) \geq 0$ natanko tedaj, ko velja $w(c) \geq 0$. V tem primeru velja $\overline{r(x)} = \overline{c}(\sum_{j=0}^n \overline{a_jx^j})/(\sum_{l=0}^m \overline{b_l}\overline{x^l})$. Torej je polje ostankov $\overline{K(x)}$ res enako $\overline{K}(\overline{x})$. □

2.4. **Henselova polja.** Iz trditev, ki smo jih pokazali v prejšnjem podpoglavju, sledi, da če je $K' \mid K$ transcendentna razširitev polja K z netrivialno valuacijo, potem razširitev valuacije ni enolično določena. Na naslednjih straneh pa bomo spoznali polja K, za katere v primeru algebraične razširitve $K' \mid K$ velja, da je pripadajoča razširitev valuacijskega kolobarja enolično določena.

Definicija 2.53. Polje z valuacijo $(K, \mathcal{O})$ je *Henselovo*, če je za vsako algebraično razširitev $K' \mid K$ razširitev valuacijskega kolobarja $\mathcal{O}'$ enolično določena.

Da dokažemo, da so polna polja z diskretno valuacijo Henselova, si bomo pomagali s Henselovo lemo. Pred tem pa nekaj definicij: za polinom $f \in \mathcal{O}[x]$, ki ga zapišemo v obliki $f(x) = a_n x^n + \cdots + a_1 x + a_0$, je $\overline{f}(x) := \overline{a_n} x^n + \cdots + \overline{a_1} x + \overline{a_0}$ in $f'(x) = n a_n x^{n-1} + \cdots + 2a_2 x + a_1$ formalni odvod f.

Izrek 2.54 ([4, izrek 1.3.1])**.** *(Henselova lema) Naj bo K polno polje z diskretno valuacijo. Naj bo $f \in \mathcal{O}[x]$ in $a_0 \in \mathcal{O}$ tak, da je $v(f(a_0)) > 2v(f'(a_0))$. Potem obstaja tak $a \in \mathcal{O}$, da je $f(a) = 0$ in $v(a_0 - a) > v(f'(a_0))$.*

Dokaz. V dokazu bomo skonstruirali Cauchyjevo zaporedje, ki bo konvergiralo proti primernemu a. Naj bo $b_0 := f'(a_0)$. Iz $v(f(a_0)) > 2v(f'(a_0)) = v(b_0^2)$ sledi, da obstaja tak $N > 0$, da velja $v(f(a_0)) \geq v(b_0^2)+N$, torej je $v(f(a_0))-v(b_0^2) = v(f(a_0)/b_0^2) > N$, zato obstaja tak $c_0 \in \mathcal{M}, v(c_0) \geq N$, da velja $f(a_0) = b_0^2 c_0$. Označimo $a_1 := a_0 - b_0 c_0$. Oglejmo si:

$$\begin{aligned} f(a_1) &= d_n a_1^n + \cdots d_1 a_1 + d_0 = \\ &= d_n (a_0 - b_0 c_0)^n + d_{n-1}(a_0 - b_0 c_0)^{n-1} + \cdots d_1 (a_0 - b_0 c_0) + d_0 = \\ &= d_n a_0^n + d_{n-1} a_0^{n-1} + \cdots d_1 a_0 + d_0 \\ &- (d_n a^{n-1} n b_0 c_0 + d_{n-1} a_0^{n-2}(n-1) b_0 c_0 + \cdots d_1 b_0 c_0) + b_0^2 c_0^2 d, \end{aligned}$$

kjer je $d \in \mathcal{O}$. Ugotovili smo, da je $f(a_1) = f(a_0) - b_0 c_0 f'(a_0) + b_0^2 c_0^2 d = b_0^2 c_0 - b_0^2 c_0 + b_0^2 c_0^2 d$. Sledi, da je $v(f(a_1)) \geq v(b_0^2) + 2N$. Postopek ponovimo za $f'(a_1)$:

$$\begin{aligned} f'(a_1) &= n d_n a_1^{n-1} + \cdots 2 d_2 a_1 + d_1 = n d_n (a_0 - b_0 c_0)^{n-1} + \ldots + d_1 \\ &= d_n a_0^{n-1} + \cdots 2 d_2 a_0 + d_1 - b_0 c_0 d' = f'(a_0) - b_0 c_0 d' = b_0 - b_0 c_0 d' \end{aligned}$$

za $d' \in \mathcal{O}$. Sledi, da je $b_1 := f'(a_1) = b_0(1 - c_0 d')$. Ker je $v(c_0) > 0$, to velja tudi za $v(c_0 d')$ in zato je $v(1 - c_0 d') = v(1) = 0$. Sledi, da je $v(b_1) = v(b_0)$. Torej je $v(f(a_1)) \geq v(b_1^2) + 2N$.

Sedaj ponovimo postopek: najprej opazimo, da obstaja tak $c_1 \in O, v(c_1) \geq 2N$, da je $f(a_1) = b_1^2 c_1$, nato definiramo $a_2 = a_1 - b_1 c_1$ in z enakim postopkom razpišemo $f(a_2)$ in $b_2 := f'(a_2)$. Enako kot prej ugotovimo, da je $v(b_2) = v(b_0)$ in $f(a_2) = b_2^2 c_2$, kjer je $v(c_2) \geq 4N$. In tako naprej.

Ko postopek ponovimo neskončnokrat, dobimo zaporedja $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}}$ in $(c_n)_{n\in\mathbb{N}}$ v O, za katera velja:

(1) $f'(a_n) = b_n$,
(2) $f(a_n) = b_n^2 c_n$,
(3) $v(b_n) = v(b_0)$,
(4) $v(c_n) \geq 2^n N$,
(5) $a_{n+1} = a_n - b_n c_n$.

Naj bo $m \leq n$. Potem je

$$v(a_n - a_m) = v(\sum_{i=m}^{n-1} (a_{i+1} - a_i)) \leq \min\{v(a_{i+1} - a_i) \mid m \geq i < n\}.$$

Ker je $a_{i+1} - a_i = b_i c_i$, je za vsak $i \in \mathbb{N}$ $v(a_{i+1} - a_i) = v(b_i c_i) \geq v(b_0) + 2^m N$ za $m \leq i \leq n$. Torej je $v(a_n - a_m) \geq 2^m N$, iz česar sledi, da je zaporedje $(a_n)_{n\in\mathbb{N}}$ Cauchyjevo, zato ima limito a v K oz., zaradi zaprtosti valuacijskega kolobarja, v $\mathcal{O}$. Ker sta vsota in produkt limit limita oz. produkt vsot, je $f(a) = \lim_{n\to\infty} f(a_n)$ in $f'(a) = \lim_{n\to\infty} f'(a_n) = \lim_{n\to\infty} b_n$, torej je tudi $(b_n)_{n\in\mathbb{N}}$ Cauchyjevo. Ker je

$v(f(a)) = v(\lim_{n\to\infty} f(a_n)) \geq 2^n N$ za vsak $n \in \mathbb{N}$, je $v(f(a)) = \infty$ in zato $f(a) = 0$. Po drugi strani iz $v(b_n) = v(b_0)$ sledi, da je $v(f'(a)) = v(b_0) < v(f(a_0))$, torej je $f'(a) \neq 0$. Ker je

$$v(a_n - a_0) = v(\sum_{i=0}^{n-1}(a_{i+1} - a_i)) \geq \min\{v(a_{i+1} - a_i) \geq v(b_0) + N,$$

je $v(a - a_0) = v((a - a_n) + (a_n - a_0)) \geq v(a_n - a_0) \geq v(b_0) + N$ za dovolj velike n. Torej je $v(a - a_0) > v(b_0) = v(f'(a))$. S tem smo dokazali vse trditve v izreku. □

Naslednja posledica Henselove leme pove, da za vsako enostavno ničlo (torej tako, da je vrednost formalnega odvoda pri njej različna od nič) $\overline{a_0} \in \overline{K}$ polinoma $\overline{f}$, kjer je $f \in \mathcal{O}[x]$ in $\overline{K}$ polje ostankov diskretnega valuacijskega kolobarja, dvignemo do ničle $a \in \mathcal{O}$.

Posledica 2.55 ([4, posledica 1.3.2])**.** *Naj bo K polje z diskretno valuacijo v. Če za polinom $f \in \mathcal{O}[x]$ obstaja tak $\overline{a_0} \in \overline{K}$, da je $\overline{f}(\overline{a_0}) = 0$ in $\overline{f'}(\overline{a_0}) \neq 0$, potem obstaja tak $a \in \mathcal{O}$, da je $f(a) = 0$ in $\overline{a} = \overline{a_0}$.*

Dokaz. Iz dejstva, da je $\overline{a_0}$ enostavna ničla $\overline{f}$, sledi $v(f(a_0)) = \infty$ in $v(f'(a_0)) < \infty$. Torej velja $v(f(a_0)) > 2v(f'(a_0))$ in zato po Henselovi lemi obstaja tak $a \in \mathcal{O}$, da je $f(a) = 0$ in $v(a_0 - a) > v(f'(a_0)) \geq 0$. Zato je $a_0 - a \in \mathcal{M}$ oz. velja $\overline{a} = \overline{a_0}$. □

V osrednjem izreku tega poglavja bomo pokazali, da imajo Henselova polja več med seboj ekvivalentnih definicij. V nadaljevanju naloge, še posebej med dokazovanjem izreka Ax-Kochen-Jeršov, jih bomo uporabljali izmenično. Najprej se prepričajmo, da je polje $(K, \mathcal{O})$ Henselovo natanko tedaj, ko je za vsako končno razsežno razširitev $K' \mid K$ razširitev $\mathcal{O} \subseteq \mathcal{O}'$ enolično določena. V eno smer je ekvivalenca očitna, da se prepričamo še v drugo, pa predpostavimo, da za neko algebraično razširitev polj $K' \setminus K$ obstajata dve različni razširitvi $\mathcal{O}'$ in $\mathcal{O}''$ za $\mathcal{O}$. Potem obstaja $x \in K' \mid K$, algebraičen nad K, ki je vsebovan v denimo $\mathcal{O}'$, ne pa tudi v $\mathcal{O}''$. Potem sta $(K(x), \mathcal{O}' \cap K(x))$ in $(K(x), \mathcal{O}'' \cap K(x))$ dve različni razširitvi $\mathcal{O}$ na $K(x)$. Preden povemo vse ekvivalentne definicije Henselovih polj, pa naredimo nekaj preprostih razmislekov. V 2.52 smo za polje K z valuacijo v definirali w, razširitev v na $K(x)$, za katero je veljalo $w(p) = \min_{0\leq i\leq n} v(a_i)$ za vsak polinom $p \in K[x]$. Če velja $w(p) = 0$, bomo rekli, da je polinom *primitiven*. Očitno je produkt primitivnih polinomov tudi primitiven polinom. Poleg tega lahko vsak polinom p zapišemo kot $p(x) = ap_1(x)$, kjer je $a \in K$ in $p_1 \in K[x]$ primitiven polinom (tu za $a \in K$ velja $v(a) = \min_{0\leq i\leq n} v(a_i)$). Prav tako za $p \in \mathcal{O}[x]$ velja, da če obstaja razcep $p = g_1 \cdots g_n$ na nerazcepne faktorje $g_i \in K[x]$, potem obstajajo $h_1, \ldots, h_n \in \mathcal{O}[x]$, nerazcepni v $K[x]$, da je $p = h_1 \cdots h_n$. Res: naj bo $p = ap_1$ in $g_i = b_i g_{i,1}$ za $1 \leq i \leq n$, kjer so p_1 in $g_{i,1}$ primitivni. Potem je $v(b_1 b_2, \cdots, b_n) = \sum_{i=0}^{n} w(g_i) = w(f) = v(a)$. Ker je $a \in \mathcal{O}$, to velja tudi za $b := b_1 b_2, \cdots, b_n$. Če definiramo $h_1 = bg_{1,1}$ in $h_i = g_{i,1}$ za $2 \leq i \leq n$, dobimo želene h_i. Pred glavnim izrekom si oglejmo še naslednji rezultat.

Lema 2.56 ([4, trditev 3.2.16])**.** *Naj bo $(K, \mathcal{O}) \subseteq (K', \mathcal{O}')$ razširitev polj z valuacijo, kjer je K' algebraično zaprtje polja K. Naj bosta valuaciji, ki pripadata $(K, \mathcal{O})$ in $(K', \mathcal{O}')$, $v : K \to \Gamma \cup \{\infty\}$ oz. $v' : K' \to \Gamma' \cup \{\infty\}$. Predpostavimo še, da je v', zožena na K, enaka v. Potem je za vsak avtomorfizem $\sigma \in Aut(K' \mid K)$ preslikava $v' \circ \sigma$ enolično določena valuacija, ki pripada valuacijskemu kolobarju $\sigma^{-1}(\mathcal{O}')$ in Γ'. Posebej velja : če je $\sigma(\mathcal{O}') = \mathcal{O}'$, potem je $v' \circ \sigma = v'$.*

Dokaz. $v' \circ \sigma : K' \to \Gamma' \cup \{\infty\}$ je preslikava, za katero velja $\sigma^{-1}(\mathcal{O}') = \{x \in K' \mid v' \circ \sigma(x) \geq 0\}$. Njena surjektivnost sledi iz surjektivnosti σ in v', aksiomi polja z valuacijo pa iz dejstva, da je σ homomorfizem. Naj bo $w : K' \to \Gamma' \cup \{\infty\}$ valuacija na K' z valuacijskim kolobarjem $\sigma^{-1}(\mathcal{O}')$, ki je razširitev v. Torej sta $v' \circ \sigma$ in w ekvivalentni valuaciji, zato po 2.13 obstaja tak izomorfizem $\tau : \Gamma \to \Gamma$, ki ohranja urejenost in za katerega velja $\tau \circ w = v' \circ \sigma$. Hočemo videti, da je τ identiteta na Γ'. Ker je σ identiteta na K, w in v', zoženi na K, pa obe enaki v, je τ identiteta na Γ. Ker ima po 2.43 vsak element Γ'/Γ končen red (saj je K' algebraična razširitev K), za vsak $\gamma \in \Gamma'$ obstaja naravno število n, da je $n\gamma \in \Gamma$. Potem je $n\tau(\gamma) = \tau(n\gamma) = n\gamma$ in zato $n(\tau(\gamma) - \gamma) = 0$. Ker je Γ' brez torzije, sledi $\tau(\gamma) = \gamma$. □

Sedaj smo prišli do ekvivalentnih definicij Henselovih polj.

Izrek 2.57 ([4, izrek 4.1.3])**.** *Naj bo $(K, \mathcal{O})$ polje z valuacijo $v : K \to \Gamma \cup \{\infty\}$. Kot ponavadi z $\mathcal{M}$ in $\overline{K}$ označimo pripadajoči maksimalni ideal in polje ostankov. Potem so naslednje trditve ekvivalentne:*

(1) *$(K, \mathcal{O})$ je Henselovo.*
(2) *Za vsak nerazcepen polinom $f \in \mathcal{O}[x]$, za katerega velja $\overline{f} \notin \overline{K}$ ($\overline{f}$ torej ni konstanten polinom) obstaja tak $g \in \mathcal{O}[x]$, da je $\overline{g} \in \overline{K}[x]$ nerazcepen in velja $\overline{f} = \overline{g}^s$ za nek $s \geq 1$.*
(3) *Naj za $f, g, h \in \mathcal{O}[x]$ velja $\overline{f} = \overline{g}\overline{h}$, pri čemer sta $\overline{g}$ in $\overline{h}$ tuja v $\overline{K}(x)$. Potem obstajata $g_1, h_1 \in \mathcal{O}[x]$, da velja $f = g_1 h_1$, $\overline{g_1} = \overline{g}$ in $\overline{h_1} = \overline{h}$, g_1 pa ima isto stopnjo kot $\overline{g}$.*
(4) *Za vsak $f \in \mathcal{O}[x]$ in $a \in \mathcal{O}$, za katera velja $\overline{f}(\overline{a}) = 0$ in $\overline{f'}(\overline{a}) \neq 0$, obstaja $b \in \mathcal{O}$, da je $f(b) = 0$ in $\overline{a} = \overline{b}$.*
(5) *Za vsak $f \in \mathcal{O}[x]$ in $a \in \mathcal{O}$, za katera velja $v(f(a)) > 2v(f'(a))$, obstaja $b \in \mathcal{O}$, za katerega je $f(b) = 0$ in $v(b - a) > v(f'(b))$.*
(6) *Vsak polinom $x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0 \in \mathcal{O}[x]$, kjer je $a_{n-1} \notin \mathcal{M}$ in $a_{n-2}, \ldots, a_0 \in \mathcal{M}$, ima ničlo v K.*
(7) *Vsak polinom $x^n + x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0 \in \mathcal{O}[x]$, kjer so $a_{n-2}, \ldots, a_0 \in \mathcal{M}$, ima ničlo v K.*

Dokaz. (1) $\Rightarrow$ (2) : Naj bo $\mathcal{O}'$ enolična razširitev $\mathcal{O}$ na K', algebraično zaprtje K. Pripadajoči maksimalni ideal in polje ostankov označimo z $\mathcal{M}'$ oz. $\overline{K}'$, pripadajoča valuacija pa naj bo $v' : K' \to \Gamma' \cup \{\infty\}$. Ker je $\mathcal{O}'$ edina razširitev $\mathcal{O}$ na K', za vsak $\sigma \in \mathrm{Aut}(K' \mid K)$ velja $\sigma(\mathcal{O}') = \mathcal{O}'$ in zato tudi $\sigma(\mathcal{M}') = \mathcal{M}'$. Potem je po 2.56 $v' \circ \sigma = v'$.

Zapišimo nerazcepen $f \in \mathcal{O}[x]$ v obliki $f(x) = \Pi_{j=1}^{n}(ax - x_j)$, kjer so $a, x_1, \ldots, x_n \in K'$, a pa n-ti koren vodilnega koeficienta f. Ker je potem $a^n \in \mathcal{O}$ in zato $v'(a^n) = v(a^n) \geq 0$, je tudi $v'(a) \geq 0$, torej je $a \in \mathcal{O}'$. Velja tudi $(-1)^n x_1 \cdots x_n = f(0) \in \mathcal{O} \subseteq \mathcal{O}'$. Iz teorije algebraičnih razširitev polj vemo, da za poljubna $1 \leq i, j \leq n$ obstaja tak $\sigma \in \mathrm{Aut}(K' \mid K)$, da je $\sigma(x_i/a) = x_j/a$. Potem za i, j velja $v'(x_i/a) = v'(\sigma(x_i/a)) = v'(x_j/a)$, iz česar sledi $v'(x_i) = v'(x_j)$. Ker je $x_1 \cdots x_n \in \mathcal{O} \subseteq \mathcal{O}'$, potem je tudi $x_i \in \mathcal{O}'$ za vsak $1 \leq i \leq n$, saj velja $v'(x_i) \geq 0$. Če je nek $x_i \in \mathcal{O}'^{\times}$, to velja za vse x_i, pa tudi za njihov produkt, zato lahko ločimo dva primera. V prvem je $x_i \in \mathcal{M}$ za vse i. Potem je $\overline{f}(x) = (\overline{a}x)^n$ in točka (2) velja. V drugem so vsi $x_i \in \mathcal{O}'^{\times}$ in sledi $\overline{f}(x) = \Pi_{i=1}^{n}(\overline{a}x - \overline{x_j})$, kjer so $\overline{x_j} \neq 0$. Ker po predpostavki $\overline{f}$ ni konstanten polinom, velja $\overline{a} \neq 0$.

Da tudi v tem primeru dokažemo točko (2), moramo pokazati, da so $\overline{x_i}$ enaki. Pa recimo nasprotno in s tem predpostavimo, da je $\overline{f} = \overline{g}\overline{h}$ za neka polinoma

$g, h \in \mathcal{O}[x]$, za katera sta $\overline{g}$ in $\overline{h}$ tuja v $\overline{K}[x]$. Naj bosta $1 \leq i, j \leq n$ taka, da je $\overline{x_i/a}$ ničla $\overline{g}$, $\overline{x_j/a}$ pa ničla $\overline{h}$. Potem je $g(x_i/a) \in \mathcal{M}'$ in $h(x_j/a) \in \mathcal{M}'$. Izberimo tak $\sigma \in \mathrm{Aut}(K' \mid K)$, da je $\sigma(x_i/a) = x_j/a$. Potem je $g(x_j/a) = g(\sigma(x_i/a)) = \sigma(g(x_i/a)) \in \sigma(\mathcal{M}') = \mathcal{M}'$, torej je $\overline{g}(\overline{x_j/a}) = \overline{h}(\overline{x_j/a}) = 0$, kar je v nasprotju s predpostavljeno tujostjo $\overline{g}$ in $\overline{h}$. Torej so vsi x_i res enaki in velja $\overline{f} = (\overline{a}x - \overline{x_1})^n$.

(2) $\Rightarrow$ (3) : Naj bo $f = g_1 \dots g_n$ razcep $f \in \mathcal{O}[x]$ na nerazcepne faktorje, pri čemer lahko, kot smo premislili, predpostavimo, da so tudi $g_i \in \mathcal{O}[x]$. Ker velja (2), za vsak g_i velja bodisi $\overline{g_i} \in \overline{K}$ bodisi obstaja $f_i \in \mathcal{O}[x]$ in $s_i \geq 1$, da je $\overline{g_i} = \overline{f_i}^{s_i}$, $\overline{f_i}$ pa je nerazcepen. Spremenimo vrstni red g_i tako, da bo za $0 \leq l \leq n$ veljalo, da je $\overline{g_i} = \overline{f_i}^{s_i}$, kjer je $\overline{f_i}$ nerazcepen polinom za $i \leq l$ in $\overline{g_i} \in \overline{K}$ za $i > l$. Brez škode za splošnost lahko predpostavimo, da noben f_i nima neničelnih koeficientov v $\mathcal{M}$ (ker se ti v kvocientu ne pojavijo, jih lahko preprosto izbrišemo, saj $\overline{f_i}$ s tem ostane enak). Ker je

$$\Pi_{i=0}^{n} \overline{g_i} = \Pi_{i=0}^{l} \overline{f_i}^{s_i} \cdot \Pi_{i=l+1}^{n} \overline{g_i} = \overline{f} = \overline{g}\overline{h},$$

lahko po morebitnem spreminjanju vrstnega reda f_i zapišemo enakosti

$$\Pi_{i=1}^{k} \overline{f_i}^{s_i} = \overline{ag}, \Pi_{i=k+1}^{l} \overline{f_i}^{s_i} = \overline{bh} \text{ in } \Pi_{i=l+1}^{n} \overline{g_i} = \overline{c},$$

kjer so $a, b, c \in \mathcal{O}^\times$ in velja $ab = c^{-1}$. To velja zato, ker sta $\overline{g}$ in $\overline{h}$ sta tuja. Naj bo

$$g_1 := a^{-1} \Pi_{i=1}^{k} f_i^{s_i} \text{ in } h_1 := (b^{-1} \Pi_{i=k+1}^{l} f_i^{s_i})(c^{-1} \Pi_{i=l+1}^{n} g_i).$$

Ker so $a^{-1}, b^{-1} \in \mathcal{O}^\times$, $\overline{g_i} = \overline{f_i}^{s_i}$ in $\Pi_{i=l+1}^{n} \overline{g_i} = \overline{c}$, velja $\overline{g_1} = \overline{g}$ in $\overline{h_1} = \overline{h}$, pa tudi $\deg g_1 = \deg \overline{g}$, saj so stopnje f_i enake stopnjam $\overline{f_i}$. f_i namreč po predpostavki nimajo neničelnih koeficientov v $\mathcal{M}$. Ker je $abc = 1$, sledi tudi $f = g_1 h_1$.

(3) $\Rightarrow$ (4) : Naj bo $\overline{a} \in \overline{K}$ enostavna ničla $\overline{f}$. Za $g(x) := x - a$ je $\overline{h} := \overline{f/g}$ polinom s koeficienti v $\overline{K}$. Poleg tega je $\overline{h}$ tuj $\overline{g}$, zato po točki (3) obstajata taka $g_1, h_1 \in \mathcal{O}[x]$, da je $f = g_1 h_1$, $\overline{g_1} = \overline{g} = x - \overline{a}$ in $\deg g_1 = \deg \overline{g}$. Zato je g_1 oblike $c(x - b)$ za $c \in \mathcal{O}^\times$ in $b \in \mathcal{O}$. Iz tega takoj sledi, da je $f(b) = g_1(b)h_1(b) = 0$. Ker je vodilni koeficient pri $\overline{g_1}$ enak $\overline{g}$, sledi, da je $\overline{c} = 1$, zato je $\overline{b} = \overline{a}$.

(4) $\Rightarrow$ (5) : Naj bosta f in a kot v predpostavkah (4). Kot smo že storili v dokazu Henselove leme za polna diskretna polja z valuacijo, lahko pokažemo, da velja $f(a - x) = f(a) - f'(a)x + x^2 g(x)$ za nek $g \in \mathcal{O}[x]$. Ker je $2v(f'(a)) < v(f(a))$, sledi $f'(a) \neq 0$. Če zgornjo enakost delimo s $f'(a)^2$ in x zamenjamo z novo spremenljivko $y := x/f'(a)$, dobimo:

$$\frac{f(a - f'(a)y)}{f'(a)^2} = \frac{f(a)}{f'(a)^2} - y + y^2 g(f'(a)y).$$

Naj bo

$$h(y) := g(f'(a)y) \text{ in } f_1(y) := f(a)/f'(a)^2 - y + y^2 h(y).$$

Ker je $a \in \mathcal{O}$ in $f, f' \in \mathcal{O}[x]$, sta tudi $f(a), f'(a) \in \mathcal{O}$, iz česar sledi, da sta h in f_1 vsebovana v $\mathcal{O}[y]$. Ker iz $2v(f'(a)) < v(f(a))$ sledi, da je $\overline{f(a)/f'(a)^2} = 0$, je $\overline{f_1}(y) = y(y\overline{h_1}(y) - 1)$. $\overline{f}$ torej ima ima enostavno ničlo 0 v $\overline{K}$. Iz (4) sledi, da ima f_1 ničlo $a' \in \mathcal{O}$, za katero je $\overline{a'} = 0$ oz. $a' \in \mathcal{M}$. Ker je $f(a - f'(a)y)/f'(a)^2 = f_1(y)$, sledi, da je $b := a - f'(a)a'$ ničla f v $\mathcal{O}$. Ker je $v(a') = v(b - a) - v(f'(a)) > 0$, sledi $v(b - a) > v(f'(a))$.

(5) $\Rightarrow$ (6) : Naj bo $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathcal{O}[x]$, $a_{n-1} \notin \mathcal{M}$, $a_{n-2}, \dots, a_0 \in \mathcal{M}$. Potem je $\overline{f} = x^n + \overline{a_{n-1}}x^{n-1} = x^{n-1}(x + \overline{a_{n-1}})$, torej je $\overline{-a_{n-1}}$ enostavna ničla $\overline{f}$, iz česar sledi $\overline{f}'(\overline{-a_{n-1}}) \neq 0$. Zaradi tega je $v(f(-a_{n-1})) > 0 = v(f'(-a_{n-1})^2)$, zato ima po (5) f ničlo v $\mathcal{O}$.

$\infty = v(f(-a_{n-1})) > v(f'(-a_{n-1}))$, zato ima po (5) f ničlo v $\mathcal{O}$.

(6) $\Rightarrow$ (7) : Očitno.

(7) $\Rightarrow$ (6) : Naj bo $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathcal{O}[x]$, $a_{n-1} \notin \mathcal{M}$, $a_{n-2}, \ldots, a_0 \in \mathcal{M}$. Naj bo $y := x/a_{n-1}$. Potem je

$$g(y) := f(y/a_{n-1})/a_{n-1}^n = y^n + y^{n-1} + a_{n-2}/a_{n-1}^2 y^{n-2} + \cdots + a_0/a_{n-1}^n.$$

Po (7) ima g ničlo $a \in \mathcal{O}$. Zato je $a' := aa_{n-1}$ ničla f.

(6) $\Rightarrow$ (1): Recimo, da $(K, \mathcal{O})$ ni Henselovo. Potem obstaja končno razsežna algebraična razširitev $K' \mid K$, za katero obstaja več različnih razširitvev $\mathcal{O}$ in za katero lahko po 2.47 brez škode za splošnost privzamemo, da je separbilna. Argument za to je enak kot pri dokazu izreka 2.49. Naj bo $\{x_1, \ldots, x_n\}$ baza razširitve K' nad K, $p_1, \ldots, p_n \in K[x]$ pa pripadajoči minimalni polinomi. Če K' dodamo vse ničle p_i za $1 \leq i \leq n$, dobimo končno razsežno Galoisovo razširitev $N \mid K$ z Galoisovo grupo $G := G(N \mid K)$. Ker je $K' \subseteq N$, ima $\mathcal{O}$ več različnih razširitev na N.

Naj bo $\mathcal{O}^*$ neka razširitev $\mathcal{O}$ na N in naj bo $H := \{\sigma \in G \mid \sigma(\mathcal{O}^*) = \mathcal{O}^*\}$. Po predpostavki je H prava podgrupa G, saj, kot smo ugotovili, za dve razširitvi $\mathcal{O}^*$ in $\mathcal{O}^{**}$ valuacije $(K, \mathcal{O})$ na N, obstaja tak $\sigma \in G$, da je $\sigma(\mathcal{O}^*) = \mathcal{O}^{**}$ Zato je L, polje fiksnih točk za H, prava razširitev K. Naj bodo $\mathcal{O}^* = \mathcal{O}_1, \ldots, \mathcal{O}_n$ vse razširitve $\mathcal{O}$ v N. Končno mnogo jih je, ker je $[N : K] < \infty$, vemo pa, da obstajata vsaj dve. Naj bo za vsak $1 \leq i \leq n$ $\mathcal{O}_i' = \mathcal{O}_i \cap L$, $\mathcal{M}_i'$ pa pripadajoči maksimalni ideal.

Naj bo $R := \cap_{i=1}^m \mathcal{O}_m'$. Po 2.46 so različni $\mathcal{O}_i'$ medsebojno neprimerljivi glede na vsebovanost, zato lahko po 2.44 sklepamo, da so $P_i := R \cap \mathcal{M}_i'$ vsi maksimalni ideali za R in velja $R_{P_i} = \mathcal{O}_i'$. Prepričajmo se, da je $P_i \neq P_1$ za vsak $i \geq 2$. V nasprotnem primeru po lemi 2.44 namreč velja $\mathcal{O}_i \cap L = \mathcal{O}_i' = R_{P_i} = R_{P_1} = \mathcal{O}_1' = \mathcal{O}_1 \cap L$. Potem obstaja tak $\sigma \in G(N \mid L) = H$, da je $\sigma(\mathcal{O}_i') = \mathcal{O}_1' = \mathcal{O}^* \cap L$. Po definiciji H sledi, da je $\mathcal{O}_i = \mathcal{O}^*$, kar pa po predpostavki ne velja. Po 2.44 zato obstaja tak $b \in R$, da je $b - 1 \in \mathcal{M}_1'$ in $b \in \mathcal{M}_i'$ za $i \geq 2$. Naj bodo $b_1, b_2, \ldots, b_n \in N$ vsi različni elementi oblike $\sigma(b)$ za $\sigma \in G(N \mid K)$. Posebej naj bo $b_1 = b$. Naj bo $p(x) = x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ minimalni polinom za b v K. p je nerazcepen v K. Ker je $p(x) = \Pi_{i=1}^n (x - b_i)$ v N, velja $a_{n-1} = (-1)^{n-1}(b_1 + \ldots + b_n) \in K$ in $a_j = (-1)^j \sum_{1 \leq i_1 < \ldots < i_{n-j} \leq n} b_{i_1} \cdots b_{i_{n-j}} \in K$. Poleg tega očitno velja, da so vsi a_i v R, torej v $\mathcal{O}_i'$ za vsak i. Ker je $\mathcal{O}_i' \cap K = \mathcal{O}$, sledi, da so $a_i \in \mathcal{O}$.

Pokažimo, da za vsak $i \geq 2$ velja $b_i \in \mathcal{M}_1'$. Ker je $b_i \neq b_1$ in $b_1 \in L$, obstaja tak $\sigma \in G \backslash H$, da je $\sigma(b_1) = b_i$. Potem je $\sigma^{-1} \in G \backslash H$, zato je $\sigma^{-1}(\mathcal{O}_1) = \mathcal{O}_j$ za nek $j \geq 2$ in posledično $\sigma^{-1}(\mathcal{M}_1') = \mathcal{M}_j'$. Ker je po predpostavki $b = b_1 \in \mathcal{M}_j' = \sigma^{-1}(\mathcal{M}_1')$, je $b_i = \sigma(b) \in \mathcal{M}_1'$.

Torej velja $b_1 \notin \mathcal{M}_1'$ in $b_i \in \mathcal{M}_1'$ za $i \geq 2$. Iz tega sledi, da je $a_{n-1} \notin \mathcal{M}_1'$ in $a_1 \in \mathcal{M}_1'$ za $i \neq n-1$. Torej je $a_{n-1} \in \mathcal{O}^\times$ in $a_i \in \mathcal{M}$ za $i \neq n-1$. Po (6) sledi, da ima p ničlo v $\mathcal{O} \subseteq K$, s čimer smo prišli do protislovja. □

Takojšnja posledica tega izreka je, da je vsako polno polje z diskretno valuacijo Henselovo. Naslednja izreka, ki ju bomo navedli brez dokaza, nam bosta podala nekaj pomembnih lastnosti razširitev polj z valuacijo na Henselova polja.

Izrek 2.58 ([9, izrek 4.3.3])**.** *Za vsako polje z valuacijo $(K, \mathcal{O})$ obstaja razširitev $(K, \mathcal{O}) \subseteq (K_1, \mathcal{O}_1)$, za katero velja:*

(1) *$(K_1, \mathcal{O}_1)$je Henselovo polje z valuacijo,*
(2) *Vsako Henselovo polje $(K_2, \mathcal{O}_2)$, ki je razširitev $(K, \mathcal{O})$, je tudi razširitev $(K_1, \mathcal{O}_1)$.*

Polju $(K_1, \mathcal{O}_1)$ z lastnostmi kot v izreku pravimo *henselizacija* polja z valuacijo $(K, \mathcal{O})$. Za henselizacijo velja naslednje:

Izrek 2.59 ([9, izrek 4.3.4])**.** *Henselizacija polja z valuacijo $(K, \mathcal{O}) \subseteq (K_1, \mathcal{O}_1)$ je separabilna in neposredna razširitev $(K, \mathcal{O})$.*

Za polje z valuacijo $(K, \mathcal{O})$ pravimo, da je *končno razvejano*, če je bodisi karakteristika polja ostankov $\overline{K}$ enaka nič bodisi je med 0 in $v(\mathrm{char}(\overline{K}))$ samo končno mnogo vrednosti valuacijske grupe Γ. V obeh primerih velja za vsako naravno število n, da je med 0 in $v(n)$ kvečjemu končno mnogo elementov Γ. Če je karakteristika $\overline{K}$ nič, je $\mathbb{Q} \subseteq \overline{K}$. Ker je $\mathcal{M} \cap \mathbb{Q} = \{0\} \subseteq \mathcal{O}$, je namreč $v(n) = 0$ za vsako naravno število n. Prespostavimo sedaj, da je $\mathrm{char}(\overline{K}) = p$. Če je $v(n) \leq v(\mathrm{char}(\overline{K}))$, je med 0 in $v(n)$ očitno končno mnogo vrednosti. V nasprotnem primeru pa vzamemo tako naravno število k, da je $v(n) \leq v(\mathrm{char}(\overline{K})^k) = kv(\mathrm{char}(\overline{K}))$. Ker je za vsak $0 \leq i < k$ med $iv(\mathrm{char}(\overline{K}))$ in $(i+1)v(\mathrm{char}(\overline{K}))$ enako mnogo vrednosti kot med 0 in $v(\mathrm{char}(\overline{K}))$, je tudi med 0 in $v(\mathrm{char}(\overline{K})^k)$ le končno mnogo vrednosti. Iz povedanega sledi, da je karakteristika končno razvejanega polja z valuacijo vedno nič. Henselizacije končno razvejanih polj z valuacijo imajo posebno lastnost.

Izrek 2.60 ([9, izrek 4.3.5])**.** *Naj bo $(K, \mathcal{O})$ končno razvejano polje z valuacijo. Potem je henselizacija $(K, \mathcal{O})$ maksimalna neposredna algebraična razširitev.*

Dokaz. Naj bo $(K, \mathcal{O}) \subseteq (K_1, \mathcal{O}_1)$ henselizacija, ki je po 2.59 neposredna razširitev. Pa recimo, da obstaja poljubna prava neposredna algebraična razširitev, ki jo označimo z $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$. Lahko se omejimo na primer $K_2 = K_1(\alpha)$ in z g označimo minimalni polinom (stopnje vsaj 2) za α v K_1. Naj bo $K_3 \mid K_2$ razpadni obseg za g. Upoštevajoč dejstvo, da je karakteristika K_1 enaka nič, sklepamo, da je $K_3 \mid K_1$ Galoisova razširitev. Pripadajoča Galoisova grupa $G = G(K_3 \mid K_1)$ je končna. Naj bo $n := |G|$. Vsota $a := \frac{1}{n} \sum_{\sigma \in G} \sigma(\alpha)$ je vsebovana v K_1. Res: če je minimalni polinom za $g \in K[x]$ stopnje n, je $(-1)^{n-1} \sum_{\sigma \in G} \sigma(a)$ njegov koeficient pri x^{n-1}.

Naj bo v valuacija, ki pripada $(K_3, \mathcal{O}_3)$. Pokazali bomo, da obstaja $b \in K_1$, za katerega velja

$$v(\alpha - a) + v(n) < v(\alpha - b). \tag{1}$$

Ker je $(K_2, \mathcal{O}_2)$ neposredna razširitev $(K_1, \mathcal{O}_1)$, torej velja $\Gamma_1 = \Gamma_2$ in$\overline{K}_1 = \overline{K_2}$, obstaja tak $c \in \mathcal{O}_1$, da je $v(\alpha - a) = v(c)$, zato je $(\alpha - a)c^{-1}$ obrnljiv v $\mathcal{O}_2$. Potem lahko najdemo tudi $d \in \mathcal{O}_1$, da je $\overline{(\alpha - a)c^{-1}} = \overline{d}$. Velja $v((\alpha - a)c^{-1} - d) > 0$. Če definiramo $b_1 := a + cd \in K_1$, potem velja $v(\alpha - a) = v(c) < v(c(\frac{\alpha - a}{c} - d)) = v(\alpha - a - cd) = v(\alpha - b_1)$. Sedaj ponovimo zgornji postopek, kjer namesto a vzamemo b_1. Tako dobimo $b_2 \in K_1$, za katerega velja $v(\alpha - a) < v(\alpha - b_1) < v(\alpha - b_2)$.Če ta postopek ponovimo na b_2 in tako naprej, slej ko prej pridemo do $b = b_i$ da velja (1), saj je med $v(\alpha - a)$ in $v(\alpha - a) + v(n)$ le končno mnogo vrednosti Γ_1.

Zaradi enoličnosti razširitev $\mathcal{O}_i$ polja $\mathcal{O}$ na K_i za $i = 1, 2$ velja $\sigma(\mathcal{O}_i) = \mathcal{O}_i$ za vsak $\sigma \in G$. Ker iz tega po 2.56 sledi $v(\sigma(a)) = v(a)$ za vsak $a \in K_2 = K_1(\alpha)$, je za vsak $\sigma \in G$ $v(\alpha - b) = v(\sigma(\alpha - b)) = v(\sigma(\alpha) - b)$. Potem je $v(\alpha - a) + v(n) < v(\alpha - b) \leq v(\sum_{\sigma \in G}(\sigma(\alpha) - b))$. Ker po definiciji a velja $\sum_{\sigma \in G}(\sigma(\alpha) - b) = n(a - b)$, je $v(\alpha - a) + v(n) < v(n(a - b))$ in zato velja $v(\alpha - a) < v(a - b)$. Potem je $v(\alpha - a) < \min\{v(a - b), v(\alpha - b)\} \leq v((\alpha - b) - (a - b)) = v(\alpha - a)$, s čimer smo prišli do protislovja.

$(K_1, \mathcal{O}_1)$ je torej res maksimalna neposredna algebraična razširitev $(K, \mathcal{O})$. $\square$

3. Izomorfnost in elementarna ekvivalenca modelov

Na začetku razdelka bomo definirali osnovne pojme teorije modelov, kot so jezik, struktura, formula, stavek in model. Potem bomo za primere definiranih pojmov predstavili jezik in teorijo urejenih abelovih grup in valuacijskih polj, ki se jih bomo poslužili predvsem v naslednjem poglavju.

Vsaki družini struktur z določenimi lastnostmi, kot so grupe ali polja, pripada jezik in množica aksiomov, napisanih v tem jeziku, ki jih vse tovrstne strukture izpolnjujejo. Ta jezik je sestavljen iz:

(1) logičnih simbolov in kvantifikatorjev $\neg, \vee, \wedge, \rightarrow, \leftrightarrow \exists, \forall$ in $\doteq$,
(2) številno mnogo spremenljivk v_n za $n \in \mathbb{N}_0$,
(3) funkcijskih simbolov f,
(4) relacijskih simbolov R,
(5) konstantnih simbolov c ter
(6) oklepajev in veznikov, ki bodo služili za lažjo berljivost.

Vsakemu funkcijskemu in relacijskemu simbolu bo pripadala tudi njegova kratnost. Z $\mathcal{F}, \mathcal{R}$ in $\mathcal{K}$ bomo označili množice vseh funkcijskih, relacijskih in konstantnih simbolov jezika, z Vbl pa množico vseh spremenljivk. Jezik $\mathcal{L}$ bo natanko določen z množicami funkcijskih, relacijskih in konstantnih simbolov skupaj z njihovimi kratnostmi, zato bomo za večjo jasnost jezik označili z $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \mathcal{K})$.

S pomočjo rekurzivne definicije definiramo posebni kategoriji nizov *izrazov* jezika $\mathcal{L}$, ki jih bomo imenovali tudi $\mathcal{L}$-izrazi:

(1) Vsaka spremenljivka v_n in vsaka konstanta $c \in \mathcal{K}$ je izraz.
(2) Če so $t_1, \ldots, t_n$ izrazi in $f \in \mathcal{F}$ funkcija kratnosti $n \in \mathcal{N}$, je tudi $f(t_1, \ldots, t_n)$ izraz.

S pomočjo rekurzivne definicije definiramo tudi *formule* jezika $\mathcal{L}$ oz. $\mathcal{L}$-formule:

(1) Za vsaka $\mathcal{L}$-izraza t_1 in t_2 je izraz $t_1 \doteq t_2$ formula.
(2) Če je $R \in \mathcal{R}$ relacijski simbol kratnosti n, je za vse $\mathcal{L}$-izraze $t_1, \ldots, t_n$ izraz $R(t_1, \ldots, t_n)$ formula.
(3) Če sta Φ_1 in Φ_2 poljubni $\mathcal{L}$-formuli, potem so tudi $\neg\Phi_1$, $\Phi_1 \vee \Phi_2$, $\Phi_1 \wedge \Phi_2$, $\Phi_1 \rightarrow \Phi_2$ in $\Phi_1 \leftrightarrow \Phi_2$ $\mathcal{L}$-formule.
(4) Če je v spremenljivka in Φ formula, sta tudi $\forall v\Phi$ in $\exists v\Phi$ formuli.

V primeru formul $\forall v\Phi$ in $\exists v\Phi$ pravimo, da so vse pojavitve spremenljivke v v Φ *vezane* oz. *v obsegu kvantifikatorja* $\forall$ oz. $\exists$. Če spremenljivka v formuli Φ ni zajeta v nobenem kvantifikatorju, pravimo, da je *prosta spremenljivka* formule Φ. Formuli, ki nima prostih spremenljivk, pravimo *stavek* ali, natančneje, *$\mathcal{L}$-stavek*.

Sedaj lahko definiramo strukture in modele. *$\mathcal{L}$-struktura U* je množica, pri kateri za vsak funkcijski simbol $f \in \mathcal{F}$ kratnosti $n \in \mathbb{N}$ obstaja funkcija $f^U : D \rightarrow U$ z domeno $D \subseteq U^n$, za vsak relacijski simbol $R \in \mathcal{R}$ kratnosti $n \in \mathbb{N}$ obstaja relacija $R^U \subseteq U^n$ in za vsak konstantni simbol $c \in \mathcal{K}$ obstaja $c^U \in U$, ki mu pravimo konstanta. Funkciji $h : \text{Vbl} \rightarrow U$ pravimo *evaluacija* oz. *interpretacija spremenljivk* v U. Če je h interpretacija, x spremenljivka in $a \in U$, potem lahko definiramo interpretacijo $h\binom{x}{a} : \text{Vbl} \rightarrow U$ s predpisom

$$h\binom{x}{a}(v) := \begin{cases} h(v) & ; v \neq x \\ a & ; v = x, \end{cases}$$

ki se od h razlikuje kvečjemu v vrednosti natanko določene spremenljivke x. Naj bo U neka $\mathcal{L}$-struktura in $h : \mathrm{Vbl} \to U$ interpretacija. Najprej bomo z rekurzijo definirali vrednosti $\mathcal{L}$-izraza t v U pod h, ki ga bomo označili s $t^U[h]$:

(1) za konstantni simbol $c \in \mathcal{K}$ je $c^U[h] = c^U$,
(2) za spremenjivko v je $v^U[h] = h(v)$,
(3) za izraze $t_1, \ldots, t_n$ in funkcijski simbol $f \in \mathcal{F}$ kratnosti n je $f(t_1, \ldots, t_n)^U[h] = f^U(t_1[h], \ldots, t_n[h])$.

Z rekurzijo bomo definirali tudi pomen trditve, da je $\mathcal{L}$-formula Φ *izpolnjena v U pod interpretacijo h*, kar bomo označili z $U \models \Phi[h]$ (in v nasprotnem primeru uporabili oznako $U \not\models \Phi[h]$):

(1) $U \models t_1 \doteq t_2$ velja natanko tedaj, ko je $t_1^U[h] = t_2^U[h]$.
(2) Če je $R \in \mathcal{R}$ relacijski simbol kratnosti n, potem je $U \models R(t_1, \ldots, t_n)$ natanko tedaj, ko je $(t_1^U[h], \ldots, t_n^U[h]) \in R^U$, ali, krajše, $R^U(t_1^U[h], \ldots, t_n^U[h])$.
(3) $U \models \neg\Phi[h]$ velja natanko tedaj, ko velja $U \not\models \Phi[h]$.
(4) $U \models \Phi_1 \vee \Phi_2[h]$ velja natanko tedaj, ko velja najmanj ena od trditev $U \models \Phi_1[h]$ in $U \models \Phi_2[h]$.
(5) $U \models \Phi_1 \to \Phi_2[h]$ velja natanko tedaj, ko velja vsaj ena od trditev $U \not\models \Phi_1[h]$ in $U \models \Phi_2[h]$.
(6) $U \models \Phi_1 \leftrightarrow \Phi_2[h]$ velja natanko tedaj, ko velja $U \models \Phi_1 \to \Phi_2[h]$ in $U \models \Phi_2 \to \Phi_1[h]$.
(7) Če je x spremenljivka, potem je $U \models \forall x\Phi[h]$ natanko tedaj, ko je $U \models \Phi[h\binom{x}{a}]$ za vsak $a \in U$.
(8) Če je x spremenljivka, potem je $U \models \exists x\Phi[h]$ natanko tedaj, ko obstaja najmanj en $a \in U$, da velja $U \models \Phi[h\binom{x}{a}]$.

Formulam oblike (1) in (2) bomo rekli tudi *atomarne formule* oz., če bodo brez prostih spremenljivk, *atomarni stavki*. Pri osnovah logike smo se naučili izražati logične veznike in kvantifikatorje med seboj ter pokazali, da je vsaka izjava ekvivalentna izjavi, v kateri nastopajo $\neg$, $\wedge$ in $\forall$, ne pa tudi drugi vezniki in kvantifikatorji. Na popolnoma analogen način kot tam lahko to pokažemo tudi v tem primeru, zato bomo od tega trenutka naprej privzeli, da za vsako $\mathcal{L}$-strukturo U in vsako interpretacijo h ter za vsako $\mathcal{L}$-formulo Φ obstaja taka $\mathcal{L}$-formula Φ', v kateri izmed vseh veznikov in kvantifikatorjev nastopajo le $\neg$, $\wedge$ in $\forall$, da velja $U \models \Phi[h]$ če in samo če velja $U \models \Phi'[h]$. Povedano drugače, da velja $U \models \Phi \leftrightarrow \Phi'[h]$. Zato bomo, ko bomo dokazovali veljavnost neke trditve za vse $\mathcal{L}$-formule Φ z indukcijo po kompleksnosti formule Φ pri indukcijskem koraku obravnavali samo primere $\Phi = \neg\Psi$, $\Phi = \Psi_1 \wedge \Psi_2$ in $\Phi = \forall v\Psi$, kjer bo trditev za Ψ, Ψ_1 in Ψ_2 veljala po predpostavki.

Če je formula Φ stavek, torej nima nobene proste spremenljivke, potem je njena izpoljenost v U neodvisna od izbrane interpretacije spremenljivk. To je očitno res, če je Φ stavek brez kvantifikatorjev, saj v njem spremenljivk sploh ni. Pokažimo, da to velja tudi za kompleksnejše formule. Predpostavimo, da je Φ oblike $\forall x\Psi$, kjer je x edina prosta spremenljivka Ψ. Za poljuben $a \in U$ s Ψ_a označimo formulo Ψ, v kateri spremenljivko x nadomestimo s konstanto a. Ker je bil x edina prosta spremenljivka Ψ, je Ψ_a stavek, ki je manj kompleksen od Φ. Po indukcijski predpostavki je zato izpolnjenost Ψ_a v U neodvisna od interpretacije. Če za neko interpretacijo velja $U \models \forall x\Psi[h]$, to pomeni, da je $U \models \Psi[h\binom{x}{a}]$ za vsak $a \in U$. To pomeni, da velja $U \models \Psi_a[h]$ za vsak $a \in U$ in ker je veljavnost stavka Ψ_a v U neodvisna od izbirane interpretacije, velja $U \models \Psi_a[h']$ za vsak $a \in U$ in vsako interpretacijo h'.

Sledi, da velja $U \models \forall x \Psi[h'\binom{x}{a}]$ za vsak $a \in U$ in vsako interpretacijo h', torej velja $U \models \forall x \Psi[h']$ za vsak h'. Pokazali smo, da je veljavnost stavka Φ oblike $\forall x \Psi$ neodvisna od interpretacije spremenljivk. Veljavnost vsakega stavka v $\mathcal{L}$-strukturi U je torej res neodvisna od izbrane interpretacije spremenljivk, zato v primeru, ko je Φ stavek, pišemo tudi $U \models \Phi$ oz. $U \not\models \Phi$. Zdaj lahko končno povemo, kaj je model.

Definicija 3.1. Naj bo Σ množica stavkov v jeziku $\mathcal{L}$. Pravimo, da je $\mathcal{L}$-struktura U *model* množice Σ, če za vsak $\Phi \in \Sigma$ velja $U \models \Phi$.

Primer 3.2. Naj bo $\mathcal{A}$ jezik z binarnim funkcijskim simbolom $+$, enojnim funkcijskim simbolom $-$, binarnim relacijskim simbolom $\leq$ in konstanto 0. Označimo ga z $\mathcal{A} = (+, -, \leq, 0)$. Vidimo, da so vse urejene abelove grupe $\mathcal{A}$-strukture, pri čemer je očitno, kako interpretiramo zgornje simbole. Če želimo množico $\mathcal{A}$-struktur omejiti na urejene abelove grupe, pa moramo zapisati še aksiome urejenih abelovih grup. Ti aksiomi bodo $\mathcal{A}$-stavki, katerih model bodo urejene abelove grupe. Najprej zapišimo aksiome abelovih grup:

(1) $\forall x, y, z : x + (y + z) = (x + y) + z$,
(2) $\forall x : x + 0 = 0 + x = 0$,
(3) $\forall x : x + (-x) = 0$,
(4) $\forall x \exists y : -x = y$,
(5) $\forall x, y : x + y = y + x$.

Sedaj zapišimo še aksiome linearne urejetnosti:

(1) $\forall x : x \leq x$,
(2) $\forall x, y : x \leq y \wedge y \leq x \rightarrow x = y$,
(3) $\forall x, y, z : x \leq y \wedge y \leq z \rightarrow x \leq z$,
(4) $\forall x, y : x \leq y \vee y \leq x$,
in monotonosti za seštevanje:
(5) $\forall x, y, z : x \leq y \rightarrow x + z \leq y + z$.

Vsi modeli zgornje množice stavkov so urejene abelove grupe. ♢

Primer 3.3. Sedaj bomo določili tudi jezik valuacijskih polj. Kot smo pokazali z izrekom 2.12, je vsaka valuacija na polju in pripadajoča abelova grupa do izomorfizma natanko določena z valuacijskim kolobarjem. Zato bomo namesto valuacije kot preslikave definirali valuacijski kolobar polja kot enomestno relacijo V. Jezik valuacijskih polj $\mathcal{K}$ bo tako sestavljen iz binarnih funkcijskih simbolov $+$ in $\cdot$, enojnih funkcijskih simbolov $-$ in $^{-1}$, konstantnih simbolov 0 in 1 ter enomestnega relacijskega simbola V. Ker je polje abelova grupa za seštevanje, veljajo prvi štirje aksiomi iz prejšnjega primera, poleg tega pa še dodatni aksiomi za polja:

(1) $\forall x, y, z : (x \cdot y) \cdot z = x \cdot (y \cdot z)$,
(2) $\forall x, y : x \cdot 1 = 1 \cdot x = 1$,
(3) $\forall x : x = 0 \vee x \cdot x^{-1} = 1$,
(4) $\forall x : x \neq 0 \rightarrow (\exists y : x^{-1} = y)$,
(5) $\forall x, y, z : x \cdot (y + z) = x \cdot y + x \cdot z \wedge (x + y) \cdot z = x \cdot z + y \cdot z$.
(6) $\forall x, y : x \cdot y = y \cdot x$.

S spodnjimi aksiomi bomo zagotovili, da bo za vsako polje z valuacijo K množica $V^K \subseteq K$ valuacijski kolobar.

(1) $V(0) \wedge V(1)$,
(2) $\forall x : V(x) \vee V(x^{-1})$,

(3) $\forall x, y : V(x) \wedge V(y) \to V(x+y) \wedge V(x \cdot y)$.

Vsaka $\mathcal{K}$-struktura, ki izpolnjuje zgornje aksiome, je polje z valuacijo. $\diamondsuit$

Vsem urejenim abelovim grupam je skupno, da izpolnjujejo aksiome iz primera 3.2, vendar to niso edini stavki, ki veljajo zanje, saj med drugim za vse (urejene) abelove grupe velja pravilo krajšanja $\forall x, y, z : x + z = y + z \to x = y$. Po drugi strani pa obstajajo trditve, ki veljajo zgolj za nekatere primere urejenih abelovih grup, kot npr. trditev $\forall x, y : x \leq y \wedge x \neq y \to \exists z : x \leq z \wedge z \leq y \wedge z \neq x \wedge z \neq y$, ki velja v $\mathbb{R}$, ne pa tudi v $\mathbb{Z}$. Stavki, ki veljajo v vseh urejenih abelovih grupah, so formalno zapisane trditve, ki jih lahko v končno mnogo korakih dokažemo iz aksiomov za urejene abelove grupe. To dokazovanje lahko strogo formaliziramo in v celoti zapišemo v zgoraj definiranem jeziku urejenih abelovih grup $\mathcal{A}$.

Mi se bomo v nalogi bolj posvetili modelom in se v formalne dokaze, ki so med drugim končna zaporedja stavkov, ne bomo spuščali. Omenili bomo, da sta najbolj razširjena sistema dokazovana Gentzenov in Hilbertov, ki sta podrobneje predstavljena v [9] ali [12]. Pravimo, je množica stavkov Σ *konsistentna* natanko tedaj, ko ne obstaja takšen stavek Φ, da lahko iz stavkov v Σ dokažemo Φ in $\neg\Phi$ hkrati. Brez dokaza bomo navedli tudi Gödelov izrek o popolnosti, ki ima za posledico, da za poljubno konsistentno množico $\mathcal{L}$-stavkov Σ velja, da je vsak stavek izpolnjen v vsakem modelu Σ natanko tedaj, ko ga lahko iz teh aksiomov formalno dokažemo. Za vsako konkretno $\mathcal{L}$-strukturo je namreč jasno, da za vsak stavek Φ velja bodisi $U \models \Phi$ bodisi $U \models \neg\Phi$. Množico stavkov, ki veljajo v U, imenujemo *teorija* U in jo označimo s $\mathrm{Th}(U)$.

Izrek 3.4 ([9, posledica 1.5.5])**.** *(Gödel) Množica $\mathcal{L}$-stavkov Σ je konsistentna natanko tedaj, ko ima model.*

Iz Gödelovega izreka sledi za nas pomembna posledica o kompaktnosti vsake množice stavkov.

Izrek 3.5 ([9, posledica 1.5.5])**.** *Množica $\mathcal{L}$ stavkov ima model natanko tedaj, ko ima model vsaka njena končna podmnožica stavkov.*

Dokaz. Ker je implikacija iz leve očitna, moramo pokazati le implikacijo iz desne. Predpostavimo torej, da ima vsaka končna podmnožica Σ model, torej je po 3.4 konsistentna. Pa recimo, da Σ nima modela, torej je, spet po 3.4, nekonsistentna. Potem obstaja taka trditev Φ, da lahko iz stavkov Σ dokažemo tako Φ kot tudi $\neg\Phi$. Ker so dokazi končna zaporedja trditev, obstaja končna podmnožica $\Sigma' \subseteq \Sigma$, ki je nekonsistentna. Prišli smo do protislovja. $\square$

3.1. **Izomorfnost, elementarna ekvivalentnost, podstrukture.** V tem razdelku bomo med seboj primerjali različne $\mathcal{L}$-strukture. Najprej bomo definirali homomorfizem dveh $\mathcal{L}$-struktur.

Definicija 3.6. Preslikava $\tau : U \to U'$ je *homomorfizem* $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \mathcal{K})$-struktur U in U', če velja:

(1) $\tau(c^U) = c^{U'}$ za vsak $c \in \mathcal{K}$,
(2) $\tau(f^U(a_1, \ldots, a_n)) = f^{U'}(\tau(a_1), \ldots, \tau(a_n))$ za vsak $f \in \mathcal{F}$ kratnosti n in $a_1, \ldots, a_n \in U$, ter
(3) za vsak $R \in \mathcal{R}$ kratnosti n velja implikacija: če je $R^U(a_1, \ldots, a_n)$, potem sledi $R^{U'}(\tau(a_1), \ldots, \tau(a_n))$ za vse $a_1, \ldots, a_n \in U$.

Injektivnemu homomorfizmu pravimo *vložitev*. Če za homomorfizem τ obstaja tak homomorfizem $\tau' : U' \to U$, da je $\tau' \circ \tau = id_U$ in $\tau \circ \tau' = id_{U'}$, potem je τ *izomorfizem*. Vložitev $\mathcal{L}$-struktur je izomorfizem med prasliko in sliko vložitve.

Jasno je, da je vsak izomorfizem tudi bijekcija. Če med $\mathcal{L}$-strukturama U in U' obstaja izomorfizem, pravimo, da sta *izomorfni*. To označimo z $U \cong U'$. Sedaj bomo formalizirali zamenljivost ene izomorfne strukture z drugo, ki jo pogosto implicitno uporabljamo v matematiki.

Definicija 3.7. Naj bo $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \mathcal{K})$ jezik. $\mathcal{L}$-strukturi U in U' sta *elementarno ekvivalentni*, če za vsak $\mathcal{L}$-stavek Φ velja $U \models \Phi$ natanko tedaj, ko velja $U' \models \Phi$. V tem primeru pišemo $U \equiv U'$.

Trditev 3.8 ([9, izrek 2.2.1])**.** *Naj bo $\tau : U \to U'$ izomorfizem $\mathcal{L}$-struktur. Potem za vsako interpretacijo $h : Vbl \to U$ velja:*

(1) $\tau(t^U[h]) = t^{U'}[\tau \circ h]$ *za vsak $\mathcal{L}$-izraz t,*
(2) *za vsako $\mathcal{L}$-formulo Φ velja $U \models \Phi[h]$ natanko tedaj, ko je $U' \models \Phi[\tau \circ h]$.*

Dokaz. Obe točki bomo dokazali z indukcijo glede na komplelsnost izraza oziroma formule. Za krajši zapis definirajmo interpretacijo $h' := \tau \circ h$. Pri dokazu točke (1) najprej predpostavimo, da je $t = c \in \mathcal{K}$. Potem je (neodvisno od interpretacije h) $t^{U'} = c^{U'} = \tau(c^U) = \tau(t^U)$ po definiciji izomorfizma. Če je t spremenljivka v, je $t^{U'}[h'] = h'(v) = \tau(h(v)) = \tau(t^U[h])$. Če je $f \in \mathcal{F}$ kratnosti n in $t_1, \ldots, t_n$ izrazi, je $t^{U'}[h'] = f^{U'}(t_1^{U'}[h'], \ldots, t_n^{U'}[h']) = f^{U'}(\tau(t_1^U[h]), \ldots, \tau(t_n^U[h])) = \tau(f^U(t_1^U[h], \ldots, t_n^U[h])) = t^U[h]$ po definiciji izomorfizma in indukcijski predpostavki.

Za dokaz točke (2) pa začnemo pri atomarnih formulah:

$$\begin{aligned} U \models t_1 \doteq t_2[h] &\Leftrightarrow t_1^U[h] = t_2^U[h] \Leftrightarrow \tau(t_1^U[h]) = \tau(t_2^U[h]) \\ &\Leftrightarrow t_1^{U'}[h'] = t_2^{U'}[h'] \Leftrightarrow U' \models t_1 \doteq t_2[h']. \end{aligned}$$

Tu uporabimo že dokazano točko (1) in dejstvo, da je τ injektivna. Za n-mestni relacijski simbol $R \in \mathcal{R}$ je

$$\begin{aligned} U \models R(t_1, \ldots, t_n)[h] &\Leftrightarrow R^U(t_1[h], \ldots, t_n[h]) \Leftrightarrow R^{U'}(\tau(t_1[h]), \ldots, \tau(t_n[h])) \\ &\Leftrightarrow R^{U'}(t_1^{U'}[h'], \ldots, t_n^{U'}[h']) \Leftrightarrow U' \models R(t_1, \ldots, t_n)[h']. \end{aligned}$$

Indukcijska koraka, pri katerih je Φ oblike $\neg\Psi$ ali $\Psi_1 \wedge \Psi_2$, kjer trditev velja za formule Ψ, Ψ_1 in Ψ_2, je zelo enostavna in jo bomo izpustili. V primeru, ko je $\Phi = \forall x \Psi$ za neko spremenljivko x, pa sklepamo tako: $U \models \forall x \Phi$ velja natanko tedaj, ko je $U \models \Psi[h\binom{x}{a}]$ za vsak $a \in U$, kar se po indukcijski predpostavki zgodi natanko tedaj, ko je $U' \models \Psi[\tau(h\binom{x}{a})]$za vsak $a \in U$. Ker je, kot ni težko videti, $\tau(h\binom{x}{a}) = \tau(h)\binom{x}{\tau(a)} = h'\binom{x}{\tau(a)}$ in je τ bijekcija, to velja natanko tedaj, ko je $U' \models \Psi[h'\binom{x}{a'}]$ za vsak $a' \in U'$, oz. ko velja $U' \models \Phi[h']$. S tem smo pokazali trditev. □

Če se spomnimo, da je vsak stavek kot formula brez prostih spremenljivk neodvisen od interpretacije le-teh, potem iz trditve takoj dobimo spodnjo posledico.

Posledica 3.9. *Če sta $\mathcal{L}$-strukturi U in U' izomorfni, potem sta elementarno ekvivalentni.*

Kot se izkaže, obratno v splošnem ne velja, saj po izreku Löwenheima in Skolema navzgor, ki ga bomo navedli spodaj, za vsako neskončno $\mathcal{L}$-strukturo U in vsako kardinalno število κ, večje ali enako $|U|$, obstaja $\mathcal{L}$-struktura U' kardinalnosti

κ, za katero velja $U \equiv U'$. Sedaj lahko definiramo podstrukture in elementarne podstrukture.

Definicija 3.10. Naj bo U $\mathcal{L}$-struktura in $U' \subseteq U$. Pravimo, da je U' *podstruktura* U, če vsebuje c^U za vsak $c \in K$ in če je zaprta za funkcije f^U oz. velja da je $f^U(x_1, \ldots, x_n) \in U'$ za vse $x_i \in U'$ in vsak $f \in \mathcal{F}$.

Za vsak $f \in \mathcal{F}$, $R \in \mathcal{R}$ (kratnosti n) in $c \in \mathcal{K}$ je seveda $f^{U'} = f^U|_{U'}$, $R^{U'} = R^U \cap U'^n$ in $c^{U'} = c^U$.

Definicija 3.11. Naj bo $U' \subseteq U$ podstruktura. Pravimo, da je U' *elementarna podstruktura* U, če za vsako $\mathcal{L}$-formulo Φ in vsako interpretacijo h na U' velja $U' \models \Phi[h]$ natanko tedaj, ko velja $U \models \Phi[h]$. V tem primeru pravimo, da je U *elementarna nadstruktura* U' in pišemo $U' \preceq U$.

Naj bo $\tau : V \to U$ vložitev V v elementarno podstrukturo $U' \preceq U$. V tem primeru za vsako $\mathcal{L}$-formulo Φ in vsako interpretacijo h na V velja $V \models \Phi[h] \Leftrightarrow U' \models \Phi[\tau \circ h] \Leftrightarrow U \models \Phi[\tau \circ h]$ po trditvi 3.8 in zaradi (očitne) elementarne ekvivalentnosti U' in U. V tem primeru je, če si ogledamo spodnjo definicijo, τ elementarna vložitev.

Definicija 3.12. Naj bo $\tau : V \to U$ vložitev $\mathcal{L}$-struktur. Če velja $V \models \Phi[h]$ natanko tedaj, ko velja $U \models \Phi[\tau \circ h]$ za vsako $\mathcal{L}$-formulo Φ in vsako interpretacijo $h : \mathrm{Vbl} \to V$, potem je τ *elementarna vložitev*.

Z drugimi besedami, vložitev τ je elementarna vložitev natanko tedaj, ko je njena slika elementarna podstruktura. Kot je jasno, iz $U' \preceq U$ sledi $U' \equiv U$ za vsako podstrukturo $U' \subseteq U$, obratno pa ne velja. Obstajajo namreč elementarno ekvivalentne podstrukture, ki pa niso elementarne podstrukture. Najenostavnejši primer najdemo v jeziku z binarno relacijo $\leq$, kjer sta $(\mathbb{N}_0, \leq)$ in $(\mathbb{N}, \leq)$- strukturi, za kateri veljajo aksiomi linearne urejenosti. Očitno je $\mathbb{N}$ podstruktura $\mathbb{N}_0$, $\tau : n \to n-1$ pa izomorfizem, iz česar sledi izomorfnost obeh struktur. Toda $\mathbb{N}$ ni elementarna podstruktura $\mathbb{N}_0$. Res - če je $h : \mathrm{Vbl} \to \mathbb{N}$ interperetacija in v spremenljivka, za katero velja $h(v) = 1$, potem velja $\mathbb{N} \models \forall x\ v \leq x[h]$, ne pa tudi $\mathbb{N}_0 \models \forall x\ v \leq x[h]$.

3.1.1. *Elementarne verige in unije struktur.* Sedaj bomo spoznali poseben primer elementarne razširitve. Naj bo α ordinalno število in $(U_\gamma)_{\gamma<\alpha}$ zaporedje $\mathcal{L}$-struktur, kjer za $\delta < \gamma < \alpha$ velja $U_\delta \subseteq U_\gamma$. To zaporedje imenujemo α*-veriga*. Poseben primer α-verige je *elemenrarna* α*-veriga*, za katero velja $U_\gamma \preceq U_{\gamma+1}$ za vsak $\gamma + 1 < \alpha$ in $U_\lambda = \cup_{\gamma<\lambda} U_\gamma$ za vsako limitno ordinalno število $\lambda < \alpha$.

Za vsako α-verigo lahko definiramo novo strukturo U, ki ji pravimo *unija struktur*. Kot množica je U enaka $\cup_{\gamma<\alpha} U_\gamma$. Za vsak $f \in \mathcal{F}$ in $R \in \mathcal{R}$ kratnosti n ter $c \in \mathcal{C}$ in vsake $a_1, \ldots, a_n \in U$ definiramo $f^U(a_1, \ldots a_n) = f^{U_\gamma}(a_1, \ldots a_n)$ in $R^U(a_1, \ldots, a_n) \Leftrightarrow R^{U_\gamma}(a_1, \ldots, a_n)$, kjer je $\gamma < \alpha$ tak, da so $a_1, \ldots, a_n \in U_\gamma$, konstante pa definiramo s $c^U = c^{U_0}$. Ker je U_δ podstruktura U_γ za vsak $\delta \leq \gamma < \alpha$, so zgornje definicije dobre. Kot nam bo povedal spodnji izrek, je v primeru, ko je α-veriga struktur elementarna, U elementarna razširitev U_γ za vsak $\gamma < \alpha$.

Trditev 3.13 ([9, posledica 2.4.6])**.** *Naj bo α ordinalno število in $(U_\gamma)_{\gamma<\alpha}$ elementarna α-veriga. Potem za unijo struktur velja $U_\gamma \preceq U$ za vsak $\gamma < \alpha$.*

Dokaz. Trditev bomo dokazali s transfinitno indukcijo po α.

Če je $\alpha = 0$, nimamo kaj dokazovati, saj je elementarna veriga prazna, prav tako pa ne obstaja γ, manjši od α, zato je pogoj $U_\gamma \preceq U$ za vsak $\gamma < \alpha$ izpolnjen na prazno.

Če je $\alpha = \beta + 1$ naslednjiško ordinalno število, po indukcijski predpostavki velja $U_\delta \preceq \cup_{\mu<\gamma} U_\mu$ za vsak $\delta < \gamma \leq \beta$. Ker velja $U_\beta = \cup_{\gamma<\alpha} U_\gamma$, saj je $\alpha = \beta + 1$ in $U_\gamma \subseteq U_\beta$ za vsak $\gamma \leq \beta$, bo dovolj, če pokažemo $\cup_{\mu<\gamma} U_\mu \preceq U_\beta$ za vsak $\gamma < \beta$, saj je $\preceq$ tranzitivna relacija med strukturami, zato iz $U_\delta \preceq \cup_{\mu<\gamma} U_\mu \preceq U_\beta$ sledi $U_\delta \preceq U_\beta$. Če je tudi $\beta = \mu + 1$ naslednjiško število, je $U_{\gamma<\beta} U_\gamma = U_\mu$, in ker je $\mu + 1 = \beta < \alpha$, je po predpostavki $U_\mu \preceq U_{\mu+1} = U_\beta$. V primeru, ko je β limitno število, pa je po predpostavki $U_\beta = \cup_{\gamma<\beta} U_\gamma$ in zato seveda velja tudi $\cup_{\gamma<\beta} U_\gamma \preceq U_\beta$.

Sedaj naj bo α limitno ordinalno število. Najprej opazimo, da za vsaka $\gamma < \delta < \alpha$ velja $U_\gamma \preceq U_\delta$, saj je $\delta + 1 < \alpha$ in zato po indukcijski predpostavki $U_\gamma \preceq \cup_{\nu<\delta+1} U_\nu = U_\delta$.

Zdaj bomo za vsak $\gamma < \alpha$, poljubno interpretacijo $h : \mathrm{Vbl} \to U_\gamma$ in poljubno formulo Φ pokazali, da velja $U_\gamma \models \Psi[h] \Leftrightarrow U \models \Psi[h]$. Dokaza se lotimo z indukcijo po kompleksnosti formule Φ. Ker trditev velja za atomarne formule po definiciji unije struktur in je indukcijski korak v primeru $\Phi = \neg\Psi$ in $\Phi = \Psi_1 \wedge \Psi_2$ trivialen, nam ostane le primer, ko je $\Phi = \forall x \Psi$ za neko spremenljivko x in formulo Ψ, za katero zgornja ekvivalenca velja. Najprej predpostavimo, da velja $U \models \forall x \Psi[h]$. Potem velja $U \models \Psi[h\binom{x}{a}]$ za vsak $a \in U$, torej tudi za vsak $a \in U_\gamma$. Po indukcijski predpostavki glede na strukturo formule zato velja $U_\gamma \models \Psi[h\binom{x}{a}]$ za vsak $a \in U_\gamma$ in zato tudi $U_\gamma \models \Phi$. Sedaj predpostavimo $U \not\models \forall x \Psi[h]$. Potem obstaja tak $a \in U$, da velja $U \not\models \Psi[h\binom{x}{a}]$. Naj bodo $x, v_0, \ldots, v_n$ vse proste spremenljivke v Ψ in $a_i = h(v_i)$ za $0 \leq i \leq n$. Obstaja takšen $\delta < \alpha$, da so $a, a_1, \ldots, a_n \in U_\delta \subseteq \cup_{\delta<\alpha} U_\delta = U$. Brez škode za splošnost lahko vzamemo tak δ, da je $\gamma \leq \delta$. Ker po indukcijski predpostavki po kompleksnosti formul velja $U_\delta \not\models \Psi[h\binom{x}{a}]$, sledi $U_\delta \not\models \forall x \Psi[h]$, in, ker je $U_\gamma \preceq U_\delta$, potem velja tudi $U_\gamma \not\models \forall x \Psi[h]$. □

3.2. **Konstantne razširitve in diagrami.**

Definicija 3.14. Naj bo $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \mathcal{K})$ jezik in $\mathcal{K}'$ množica, za katero velja $\mathcal{K} \cap \mathcal{K}' = \emptyset$. *Konstantna razširitev* jezika $\mathcal{L}$ je jezik $\mathcal{L}' = (\mathcal{F}, \mathcal{R}, \mathcal{K} \cup \mathcal{K}')$.

Jeziku $\mathcal{L}$ tako dodamo nove konstante simbole. Če je U $\mathcal{L}$-struktura in $\sigma : \mathcal{K}' \to U$ preslikava, lahko definiramo novo strukturo U', ki jo označimo tudi z (U, σ), kjer je kot množica $U' = U$, $f^{U'} = f^U$, $R^{U'} = R^U$ in $c^{U'} = c^U$ za vse simbole $f \in \mathcal{F}, R \in \mathcal{R}, c \in \mathcal{K}$ ter $c^{U'} = \sigma(c)$ ta vsak $c \in \mathcal{K}'$. V tem primeru pravimo, da je U *zožitev* U' na jezik $\mathcal{L}$. S formulo $\Phi(v_0/c_0, \ldots, v_n/c_n)$ bomo v tem razdelku označili formulo Φ, v kateri bomo za vsak $0 \leq i \leq n$ in vsako pojavitev spremenljivke v_i nadomestili s konstanto c_i. Naslednje leme ni težko pokazati, saj naredimo le enostavno indukcijo po kompleksnosti formule Φ.

Lema 3.15 ([9, izrek 2.4.1])**.** *Naj bodo U, U' in σ takšne kot zgoraj, Φ pa $\mathcal{L}$-formula s prostimi spremenljivkami v $\{v_0, \ldots, v_n\}$. Potem za vse $c_0, \ldots, c_n \in \mathcal{K}'$ in vsako interpretacijo $h : Vbl \to U'$, kjer je za $0 \leq i \leq n$ $h(v_i) = c_i$, velja $U \models \Phi[h]$ natanko tedaj, ko velja $U' \models \Phi(v_0/\sigma(c_0), \ldots, v_n/\sigma(c_n))$.*

Oglejmo si poseben primer konstantne razširitve. Naj bo $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \mathcal{K})$ jezik in U $\mathcal{L}$-struktura, za katero lahko predpostavimo $U \cap \mathcal{K} = \emptyset$, sicer preimenujemo elemente U. Za $A \subseteq U$ z $\mathcal{L}_A$ označimo jezik $(\mathcal{F}, \mathcal{R}, \mathcal{K} \cap \mathcal{A})$, kjer je $\mathcal{A} := \{c_a \mid a \in A\}$ - množici konstantnih simbolov $\mathcal{K}$ dodamo konstanten simbol c_a za vsak $a \in A$. $U' := (U, A) := (U, \sigma)$ je $\mathcal{L}_\mathcal{A}$-struktura za $\sigma(c_a) = c_a^{U'} = a$. Oglejmo si poseben primer, ko je $A = U$. Strukturo $(U, A) = (U, U)$ bomo v nalogi označevali z $\widetilde{U}$. Naj bodo

$a_0, \ldots, a_n \in U$ in $h : \mathrm{Vbl} \to U$ taka interpretacija, da velja $h(v_i) = a_i$ za $0 \leq i \leq n$. Po zgornji lemi velja $U \models \Phi[h]$ natanko tedaj, ko velja $\widetilde{U} \models \Phi(v_0/c_{a_0}, \ldots, v_n/c_{a_n})$. Naj bo $D(\widetilde{U})$ množica vseh atomarnih stavkov in njihovih negacij, ki veljajo v $\widetilde{U}$. Tej množici pravimo *diagram* $\mathcal{L}$-strukture U. $D(\widetilde{U})$ je podmnožica $\mathrm{Th}(\widetilde{U})$. Če je V $\mathcal{L}$-struktura in $\sigma : U \to V$, potem je $V' := (V, \sigma)$ $\mathcal{L}_U$-struktura. Strogo vzeto σ slika iz $\{c_a \mid a \in U\}$, ne pa iz U, a ker sta ti dve množici očitno v bijekciji, tu formalno razliko med njima zanemarimo. Kot bomo videli v spodnjem izreku, je v posebnem primeru preslikava σ (elementarna) vložitev $\mathcal{L}$-strukture U v V.

Izrek 3.16 ([9, izrek 2.4.2])**.** *(lema o diagramu) Naj bosta U in V $\mathcal{L}$-strukturi in $\sigma : U \to V$ preslikava, s čimer postane $V' := (V, \sigma)$ $\mathcal{L}_U$-struktura. Če je (V, σ) model $D(\widetilde{U})$, potem lahko U s σ vložimo v V. Če je (V, σ) poleg tega še model $Th(\widetilde{U})$, potem je $\sigma(U) \preceq V$, torej je σ elementarna vložitev U v V.*

Dokaz. Najprej predpostavimo le, da je $V' := (V, \sigma)$ model $D(\widetilde{U})$. Pokažimo najprej, da je σ injektivna. Za različna elementa $a, b \in U$ velja $\widetilde{U} \models \neg c_a \doteq c_b$, torej je $\neg c_a \doteq c_b \in D(\widetilde{U})$. Zato velja $(V, \sigma) \models \neg c_a \doteq c_b$. Ker bi iz $\sigma(a) = \sigma(b)$ sledilo $(V, \sigma) \models c_a \doteq c_b$, velja $\sigma(a) \neq \sigma(b)$, torej je σ injektivna.

Pokazati moramo, da je σ homomorfizem $\mathcal{L}$-struktur. Naj bosta $f \in \mathcal{F}$ in $R \in \mathcal{R}$ kratnosti n in $a_0, \ldots, a_n \in U$. Za $b := f^U(a_0, \ldots, a_n) \in U$ velja $\widetilde{U} \models c_b = f(c_{a_0}, \ldots, c_{a_n})$, torej je stavek $c_b \doteq f(c_{a_0}, \ldots, c_{a_n}) \in D(\widetilde{U})$. Sledi $(V, \sigma) \models c_b \doteq f(c_{a_0}, \ldots, c_{a_n})$ in zato $\sigma(b) = f^V(\sigma(a_0), \ldots, \sigma(a_n))$, saj je $c_b^{V'} = \sigma(b)$ in $c_{a_i}^{V'} = \sigma(a_i)$. Če velja $\widetilde{U} \models R(c_{a_0}, \ldots, c_{a_n})$ oz. $\widetilde{U} \models \neg R(c_{a_0}, \ldots, c_{a_n})$, po istem premisleku sklepamo, da velja $(V, \sigma) \models R(c_{a_0}, \ldots, c_{a_n})$ oz. $(V, \sigma) \models \neg R(c_{a_0}, \ldots, c_{a_n})$, zato je $(c_{a_0}^{V'}, \ldots, c_{a_n}^{V'}) = (\sigma(a_0), \ldots, \sigma(a_n)) \in R^V$ oz. $\notin R^V$. Za $c \in \mathcal{K}$ naj bo $a = c^U$. Potem velja $U' \models c_a \doteq c$, torej tudi $(V, \sigma) \models c_a \doteq c$, torej je $c^V = c_a^V = \sigma(a) = \sigma(c^U)$. Pokazali smo, da je σ vložitev $\mathcal{L}$-strukture U v V.

Sedaj predpostavimo, da je $V' = (V, \sigma)$ model $\mathrm{Th}(\widetilde{U})$. V posebnem to pomeni, da je V' model $D(\widetilde{U})$, iz česar sledi, da je σ vložitev $\mathcal{L}$-strukture $\widetilde{U}$ v V. Pokažimo, da je σ tudi elementarna vložitev, torej da za vsako interpretacijo $h : \mathrm{Vbl} \to U$ in vsako $\mathcal{L}$-formulo Φ velja $U \models \Phi[h]$ natanko tedaj, ko velja $V \models \Phi[\sigma \circ h]$.

Recimo, da velja $U \models \Phi[h]$, kjer so $v_0, \ldots, v_n$ proste spremenljivke Φ. Naj bo $a_i = h(v_i)$ za $0 \leq i \leq n$. Iz $U \models \Phi[h]$ sledi $\widetilde{U} \models \Phi(v_0/c_{a_0}, \ldots, v_n/c_{a_n})$, torej je $\Phi(v_0/c_{a_0}, \ldots, v_n/c_{a_n}) \in \mathrm{Th}(\widetilde{U})$, zaradi česar velja $V' \models \Phi(v_0/c_{a_0}, \ldots, v_n/c_{a_n})$. Zato za vsako interpretacijo $h' : \mathrm{Vbl} \to V$, za katero je $h'(v_i) = c_{a_i}^V = \sigma(a_i) = \sigma(h(v_i))$ za $0 \leq i \leq n$, velja $V \models \Phi[h']$. Ker je $\sigma \circ h(v_i) = \sigma(c_{a_i})$, sledi $V \models \Phi[\sigma \circ h]$.

Pokazali smo, da iz $U \models \Phi[h]$ sledi $V \models \Phi[\sigma \circ h]$, za dokaz obratne smeri pa zadošča, če dokazano prenesemo na formulo $\neg\Phi$. □

Za nas bo pomembna naslednja posledica leme o diagramu. Pravimo, da je podstruktura $U_1 \subseteq U$ *končno generirana*, če obstajata taka končna podmnožica $A \subseteq U_1$, da je njeno zaprtje glede na funkcije f^U in konstante c^U enako U_1.

Posledica 3.17 ([9, izrek 2.4.5])**.** *Naj bo U $\mathcal{L}$-struktura, Σ pa množica $\mathcal{L}$-stavkov. Če za vsako končno generirano podstrukturo U velja, da jo je mogoče vložiti v nek model Σ, potem lahko U vložimo v nek model Σ.*

Dokaz. Po lemi o diagramu zadošča pokazati, da ima množica $\mathcal{L}_U$-stavkov $\Sigma \cup D(\widetilde{U})$ model $V' := (V, \sigma)$, saj bo v tem primeru $\sigma : U \to V$ vložitev $\mathcal{L}$-struktur, V pa bo kot zožitev V' na jezik $\mathcal{L}$ model množice $\mathcal{L}$-stavkov Σ. Po izreku o kompaktnosti 3.5

bo dovolj, če pokažemo, da ima vsaka končna podmnožica $\Sigma \cup D(\widetilde{U})$ model. Taka končna podmnožica pa je nujno vsebovana v $\Sigma \cup A$, kjer je $A \subseteq D(\widetilde{U})$ končna. Zato se v stavkih iz A lahko pojavi samo končno mnogo različnih konstantnih simbolov $c_{a_o}, \ldots, c_{a_n}$ za $a_0, \ldots, a_n \in U$. Naj bo $U_1 \subseteq U$ podstruktura, generirana z $a_o, \ldots, a_n$. Po predpostavki obstaja $\mathcal{L}$-struktura M, ki je model Σ, in vložitev $\sigma : U_1 \to M$. Za poljubno razširitev σ' preslikave σ iz U_1 na U opazimo, da je $\mathcal{L}_U$-struktura (M, σ') model za A, torej je tudi model za $\Sigma \cup A$. S tem je dokaza konec. □

3.3. **Tipi in nasičene strukture.** Naj bo U $\mathcal{L}$-struktura in $A \subseteq U$. $\mathcal{L}$ razširimo na $\mathcal{L}_A$ s konstantnimi simboli c_a za vsak $a \in A$. Za $\mathcal{L}_A$-formulo Φ z edino prosto spremenljivko x pravimo, da je *izpolnjena* v $\mathcal{L}_A$-strukturi (U, A), če velja $(U, A) \models \exists x \Phi$. V tem primeru obstaja tak $a \in U$, da velja $(U, A \cup \{a\}) \models \Phi(x/c_a)$. Za $\Sigma(x)$, množico $\mathcal{L}_A$-formul s prosto spremenljivko x, pravimo, da je *izpolnjena* v U z nekim $a \in U$, če velja $(U, A \cup \{a\}) \models \Phi(x/c_a)$ za vsak $\Phi \in \Sigma(x)$. To označimo z $(U, A) \models \Sigma(c_a)$, pri čemer s $\Sigma(c)$ za poljuben konstanten simbol c označimo množico $\{\Phi(x/c) \mid \Phi \in \Sigma(x)\}$. Če je $\Sigma(x) = \{\Phi_1, \ldots, \Phi_n\}$ končna, to pomeni, da velja $(U, A) \models \exists x(\Phi_1 \wedge \ldots \wedge \Phi_n)$. V tem poglavju bomo spoznali množice formul, katerih vsaka končna podmnožica je izpolnjena v neki strukturi U.

Definicija 3.18. Naj bo U $\mathcal{L}$-struktura, $A \subseteq U$ in $\Sigma(x)$ množica $\mathcal{L}_A$-formul s prosto spremenljivko x. $\Sigma(x)$ je *tip* (U, A), če je v (U, A) izpolnjena vsaka končna podmnožica $\Sigma(x)$.

Vsak končen tip (U, A) je avtomatično izpolnjen v (U, A), kar pa, kot bosta pokazala spodnja enostavna primera, v splošnem ne velja tudi za neskončne tipe.

Primer 3.19. Jezik $\mathcal{L}$ razširimo na $\mathcal{L}_U$, kjer je U neskončna $\mathcal{L}$-struktura. Za vsak $a \in U$ naj bo Φ_a $\mathcal{L}_U$-formula $\neg x \doteq c_a$. Očitno je vsaka končna podmožica $\{\Phi_a \mid a \in U\}$ izpolnjena v $\widetilde{U}$, saj je U neskončna. $\Sigma(x)$ pa ni izpolnjena v U, saj za vsak element $a \in U$ velja $a = c_a^{\widetilde{U}}$. ♢

Tipe v strukturi si lahko predstavljamo kot opis nekeka elementa b, ki je lahko v U ali pa ga lahko v U brez težav dodamo, kot nam bosta pokazala spodnji primer in izrek.

Primer 3.20. Vzemimo model za linearno urejenost $\mathbb{N}$ in jezik $\mathcal{L} = \{\leq\}$ razširimo s konstantami c_n za vsak $n \in \mathbb{N}$. Očitno je, da je množica formul $\{c_n \leq x \mid n \in \mathbb{N}\}$ tip $\widetilde{\mathbb{N}}$, ki v $\widetilde{\mathbb{N}}$ ni izpolnjen. Je pa izpolnjen v $\mathcal{L}_{\mathbb{N} \cup \{\infty\}}$-strukturi $\widetilde{\mathbb{N} \cup \{\infty\}}$, če $\leq$ razširimo na $\leq_\infty$, kjer je $n \leq_\infty m$ natanko tedaj, ko je $n \leq m$, in $l \leq_\infty \infty$ za vse za $m, n, l \in \mathbb{N}$. Neformalno rečeno: obstoj elementa ∞ ni v protislovju z nobenim stavkom iz $\mathrm{Th}(\mathbb{N})$. ♢

Izrek 3.21 ([9, izrek 2.5.1])**.** *Naj bo U $\mathcal{L}$-struktura in $A \subseteq U$. Za množico $\mathcal{L}_A$-formul $\Sigma(x)$ s prosto spremenljivko x sta naslednji trditvi ekvivalentni:*

(1) *$\Sigma(x)$ je tip (U, A).*
(2) *Obstaja elementarna razširitev $U \preceq U_1$ in $A_1 \subseteq U_1$, da velja $(U_1, A_1) \models \Sigma(c_a)$ za nek $a \in A_1$.*

Dokaz. Naj bo $\Sigma(x)$ tip (U, A). Jezik $\mathcal{L}_A$ razširimo z novim konstantnim simbolom c. Naj bo $\Sigma' := \mathrm{Th}(U, A) \cup \Sigma(c)$ in recimo, da obstaja model Σ', ki ga imenujemo U_1. Iz leme o diagramu sledi, da je zožitev U_1 na jezik $\mathcal{L}_A$ (brez c) elementarna razširitev (U, A), obenem pa velja $(U_1, A \cup \{a\}) \models \Sigma(c)$, kjer je $a \in U_1$ tak, da velja $c^{U_1} = a = c_a^{U_1}$. Sledi $(U_1, A \cup \{a\}) \models \Sigma(c_a)$. Zato nam preostane, da pokažemo,

da ima Σ' model oz., zaradi kompaktnosti, da ima model vsaka končna podmnožica Σ'. Vsaka taka končna podmnožica pa je vsebovana v $\mathrm{Th}(U,A) \cup \Pi(c)$, kjer je $\Pi(c) = \{\Phi_1, \ldots, \Phi_n\}$ končna podmnožica $\Sigma(c)$. To pa velja zato, ker za $U' := (U, A)$ velja $U' \models \exists x(\Phi_1 \wedge \ldots \wedge \Phi_n)$. Torej obstaja tak $a \in U$, ki izpolnjuje $\Phi_1, \ldots, \Phi_n$. Na množici $\{c\}$ definiramo preslikavo $\sigma(c) = a$, s čimer dobimo $(U, \sigma) \models \Pi(c)$. (U, σ) je zato model $\mathrm{Th}(U, A) \cup \Pi(c)$. Pokazali smo, da ima Σ' model, ki izpolnjuje $\Sigma(x)$.

Obratno: če obstaja taka elementarna razširitev $U \preceq U_1$ in $A_1 \subseteq U_1$, da velja $(U_1, A_1) \models \Sigma(c_a)$ za nek $a \in A_1$, potem za vsako končno družino formul $\Phi_1, \ldots, \Phi_n \in \Sigma$ velja $(U_1, A) \models \exists x(\Phi_1 \wedge \ldots \wedge \Phi_n)$, iz česar zaradi elementarne ekvivalentnosti sledi tudi $(U, A) \models \exists x(\Phi_1 \wedge \ldots \wedge \Phi_n)$. □

Sedaj bomo spoznali $\mathcal{L}$-strukture U, ki bodo realizirale vse tipe v jeziku $\mathcal{L}_A$, pri čemer bo veljala omejitev na kardinalnost množice $A \subseteq U$.

Definicija 3.22. Naj bo U $\mathcal{L}$-struktura in κ neko neskončno kardinalno število. Pravimo, da je U *κ-nasičena* struktura, če za vsako množico $A \subseteq U$, za katero je $|A| < \kappa$, U izpolnjuje vsak $\mathcal{L}_A$ tip $\Sigma(x)$. Če je U $|U|$-nasičena, pravimo, da je *nasičena*.

Najprej povejmo nekaj jasno razvidnih lastnosti nasičenosti. Če je U končna $\mathcal{L}$- struktura z elementi $\{a_0, \ldots, a_n\}$, potem $\mathcal{L}_U$-struktura $\widetilde{U}$ nima nobene prave elementarne razširitve, saj v njej velja trditev $\forall x(x = c_{a_0} \vee \ldots \vee x = c_{a_n})$, ki ne mora veljati v nobeni $\mathcal{L}_U$, ki ima več kot $n+1$ elementov. Iz tega po izreku 3.21 sledi, da je vsak tip U izpolnjen v U, torej je U κ-nasičena za vsak κ. Če pa je U neskončna κ-nasičena $\mathcal{L}$ struktura, potem velja $\kappa \leq |U|$, sicer bi bil v U izpolnjen tudi tip iz primera 3.19.

Naj bo U κ-nasičena $\mathcal{L}$-struktura. Jezik $\mathcal{L}$ razširimo z manj kot κ novimi simboli, zbranimi v množico $\mathcal{K}'$. Za preslikavo $\sigma : \mathcal{K}' \to U$ definiramo $K := \sigma(\mathcal{K}') \subseteq U$ in $\mathcal{L}' := \mathcal{L}_{\mathcal{K}'}$. Potem je tudi $\mathcal{L}'$-struktura (U, σ) κ-nasičena. Res: naj bo $A \subseteq U, |A| < \kappa$ in $\Sigma(x)$ tip v jeziku ${\mathcal{L}'}_A$. Če zamenjamo konstantne simbole iz $\mathcal{K}'$ s c_a za $a \in \mathcal{K}$, vidimo, da je $\Sigma(x)$ tip $\mathcal{L}_{A \cup K}$, in ker je $|A \cup K| < \kappa$, ga U izpolnjuje. Zato ga izpolnjuje tudi $((, \sigma)$. Sklep: κ-nasičenost $\mathcal{L}$-strukture se ohrani, če $\mathcal{L}$ razširimo z manj kot κ konstantami.

Za jezik $\mathcal{L}$ definirajmo $\kappa_{\mathcal{L}} := \max\{\aleph_0, |\mathcal{F}|, |\mathcal{R}|, |\mathcal{K}|\}$, ki bo oznaka za kardinalnost jezika. Z njeno pomočjo lahko definiramo tudi moči množic vseh $\mathcal{L}$-izrazov, stavkov in formul $\mathrm{Tm}(\mathcal{L})$, $\mathrm{Sent}(\mathcal{L})$ in $\mathrm{Form}(\mathcal{L})$. Ker je vsak izraz končno zaporedje spremenljivk (katerih je $\aleph_0$ mnogo), konstantnih in funkcijskih simbolov ter ločil in oklepajev (katerih je končno mnogo), je $|\mathrm{Tm}(\mathcal{L})| \leq \max\{\aleph_0, |\mathcal{F}|, |\mathcal{K}|\}$. Obratna neenakost sledi iz dejstva, da je vsaka spremenljivka, vsak konstanten simbol $c \in \mathcal{K}$ in $f(v_0)$ za vsak funkcijski simbol $f \in \mathcal{F}$ izraz. Ker je vsaka $\mathcal{L}$-formula končno zaporedje spremenljivk, $\mathcal{L}$-izrazov, relacijskih simbolov ter logičnih veznikov, kvantifikatorjev in ločil (ki jih je končno mnogo), vsak stavek pa formula, je $|\mathrm{Sent}(\mathcal{L})| \leq |\mathrm{Form}(\mathcal{L})| \leq \kappa_L$. Obratne neenakosti sledijo iz dejstva, da je $R(t, \ldots, t) \in \mathrm{Sent}(\mathcal{L})$ za vsak izraz t in vsak relacijski simbol $R \in \mathcal{R}$.

Naslednja izreka, ki smo ju v nekoliko manjši splošnosti spoznali pri logiki in ju zato ne bomo dokazovali, nam povesta, da za vsako $\mathcal{L}$-strukturo U obstajata elementarna podstruktura ali razširitev U moči κ za skoraj vsako kardinalnost κ.

Izrek 3.23 ([9, izrek 2.3.3])**.** *(Löwenheim-Skolem navzdol) Naj bo U $\mathcal{L}$-struktura z neskončne kardinalnosti in $B \subseteq U$. Potem obstaja elementarna podstruktura $U' \preceq U$, da velja $B \subseteq U'$ in $|U'| \leq \max\{|B|, \kappa_L\}$. Če velja $\kappa_l \leq |B|$, velja še $|U'| = |B|$.*

Izrek 3.24 ([9, izrek 2.4.3]). *(Löwenheim-Skolem navzgor) Naj bo U $\mathcal{L}$-struktura neskončne kardinalnosti. Potem za vsako kardinalno število $\kappa \geq \max\{\kappa_{\mathcal{L}}, |U|\}$ obstaja elementarna razširitev $U \preceq U'$ kardinalnosti κ.*

Izrek 3.25 ([9, izrek 2.5.2]). *Naj bo $\mathcal{L}$ jezik, $\kappa \geq \kappa_{\mathcal{L}}$ kardinalno število, κ^+ njegov naslednik in U $\mathcal{L}$-struktura kardinalnosti kvečjemu 2^κ. Potem obstaja κ^+-nasičena elementarna razširitev $U \preceq U'$ kardinalnosti kvečjemu 2^κ.*

Opomba 3.26. Če privzamemo, da velja hipoteza kontinuuma, po kateri je $\kappa^+ = 2^\kappa$ za vsako neskončno kardinalno število κ, iz 3.25 in izreka Löwenheim-Skolem - navzdol, sledi, da za vsako kardinalno število $\kappa \geq \kappa_L$ obstaja nasičena struktura kardinalnosti κ.

Dokaz. V dokazu bomo skonstruirali elementarno κ^+-verigo, katere unija bo, kot bomo videli, iskana κ^+-nasičena struktura. Za vsak $\lambda < \kappa^+$ bosta, kot bomo pokazali z indukcijo, veljala dva pogoja:

(1) $|U_\lambda| \leq 2^\kappa$,
(2) $U_{\lambda+1}$ izpolnjuje vse tipe $\Sigma(x)$ v U_λ, za katere velja $|\Sigma(x)| \leq \kappa$.

Za vsako ordinalno število $\lambda < \kappa^+$ bomo definirali elementarno razširitev $U \preceq U_\lambda$. Začetek verige definiramo z $U_0 := U$. Pogoj (1) velja za U_0 po predpostavki izreka, pogoj (2) pa je izpolnjen na prazno. V primeru, ko je $\lambda = \beta + 1$ naslednjiško število, bomo definirali $U_{\beta+1}$ kot unijo elementarne verige.

Najprej pokažimo, da je vseh tipov $\Sigma(x)$ v U_λ, za katere velja $|\Sigma(x)| \leq \kappa$, kvečjemu 2^κ. Res: če jezik $\mathcal{L}$ razširimo s konstantnimi simboli c_a za $a \in U_\lambda$, dobimo jezik $\mathcal{L}_{U_\lambda}$, za katerega velja $\kappa_{\mathcal{L}_{U_\lambda}} = \max\{|U_\lambda|, \kappa_{\mathcal{L}}\} \leq 2^\kappa$ po indukcijski predpostavki (za U_λ namreč velja pogoj (1)) in dejstvu, da velja $\kappa_{\mathcal{L}} \leq \kappa$. Iz tega sledi, da je vseh $\mathcal{L}_{U_\lambda}$-formul kvečjemu 2^κ. Zato je vseh naborov $\mathcal{L}_{U_\lambda}$-formul moči največ κ kvečjemu $(2^\kappa)^\kappa = 2^\kappa$. Vse tipe $\Sigma(x)$ v U_λ, ki vsebujejo kvečjemu κ mnogo formul, indeksiramo z ordinalnim številom $\nu \leq 2^\kappa$: $(\Sigma_\alpha(x))_{\alpha<\nu}$.

Sedaj definiramo elementarno ν-verigo:

- $V_0 := U_\lambda$
- Za naslednjiško ordinalno število $\alpha + 1$ naj bo $V_{\alpha+1}$ neka elementarna razširitev V_α, ki izpolnjuje $\Sigma_\alpha(x)$ in za katero velja $|V_{\alpha+1}| \leq 2^\kappa$.

Pokažimo, da taka elementarna razširitev obstaja. Po 3.21 obstaja elementarna razširitev $V_\alpha \preceq V'$, in $A' \subseteq V'$, da velja $(V', A') \models \Sigma_\alpha(c_b)$ za nek $b \in A'$. Strukturo (V', A') zožimo na jezik $\mathcal{L}_{V_\alpha}$, za katerega velja (kot smo že razmislili zgoraj) $\kappa_{\mathcal{L}_{V_\alpha}} \leq 2^\kappa$. Dobljena struktura V'' je po lemi o diagramu elementarna razširitev V_α. Po izreku Löwenheim-Skolem - navzdol zato obstaja taka $\mathcal{L}_{V_\alpha}$-struktura $V_{\alpha+1} \preceq V''$, ki vsebuje $V_\alpha \cup \{b\}$ in ima kardinalnost kvečjemu 2^κ.

- Če je $\alpha < \nu$ limitno število, V_α definiramo kot unijo $\cup_{\mu<\alpha} V_\mu$.

Struktura $U_{\beta+1} := \cup_{\alpha<\nu} V_\alpha$ je po trditvi 3.13 elementarna razširitev U_β. Po konstrukciji je jasno, da $U_{\beta+1}$ izpolnjuje vse tipe v U_λ, ki imajo kvečjemu κ formul, saj za vsak tak tip $\Sigma(x)$ obstaja $\alpha < \nu$, da ga V_α izpolnjuje, $U_{\beta+1}$ pa je elementarna razširitev vseh takih V_α. Ker velja $U_{\beta+1} = \cup_{\alpha<\nu} V_\alpha$, kjer je $\nu \leq 2^\kappa$ in $|V_\alpha| \leq 2^\kappa$ za vsak $\alpha < \nu$, je $|U_{\beta+1}| \leq 2^\kappa \cdot 2^\kappa = 2^\kappa$, torej je izpolnjen tudi pogoj (1).

Sedaj ko smo definirali verigo $(U_\lambda)_{\lambda<\kappa^+}$, pokažimo, da je njena unija $U' := \cup_{\lambda<\kappa^+} U_\lambda$ iskana κ^+-nasičena struktura. Ker je $\kappa^+ \leq 2^\kappa$ in po pogoju (1) velja $|U_\lambda| < 2^\kappa$ za vsak $\lambda \leq \kappa^+$, potem sledi $|U'| \leq 2^\kappa \cdot 2^\kappa = 2^\kappa$. Preverimo še κ^+-nasičenost. Naj bo Σ tip strukture (U', A), kjer je $A \subseteq U'$, $|A| < \kappa^+$ oz. $|A| \leq \kappa$.

Ker je κ^+ regularno kardinalno število (saj je nasledniško)[1] in $A \subseteq U' := \cup_{\lambda<\kappa^+} U_\lambda$, obstaja tak $\lambda < \kappa^+$, da je $A \subseteq U_\lambda$ za nek $\lambda < \kappa^+$. Ker je vseh formul Φ v jeziku $\mathcal{L}_A$ manj ali enako $\max\{\kappa_\mathcal{L}, |A|\} \leq \kappa$ po predpostavki, velja $\Sigma(x) \leq \kappa$. Zato po zgornji konstrukciji obstaja $a \in U_{\lambda+1}$, da velja $\widetilde{U_{\lambda+1}} = (U_{\lambda+1}, U_{\lambda+1}) \models \Sigma(c_a)$. Iz $U_{\lambda+1} \preceq U'$ pa sledi $\widetilde{U'} = (U', U') \models \Sigma(c_a)$. S tem je izrek dokazan. □

V naslednjem izreku bomo s $\exists$-*stavek* poimenovali stavek oblike $\exists v_0, \ldots, v_n \Psi$, kjer bo Ψ formula brez kvantifikatorjev.

Izrek 3.27 ([9, izrek 2.5.4])**.** *Naj bosta U in U' $\mathcal{L}$-strukturi in $\kappa \geq |U|$ kardinalno število. Recimo, da je U' κ-nasičena in da vsak $\exists$-stavek Φ, za katerega velja $U \models \Phi$, velja tudi $U' \models \Phi$. Potem lahko U vložimo v U'.*

Dokaz. Če za strukturi U_1 in U_2 velja implikacija $U_1 \models \Phi \implies U_2 \models \Phi$ za vsak $\exists$-stavek Φ, bomo to označili z $U_1 \overset{\exists}{\to} U_2$. Naj bo $\lambda = |U|$. Elemente $a \in U$ uredimo v zaporedje $(a_\nu)_{\nu<\lambda}$ in jeziku $\mathcal{L}$ dodamo nove konstantne simbole c_ν za vsak $\nu < \lambda$, s čimer dobimo jezik, ki ga označimo z $\mathcal{L}_\lambda$. V U' bomo skonstruirali tako zaporedje $(a'_\nu)_{\nu<\lambda}$, da bo veljalo

$$(U, (a_\nu)_{\nu<\lambda}) \overset{\exists}{\to} (U', (a'_\nu)_{\nu<\lambda}).$$

To bomo storili tako, da bo po indukciji za vsak $\beta < \lambda$ veljalo $(U, (a_\nu)_{\nu\leq\beta}) \overset{\exists}{\to} (U', (a'_\nu)_{\nu\leq\beta})$. Pokažimo, da iz tega sledi $(U, (a_\nu)_{\nu<\lambda}) \overset{\exists}{\to} (U', (a'_\nu)_{\nu<\lambda})$. Za končno kardinalno število λ je pogoj $(U, (a_\nu)_{\nu<\lambda}) \overset{\exists}{\to} (U', (a'_\nu)_{\nu<\lambda})$ ekvivalenten $(U, (a_\nu)_{\nu\leq\lambda-1}) \overset{\exists}{\to} (U', (a'_\nu)_{\nu\leq\lambda-1})$, v primeru, ko je λ neskončno kardinalno število, pa upoštevamo, da je limitno število. Predpostavimo $(U, (a_\nu)_{\nu<\lambda}) \models \Phi$. V $\mathcal{L}_\lambda$-formuli Φ nastopa zgolj končno mnogo konstantnih simbolov $c_\alpha, \alpha < \lambda$. Supremum pripadajočih α označimo z $\gamma < \alpha$. Zato velja tudi $(U, (a_\nu)_{\nu\leq\gamma}) \models \Phi$, iz česar po predpostavki sledi $(U', (a'_\nu)_{\nu\leq\gamma}) \models \Phi$. Torej v tem primeru velja $(U', (a'_\nu)_{\nu<\lambda}) \models \Phi$.

Sedaj smo pri definiciji zaporedja $(a'_\nu)_{\nu<\lambda}$. Naj bo $\beta < \gamma$ in predpostavimo, da že imamo zaporedje $(a'_\nu)_{\nu<\beta}$, za katerega za vsak $\gamma < \beta$ velja $(U, (a_\nu)_{\nu\leq\gamma}) \overset{\exists}{\to} (U', (a'_\nu)_{\nu\leq\gamma})$. Poiskati moramo primeren a'_β, da bo veljalo tudi $(U, (a_\nu)_{\nu\leq\beta}) \overset{\exists}{\to} (U', (a'_\nu)_{\nu\leq\beta})$.

Naj bo $\Sigma(x)$ množica vseh $\exists$-formul Φ v jeziku L_β , ki imajo prosto spremenljivko kvečjemu x in za katere velja $(U, (a_\nu)_{\nu\leq\beta}) \models \Phi(c_\beta)$. Velja torej $(U, (a_\nu)_{\nu\leq\beta}) \models \Sigma(c_\beta)$. Ker je $(U, (a_\nu)_{\nu\leq\beta})$ razširitev strukture $(U, (a_\nu)_{\nu<\beta})$ (razlika je namreč le v enem konstantnem simbolu v jeziku), je po 3.21 $\Sigma(x)$ tip $(U, (a_\nu)_{\nu<\beta})$, zato za vsak končen nabor $\Phi_1, \ldots, \Phi_n \in \Sigma(x)$ velja $(U, (a_\nu)_{\nu<\beta}) \models \exists x(\Phi_1 \wedge \ldots \wedge \Phi_n)$.

Vsaka formula Φ_i za $1 \leq i \leq n$ je oblike $\exists v_0^{(i)}, \ldots, v_{m_i}^{(i)} \Psi_i$, kjer je Ψ_i formula brez kvantifikatorjev in v kateri nastopajo kvečjemu spremenljivke $x, v_0^{(i)}, \ldots, v_{m_i}^{(i)}$ Z morebitnim preimenovanjem spremenjivk Φ_i lahko brez škode za splošnost predpostavimo, da za $i \neq j$ nobena spremenljivka, ki nastopa v Ψ_i razen morebiti x ne nastopa v Ψ_j. Zato je stavek $\exists x(\Phi_1 \wedge \ldots \wedge \Phi_n)$ v vsaki $\mathcal{L}_\beta$-strukturi ekvivalenten $\exists$-stavku $\exists x, v_0^{(1)}, \ldots, v_{m_1}^{(1)}, v_0^{(2)}, \ldots, v_0^{(n)}, \ldots, v_{m_n}^{(n)}(\Psi_1 \wedge \ldots \wedge \Psi_n)$.

V (fiksni) formuli $\Phi_1 \wedge \ldots \wedge \Phi_n$ nastopa kvečjemu končno mnogo simbolov c_α za $\alpha < \beta$. Supremum pripadajočih ordinalih števil α označimo z $\delta < \beta$.

[1]Spomnimo, da za regularno kardinalno število κ velja, da ne obstajata tako kardinalno število $\kappa' < \kappa$ in funkcija $f : \kappa' \to \kappa$, da je $sup_{\alpha<\kappa'} f(\alpha) = \kappa'$.

Velja $(U,(a_\nu)_{\nu\le\delta}) \models \exists x(\Phi_1\wedge\ldots\wedge\Phi_n)$ in zato, ker po indukcijski predpostavki velja $(U,(a_\nu)_{\nu\le\delta}) \overset{\exists}{\to} (U',(a_\nu)_{\nu\le\delta})$, sledi $(U',(a_\nu)_{\nu\le\delta}) \models \exists x(\Phi_1\wedge\ldots\wedge\Phi_n)$. Tu upoštevamo zgornji razmislek, da je $\exists x(\Phi_1\wedge\ldots\wedge\Phi_n)$ elementarno ekvivalenten nekemu $\exists$-stavku. Torej velja tudi $(U',(a'_\nu)_{\nu<\beta}) \models \exists x(\Phi_1\wedge\ldots\wedge\Phi_n)$.

Ugotovili smo, da je vsaka končna podmnožica $\Sigma(x)$ izpolnjena v $(U',(a_\nu)_{\nu<\beta})$. Iz κ-nasičenosti U' in neenakosti $|\Sigma(x)| \le |\mathrm{Form}(L_\beta)| \le \max\{\kappa_L,|\beta|\} \le \kappa$ sledi, da je tudi $\Sigma(x)$ izpolnjena v $(U',(a_\nu)_{\nu\le\beta})$. κ-nasičenost poljubne strukture se namreč ohrani, če jeziku dodamo manj kot κ konstant, in ker je $|\gamma| < \lambda = |U| \le \kappa$ po predpostavki, iz κ-nasičenosti U' sledi κ-nasičenost $(U',(a_\nu)_{\nu<\beta})$. Torej obstaja tak $b \in U'$, ki izpolnjuje $\Sigma(x)$. Če definiramo $a'_\beta := b$, sledi $(U',(a'_\nu)_{\nu\le\beta}) \models \Phi(a'_\beta)$ za vsak $\exists$-stavek Φ, ki velja v $(U,(a_\nu)_{\nu\le\beta})$.

Po zgornjem premisleku smo skonstruirali zaporedje $(a'_\nu)_{\nu<\lambda} \subseteq U'$, da velja $(U,(a_\nu)_{\nu<\lambda}) \overset{\exists}{\to} (U',(a'_\nu)_{\nu<\lambda})$. Ker so vsi atomarni stavki in njihove negacije $\exists$-stavki, lahko vidimo, da je $(U',(a'_\nu)_{\nu<\lambda})$ model $D(\widetilde{U})$. Res: edina razlika, na katero moramo biti pozorni, je, da imamo namesto jezika $\mathcal{L}_U$ jezik $\mathcal{L}_\lambda$, kar lahko popravimo s tem, da spremenimo vse konstantne simbole iz c_λ v c_{a_λ}. Ker je $(U',(a'_\nu)_{\nu<\lambda})$ model $D(\widetilde{U})$, po lemi o diagramu sledi, da lahko U vložimo v U', s čimer smo dokaz izreka končali. □

Naslednji izrek se dokaže zelo podobno kot zgornji. Predpostavimo, da namesto $U \overset{\exists}{\to} U'$ velja močnejši pogoj $U \equiv U'$, druge predpostavke pa so enake. Če sedaj v dokazu naredimo vse korake enake, edino tam, kjer pri konstrukciji zaporedja $(a'_\nu)_{\nu<\lambda}$ pri indukcijskem koraku vzamemo za $\Sigma(x)$ množico vseh $\mathcal{L}_\beta$- formul s prosto spremenljivko kvečjemu x namesto množice vseh $\exists$-formul v jeziku $\mathcal{L}_\beta$, dobimo, da je dobljena struktura $\mathcal{L}_\lambda$ struktura $(U',(a'_\nu)_{\nu<\lambda})$ model $\mathrm{Th}(\widetilde{U})$ in ne zgolj $D(\widetilde{U})$. Če uporabimo lemo o diagramu, iz povedanega sledi, da je $U \preceq U'$. Zapišimo ugotovitev:

Izrek 3.28 ([9, izrek 2.5.5])**.** *Naj bosta U in U' elementarno ekvivalentni $\mathcal{L}$-strukturi in $\kappa \ge |U|$ kardinalno število. Recimo, da je U' κ-nasičena. Potem obstaja elementarna vložitev U v U'.*

Naslednja posledica izreka bo pomembna pri dokazu Ax-Kochenovega izreka. Pravimo, da je U *eksistencialno zaprta* v elementarni nadstrukturi $U \subseteq U'$, če vsak $\exists$-stavek v jeziku $\mathcal{L}_U$, ki velja v U', velja tudi v U.

Posledica 3.29 ([9, izrek 2.5.5])**.** *Naj bo U podstruktura $\mathcal{L}$-struktur U_1 in U_2. Velja naslednje:*

(1) *Če je U_2 κ-nasičena struktura, kjer je $\kappa > |U_1|$ in je bodisi U eksistencialno zaprta v U_1 bodisi lahko vsako končno generirano $\mathcal{L}_U$-podstrukturo $U' \subseteq U_1$ vložimo v U_2, potem lahko (U_1,U) vložimo v (U_2,U).*

(2) *Če lahko $\mathcal{L}_U$-strukturo (U_1,U) vložimo v (U_2,U) in velja $U \preceq U_2$, potem je U eksistencialno zaprta v U_1.*

Opomba 3.30. To, da lahko (U_1,U) vložimo v (U_2,U), pomeni, da obstaja vložitev U_1 v U_2, ki je konstantna na U.

Dokaz. Po 3.27 za dokaz točke (1) zadošča pokazati, da velja $(U_1,U) \overset{\exists}{\to} (U_2,U)$. Ker je $|U| \le |U_1| < \kappa$, je tudi struktura (U_2,U) κ-nasičena, saj smo jezik razširili z manj kot κ konstantnimi simboli. Naj bo Φ $\exists$-stavek, za katerega velja $(U_1,U) \models \Phi$. Če je U eksistencialno zaprt v U_1, iz tega sledi $\widetilde{U} \models \Phi$. Torej, če je $\Phi = \exists v_0,\ldots,v_n\Psi$,

kjer je Ψ formula brez kvantifikatorjev in s prostimi spremenljivkami v $\{v_0, \ldots, v_n\}$, obstajajo taki $a_0, \ldots, a_n \in U$, da velja $\widetilde{U} \models \Psi(v_0/a_0, \ldots, v_n/a_n)$ in zato, ker je $U \subseteq U_2$, velja $(U_2, U) \models \Psi(v_0/a_0, \ldots, v_n/a_n)$, iz česar sledi $(U_2, U) \models \Phi$.

Sedaj predpostavimo, da lahko vsako končno generirano $\mathcal{L}_U$-podstrukturo (U_1, U) vložimo v (U_2, U). Naj bo Φ $\exists$-stavek, za katerega velja $(U_1, U) \models \Phi$ in ki ga tako kot v zgornjem odstavku zapišemo kot $\Phi = \exists v_0, \ldots, v_n \Psi$. Potem obstajajo taki $a_0, \ldots, a_n \in U_1$, da velja $(U_1, U) \models \Psi(v_0/a_0, \ldots, v_n/a_n)$. Naj bo $U_1' \subseteq U_1$ $\mathcal{L}_U$- podstruktura (kot taka, bodimo pozorni, vsebuje U) U_1, generirana z $a_0, \ldots, a_n \in U_1$. Po predpostavki lahko U_1' vložimo v U_2 kot $\mathcal{L}_U$-strukturo. To pomeni, da obstaja $\tau : U_1' \to U_2$, da je $\tau(a) = a$ za vsak $a \in U$. Ker velja $(U_2, U) \models \Psi(v_0/a_0, \ldots, v_n/a_n)$, velja $(U_1, U) \models \Psi(v_0/\tau(a_0), \ldots, v_n/\tau(a_n))$, ker je τ vložitev (in v posebnem homomorfizem), Ψ pa nima kvantifikatorjev. Torej velja $(U_2, U) \models \Phi$.

Dokažimo še točko (2): naj bo Φ $\exists$-stavek jezika $\mathcal{L}_U$, za katerega velja $(U_1, U) \models \Phi$. Po istem razmisleku kot v prejšnjem primeru (z upoštevanjem, da je Φ $\exists$-stavek, (U_1, U) pa lahko vložimo v (U_2, U)) sklepamo, da velja $(U_2, U) \models \Phi$ in zato (ker je $U \preceq U_2$) $\widetilde{U} \models \Phi$. □

3.4. **Ultraprodukti.** Ultraprodukt družine $\mathcal{L}$ - struktur U_s, $s \in S$, si lahko predstavljamo kot neke vrste kvocient velikega produkta struktur po neprazni indeksni množici S. Za formalno pravilno definicijo ultraprodukta struktur pa moramo še prej definirati ultrafiltre.

3.4.1. *Ultrafiltri.* Najprej si oglejmo, kaj je filter na neprazni množici.

Definicija 3.31. Naj bo S neprazna množica. *Filter* na množici S je družina množic $\mathcal{F} \subseteq \mathcal{P}(S)$, za katero velja:

(1) $S \in \mathcal{F}, \emptyset \notin \mathcal{F}$,
(2) $X \in \mathcal{F}, Y \in \mathcal{F} \Rightarrow X \cap Y \in \mathcal{F}$,
(3) $X \in \mathcal{F}, X \subseteq Y \subseteq S \Rightarrow Y \in \mathcal{F}$.

Primer 3.32. Množica $\{S\}$ je *trivialen* filter na S, ki je hkrati najmanjši filter na poljubni množici S.

Če je $A \subseteq S$ neprazna, potem je množica $\{X \subseteq S \mid A \subseteq X\}$ filter na S. Takšnemu filtru pravimo *glavni filter na S, generiran z A*. V nasprotnem primeru je *neglavni*. Primer neglavnega filtra je družina $\{X \subseteq S \mid S \setminus X \text{ je končna}\}$ vseh podmnožic s končnim komplementom oz. kokončnih množic neke neskončne množice S. Temu filtru pravimo *filter kokončnih množic*. Če je S končen, je ta družina enaka $\mathcal{P}(S)$, ki ni filter. ♢

Filter $\mathcal{F}$ na S je *maksimalen*, če ne obstaja tak filter $\mathcal{F}'$, da velja $\mathcal{F} \subsetneq \mathcal{F}' \subseteq \mathcal{P}(S)$. Primer maksimalnega filtra bi bil glavni filter $\mathcal{F}$, generiran z množico $\{a\}$ za nek $a \in S$. Res, za vsak filter $\mathcal{F} \subsetneq \mathcal{F}' \subseteq \mathcal{P}(S)$ bi obstajal tak $X \in \mathcal{F}'$, da bi veljalo $a \notin X$. Ker pa je $\{a\} \in \mathcal{F} \subsetneq \mathcal{F}'$, po drugem aksiomu za filtre velja $\{a\} \cap X = \emptyset \in \mathcal{F}'$, kar pa je v nasprotju s prvim aksiomom za filtre.

Definicija 3.33. Neprazna družina množic $\mathcal{G}$ ima *lastnost končnih presekov*, če za vsako končno poddružino množic $X_1, X_2, \ldots, X_m \in \mathcal{G}$ velja $\cap_{i=1}^m X_i \neq \emptyset$.

Če družina množic ne vsebuje prazne množice in je zaprta za končne preseke, ima lastnost končnih presekov. Zato je jasno, da ima vsak filter lastnost končnih presekov, velja pa še več.

Lema 3.34 ([6, izrek 11.1.7]). *Vsako neprazno družino množic $\mathcal{G} \subseteq \mathcal{P}(S)$ z lastnostjo končnih presekov lahko razširimo do filtra $\mathcal{F} \supseteq \mathcal{G}$.*

Dokaz. Naj bo $\mathcal{F}$ množica vseh takih $X \subseteq S$, da obstaja končen presek $\cap_{i=1}^{n} X_i \subseteq X$, kjer je $X_i \in \mathcal{G}$ za vsak i. Očitno $\mathcal{F}$ vsebuje $\mathcal{G}$, pokažimo še, da je filter. Jasno je, da je $S \in \mathcal{F}$, in ker ima $\mathcal{G}$ lasnost končnih presekov, ne obstaja končen presek množic iz $\mathcal{G}$, ki bi bil vsebovan v prazni množici. Če je $\cap_{i=1}^{n} X_i \subseteq X$ in $\cap_{j=1}^{m} Y_j \subseteq Y$ za $X_i, Y_j \in \mathcal{G}$, je $\cap_{i=1}^{n} X_i \cap \cap_{j=1}^{m} Y_j \subseteq X \cap Y$, torej je $\mathcal{F}$ zaprta za končne preseke. Za $X \subseteq Y$, za katere velja $\cap_{i=1}^{n} X_i \subseteq X \subseteq Y$, pa je očitno tudi $Y \in \mathcal{F}$. □

Sedaj lahko definiramo poseben razred filtrov.

Definicija 3.35. Filter $\mathcal{U}$ na S je *ultrafilter*, če za vsak $X \subseteq S$ velja $X \in \mathcal{U}$ ali $S \setminus X \in \mathcal{U}$.

Iz zaprtosti filtrov za preseke sledi, da ultrafilter vsebuje neko podmnožico S natanko tedaj, ko ne vsebuje njenega komplementa. Ultrafiltre lahko karakteriziramo tudi drugače, kot bo pokazala spodnja lema.

Lema 3.36 ([6, izrek 11.2.3]). *Filter $\mathcal{F}$ na množici S je ultrafilter natanko tedaj, ko je maksimalen.*

Dokaz. Očitno je, da je vsak ultrafilter maksimalen, saj bi vsaka njegova razširitev vsebovala neko množico $X \subseteq S$ in hkrati njen komplement $S \setminus X$ in zato zaradi zaprtosti filtrov za preseke tudi $\emptyset$.

Obratno: naj bo $\mathcal{F}$ filter, ki ni ultrafilter. Torej obstaja tak $X \subseteq S$, da velja $X, S \setminus X \notin \mathcal{F}$. Naj bo $\mathcal{G} := \mathcal{F} \cup \{X\}$. Pokažimo, da ima $\mathcal{G}$ lastnost končnih presekov, pri čemer moramo to lastnost preveriti samo tiste preseke, med katerimi je tudi X. Pa recimo, da obstajajo taki $X_i \in \mathcal{F}$, da je $\cap_{i=1}^{n} X_i \cap X = \emptyset$. Potem je $\cap_{i=1}^{n} X_i \subseteq S \setminus X$. Ker je $\cap_{i=1}^{n} X_i \in \mathcal{F}$, to velja tudi za $S \setminus X$, saj je $\mathcal{F}$ filter na S, kar pa po predpostavki ne drži. Po 3.34 lahko $\mathcal{G}$ razširimo do filtra $\mathcal{F}'$. Ker ta filter vsebuje tako $\mathcal{F}$ kot tudi $X \notin \mathcal{F}$, smo pokazali, da $\mathcal{F}$ ni maksimalen filer. □

En primer glavnega ultrafiltra, generiranega s singeltonom, smo že omenili. Ni težko videti, da je glavni filter ultrafilter natanko tedaj, ko je generiran s singeltonom. Za to, da se prepričamo, da obstajajo tudi neglavni ultrafiltri, pa bomo dokazali, da lahko vsak (med drugim neglavni) filter razširimo do ultrafiltra. Najprej bomo dokazali lemo.

Lema 3.37 ([6, izrek 11.2.5]). *Unija $\mathcal{C} := \cup C$ vsake neprazne naraščajoče verige filtrov C na množici S je tudi sama filter na S.*

Dokaz. Očitno je $\emptyset \notin \mathcal{C}$ in $S \in \mathcal{C}$. Za $X, Y \in \mathcal{C}$ naj bo $\mathcal{F} \in C$ tak filter, ki vsebuje X in Y in zato tudi njun presek $X \cap Y$. Torej velja $X \cap Y \in \mathcal{F} \subseteq \mathcal{C}$. Na enak se prepričamo, da za $\mathcal{C}$ velja tudi tretji aksiom za filtre. □

Izrek 3.38 ([6, izrek 11.2.5]). *Vsak filter $\mathcal{F}$ na S lahko razširimo do ultrafiltra $\mathcal{U} \supseteq \mathcal{F}$.*

Dokaz. Naj bo F množica vseh filtrov, ki vsebujejo $\mathcal{F}$, ki jih uredimo glede na vsebovanost. Po prejšnji lemi ima vsaka neprazna veriga v F zgornjo mejo, iz česar po Zornovi lemi sledi, da ima F maksimalen element $\mathcal{U}$. Po 3.36 je $\mathcal{U}$ zaradi maksimalnosti tudi ultrafilter. Ker je vsebovan v F, vsebuje $\mathcal{F}$. Trditev je dokazana. □

Naj bo S neskončna množica. Ultrafiltru $\mathcal{U}$, ki je razširitev filtra kokončnih množic na S, pravimo *ultrafilter kokončnih množic*.

3.4.2. *Ultraprodukti.* Naj bo $\mathcal{U}$ ultrafilter na neprazni množici I. Sedaj lahko definiramo ultraprodukt $\mathcal{L}$-struktur $U_i, i \in I$, kjer je $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \mathcal{K})$ jezik. Najprej na produktu vseh struktur $\Pi_{i\in I}U_i$, definiramo relacijo $\sim$:

$$(a_i)_{i\in I} \sim (b_i)_{i\in I} \Leftrightarrow \{i \in I \mid a_i = b_i\} \in \mathcal{U}.$$

Pokažimo, da je $\sim$ ekvivalenčna relacija na $\Pi_{i\in I}U_i$. Ker je $I \in \mathcal{U}$, je $(a_i)_{i\in I} \sim (a_i)_{i\in I}$ za vsak $(a_i)_{i\in I} \in \Pi_{i\in I}U_i$, torej je $\sim$ refleksivna relacija. Simetričnost je očitna, zato nam ostane še tranzitivnost: naj za $(a_i)_{i\in I}, (b_i)_{i\in I}$ in $(c_i)_{i\in I} \in \Pi_{i\in I}U_i$ velja $(a_i)_{i\in I} \sim (b_i)_{i\in I}$ in $(b_i)_{i\in I} \sim (c_i)_{i\in I}$. Množica $\{i \in I \mid a_i = c_i\}$ vsebuje presek $\{i \in I \mid a_i = b_i\} \cap \{i \in I \mid b_i = c_i\} \in \mathcal{U}$, torej je tudi sama v $\mathcal{U}$. Sledi $(a_i)_{i\in I} \sim (c_i)_{i\in I}$. $\sim$ je torej res ekvivalenčna relacija na $\Pi_{i\in I}U_i$.

Sedaj pokažimo, da lahko s pomočjo dane ekvivalenčne relacije iz $\mathcal{U}$ naredimo novo $\mathcal{L}$-strukturo. Na množici ekvivalenčnih razredov $\overline{(a_i)_{i\in I}} \in U := (\Pi_{i\in I}U_i)/\mathcal{U}$ definiramo za vsak $f \in \mathcal{F}$

$$f^U(\overline{(a_{1,i})_{i\in I}}, \ldots, \overline{(a_{n,i})_{i\in I}}) := \overline{(f^{U_i}(a_{1,i}, \ldots, a_{n,i}))_{i\in I}}.$$

Pokažimo, da je ta definicija neodvisna od izbranih predstavnikov $(a_{k,i})_{i\in I}$ ekvivalenčnih razredov $\overline{(a_{k,i})_{i\in I}}$. Če velja $(a_{k,i})_{i\in I} \sim (b_{k,i})_{i\in I}$ za vsak $1 \leq k \leq n$, je $\cap_{k=1}^n \{i \in I \mid a_{k,i} = b_{k,i}\} \in \mathcal{U}$. Ker je ta množica vsebovana v $\{i \in I \mid f^{U_i}(a_{1,i}, \ldots, a_{n,i}) = f^{U_i}(b_{1,i}, \ldots, b_{n,i})\}$ je tudi ta vsebovana v $\mathcal{U}$, iz česar sledi

$$(f^{U_i}(a_{1,i}, \ldots, a_{n,i}))_{i\in I} \sim (f^{U_i}(b_{1,i}, \ldots, b_{n,i}))_{i\in I}.$$

Torej je f^U res dobro definirana funkcija na ekvivalenčnih razredih.

Za n-kratni relacijski simbol $R \in \mathcal{R}$ pa definiramo relacijo R^U na U s predpisom

$$R^U(\overline{(a_{1,i})_{i\in I}}, \ldots \overline{(a_{n,i})_{i\in I}}) \Leftrightarrow \{i \in I \mid R^{U_i}(a_{1,i} \ldots, a_{n,i})\} \in \mathcal{U}.$$

Če je v tem primeru $(a_{k,i})_{i\in I} \sim (b_{k,i})_{i\in I}$ za vsak $1 \leq k \leq n$, je $\cap_{k=1}^n \{i \in I \mid a_{k,i} = b_{k,i}\} \in \mathcal{U}$. Množica $\{i \in I \mid (b_{1,i}, \ldots b_{k,i}) \in R^{U_i}\}$ vsebuje $\cap_{k=1}^n \{i \in I \mid a_{k,i} = b_{k,i}\} \cap \{i \in I \mid (a_{1,i}, \ldots, a_{k,i}) \in R^{U_i}\} \in \mathcal{U}$, zato je tudi sama v $\mathcal{U}$ in velja $R^U(\overline{(b_{1,i})_{i\in I}}, \ldots, \overline{(b_{n,i})_{i\in I}})$. Za vsak $c \in \mathcal{K}$ pa definiramo $c^U := \overline{(c^{U_i})_{i\in I}}$.

Pokazali smo, da je množica U z danimi funkcijami, relacijami in konstantami tudi sama $\mathcal{L}$- struktura. Tej strukturi pravimo *ultraprodukt* $\mathcal{L}$-struktur $(U_i)_{i\in I}$ glede na ultrafilter $\mathcal{U}$.

Sedaj bomo na podoben način kot zgoraj za množico $\{h_i \mid i \in I\}$ evaluacij na U_i definirali evaluacijo $\overline{(h_i)_{i\in I}} : \mathrm{Vbl} \to U$ na naslednji način: za spremenljivko v naj bo $\overline{(h_i)_{i\in I}}(v) := \overline{(h_i(v))_{i\in I}}$. Za $a = \overline{(a_i)}_{i\in I} \in U$ velja $\overline{(h_i)_{i\in I}}\binom{x}{a} = \overline{(h_i\binom{x}{a_i})_{i\in I}}$, in enako kot smo to storili za funkcije in relacije, lahko preverimo, da je enakost neodvisna od izbranega predstavnika ekvivalenčnega razreda za a. Z vsem, kar smo do sedaj definirali, lahko dokažemo Łošev izrek, še prej pa krajšo trditev.

Trditev 3.39. *Naj bo $U := (\Pi_{i\in I}U_i)/\mathcal{U}$ ultraprodukt $\mathcal{L}$-struktur U_i. Za vsak izraz t v jeziku $\mathcal{L}$ in vsako množico evaluacij $\{h_i \mid i \in I\}$ je $t^U[\overline{(h_i)_{i\in I}}] = \overline{(t^{U_i}[h_i])_{i\in I}}$*

Dokaz. Trditev dokažemo z indukcijo po kompleksnosti izraza t. Če je $t = c \in \mathcal{K}$, je po definiciji $t^U = c^U = \overline{(c^{U_i})}_{i\in I} = \overline{(t^{U_i})_{i\in I}}$. V tem primeru smo pokazali, da velja enakost, saj so vrednosti t^U in t^{U_i} neodvisne od evaluacij. Če je t spremenljivka, je $t^U[\overline{(h_i)_{i\in I}}] = \overline{(h_i)_{i\in I}}(v) = \overline{(h_i(v))_{i\in I}} = \overline{(t^{U_i}[h_i])_{i\in I}}$. Če pa je f n-mestni funkcijski

simbol, $t_1, \ldots, t_n$ pa $\mathcal{L}$-izrazi, je po definiciji f^U in indukcijski predpostavki

$$f(t_1, \ldots, t_n)^U[\overline{(h_i)_{i\in I}}] = f^U(t_1^U[\overline{(h_i)_{i\in I}}], \ldots, t_n^U[\overline{(h_i)_{i\in I}}])$$
$$= f^U(\overline{(t_1^{U_i}[h_i])_{i\in I}}, \ldots, \overline{(t_n^{U_i}[h_i])_{i\in I}}) = \overline{(f(t_1, \ldots, t_n)^{U_i}[h_i])_{i\in I}}.$$

Trditev je tako dokazana. □

Izrek 3.40 ([9, izrek 2.6.2]). *(Łoś) Naj bo $U := (\Pi_{i\in I}U_i)/\mathcal{U}$ ultraprodukt $\mathcal{L}$-struktur U_i. Potem za vsako množico evaluacij $\{h_i \mid i \in I\}$ in vsako $\mathcal{L}$-formulo Φ velja $U \models \Phi[\overline{(h_i)_{i\in I}}]$ natanko tedaj, ko je $\{i \in I \mid U_i \models \Phi[h_i]\} \in \mathcal{U}$. V posebnem za vsak stavek Φ velja $\mathcal{U} \models \Phi$ natanko tedaj, ko je množica $\{i \in I \mid U_i \models \Phi\} \in \mathcal{U}$.*

Dokaz. Izrek bomo pokazali z indukcijo po kompleksnosti $\mathcal{L}$-formule Φ.

Če je Φ oblike $t_1 \doteq t_2$, velja $U \models \overline{t_1 \doteq t_2[(h_i)_{i\in I}]}$ natanko tedaj, ko velja $t_1^U[\overline{(h_i)_{i\in I}}] = t_2^U[\overline{(h_i)_{i\in I}}]$ oz., po zgornji trditvi, $\overline{(t_1^{U_i}[h_i])_{i\in I}} = \overline{(t_2^{U_i}[h_i])_{i\in I}}$. To pa se zgodi natanko tedaj, ko je množica $\{i \in I \mid t_1^{U_i}[h_i] = t_2^{U_i}[h_i]\} = \{i \in I \mid U_i \models \Phi[h_i]\} \in \mathcal{U}$.

Če je Φ oblike $R(t_1, \ldots, t_n)$, je po definiciji $\mathcal{U} \models \overline{R(t_1, \ldots, t_n)[(h_i)_{i\in I}]}$ natanko tedaj, ko velja $R^U(t_1^U[\overline{(h_i)_{i\in I}}], \ldots, t_n^U[\overline{(h_i)_{i\in I}}])$. Upoštevajoč, da je za vsak $1 \leq k \leq n$ $t_k^U[\overline{(h_i)_{i\in I}}] = \overline{(t_k^{U_i}[h_i])_{i\in I}}$ in definicijo R^U, sledi, da se to zgodi natanko tedaj, ko je $\{i \in I \mid R^{U_i}(t_1, \ldots, t_n)[h_i]\} = \{i \in I \mid U_i \models \Phi[h_i]\} \in \mathcal{U}$.

Naj bo $\Phi = \neg\Psi$. Potem velja

$$\begin{aligned} U \models \Phi[\overline{(h_i)_{i\in I}}] &\Leftrightarrow U \not\models \Psi[\overline{(h_i)_{i\in I}}] \Leftrightarrow \{i \in I \mid U_i \models \Psi[h_i]\} \notin \mathcal{U} \\ &\Leftrightarrow I \setminus \{i \in I \mid U_i \models \Psi[h_i]\} \in \mathcal{U} \Leftrightarrow \{i \in I \mid U_i \not\models \Psi[h_i]\} \in \mathcal{U} \\ &\Leftrightarrow \{i \in I \mid U_i \models \Phi[h_i]\} \in \mathcal{U}. \end{aligned}$$

Če je Φ oblike $\Psi_1 \wedge \Psi_2$, velja

$$\begin{aligned} U \models \Phi[\overline{(h_i)_{i\in I}}] &\Leftrightarrow U \models \Psi_1[\overline{(h_i)_{i\in I}}] \text{ in } U \models \Psi_2[\overline{(h_i)_{i\in I}}] \\ &\Leftrightarrow \{i \in I \mid U_i \models \Psi_1[h_i]\} \in \mathcal{U} \text{ in } \{i \in I \mid U_i \models \Psi_2[h_i]\} \in \mathcal{U} \\ &\Leftrightarrow \{i \in I \mid U_i \models \Psi_1[h_i]\} \cap \{i \in I \mid U_i \models \Psi_2[h_i]\} \in \mathcal{U} \\ &\Leftrightarrow \{i \in I \mid U_i \models (\Psi_1 \wedge \Psi_2)[h_i]\} \in \mathcal{U} \\ &\Leftrightarrow \{i \in I \mid U_i \models \Phi[h_i]\} \in \mathcal{U}. \end{aligned}$$

Recimo, da je Φ oblike $\forall x\Psi$. Potem je $U \models \Phi[\overline{(h_i)_{i\in I}}]$ natanko tedaj, ko je $U \models \Psi[\overline{(h_i)_{i\in I}}\binom{x}{a}]$ za vsak $a \in U$ oz., kot smo premislili zgoraj ob definiciji evaluacije $\overline{(h_i)_{i\in I}}$, $U \models \Psi[\overline{(h_i)_{i\in I}\binom{x}{(a_i)_{i\in I}}}]$ za vsak $(a_i)_{i\in I} \in \Pi_{i\in I}U_i$. To se po indukcijski predpostavki zgodi natanko tedaj, ko je za vsak $(a_i)_{i\in I} \in \Pi_{i\in I}U_i$ množica $\{i \in I \mid U_i \models \Psi[h_i\binom{x}{a_i}]\} \in \mathcal{U}$.

Slednje velja natanko tedaj, ko je množica $\{i \in I \mid U_i \models \Psi[h_i\binom{x}{a_i}]$ za vse $a_i \in U_i\} \in \mathcal{U}$. Res: naj bo $A := \{i \in I \mid U_i \models \Psi[h_i\binom{x}{a_i}]$ za vse $a_i \in U_i\} = \{i \in I \mid U_i \models \forall x\Psi[h_i]\} \in \mathcal{U}$. Potem je za vsak $(a_i)_{i\in I} \in \Pi_{i\in I}U_i$ množica $A \subseteq \{i \in I \mid U_i \models \Psi[h_i\binom{x}{a_i}]\}$. Če je $A \in \mathcal{U}$, potem to velja tudi za vse množice $\{i \in I \mid U_i \models \Psi[h_i\binom{x}{a_i}]\}$, s čimer smo dokazali implikacijo iz desne v levo.

Za dokaz obratne smeri pa predpostavimo, da velja $A \notin \mathcal{U}$, zato je njen komplement $V := \{i \in I \mid U_i \not\models \Psi[h_i\binom{x}{a_i}]$ za nek $a_i \in U_i\} \in \mathcal{U}$. Definiramo $(b_i)_{i\in I} \in \Pi_{i\in I}U_i$:

če je $i \in V$, naj bo $b_i \in U_i$ tak, da velja $U_i \not\models \Psi[h_i\binom{x}{b_i}]$, sicer pa naj bo b_i poljuben. Torej je $V = \{i \in I \mid U_i \not\models \Psi[h_i\binom{x}{b_i}]\}$. Ker je $V \in \mathcal{U}$, to velja tudi za $\{i \in I \mid U_i \not\models \Psi[h_i\binom{x}{b_i}]\}$, in zato komplement te množice $\{i \in I \mid U_i \models \Psi[h_i\binom{x}{b_i}]\}$ ni v $\mathcal{U}$. Potem ne velja, da je $\{i \in I \mid U_i \models \Psi[h_i\binom{x}{a_i}]\} \in \mathcal{U}$ za vsak $(a_i)_{i\in I} \in \Pi_{i\in I}U_i$.

Ker pa za vsak $i \in I$ velja $U_i \models \Psi[h_i\binom{x}{a_i}]$ za vse $a_i \in U_i$ natanko tedaj, ko velja $U_i \models \forall x\Psi[h_i]$, smo pokazali, da je $\{i \in I \mid U_i \models \Psi[h_i\binom{x}{a_i}]$ za vse $a_i \in U_i\} = \{i \in I \mid U_i \models \forall x\Psi[h_i]\} = \{i \in I \mid U_i \models \Phi\}$. S tem je dokazana ekvivalenca iz izreka tudi v zadnjem primeru. □

Omenimo še, da so za raziskovanje zanimivi zgolj ultraprodukti nad neglavnimi ultrafiltri. Če si namreč ogledamo ultrafilter $\mathcal{F} := \{X \subseteq I \mid \{i\} \subseteq X\}$ za nek $i \in I$ in je U ultraprodukt struktur U_i glede na $\mathcal{F}$, ni težko videti, da za vsako množico valuacij $(h_i)_{i\in I}$ na U_i in vsako $\mathcal{L}$-formulo velja $U \models \Phi[\overline{(h_i)_{i\in I}}]$ natanko tedaj, ko velja $U_i \models \Phi[h_i]$. Torej je ultraprodukt elementarno ekvivalenten enemu od modelov, ki ga sestavljajo. Enako nezanimiv je ultraprodukt množice elementarno ekvivalentnih struktur nad poljubnim ultrafiltrom, saj za vsak stavek velja, da velja bodisi v vseh strukturah bodisi v nobeni, iz česar sledi, da je ultraprodukt elementarno ekvivalenten strukturam, ki ga sestavljajo.

Mi bomo kasneje obravnavali valuacijski polji $\cap_{p\in\mathbb{P}}\mathbb{Q}_p/\mathcal{P}$ in $\cap_{p\in\mathbb{P}}\mathbb{Z}_p((t))/\mathcal{P}$, kjer bo $\mathcal{P}$ ultrafilter nad filtrom kokončnih množic na množici praštevil $\mathbb{P}$. V naslednjem poglavju bomo pokazali, da sta ti dve valuacijski polji elementarno ekvivalentni.

4. Izrek Ax-Kochen-Eršov

V tem poglavju bomo, tako kot smo to naredili že prej, polje z valuacijo označili s parom $(K, \mathcal{O})$, kjer bo $\mathcal{O}$ pripadajoč valuacijski kolobar. Jezik polj z valuacijami, ki ga bomo označili s $\mathcal{K} = (+, \cdot, -, ^{-1}, V)$, bo isti, kot smo ga definirali v tretjem poglavju. Za lažje branje dodajmo samo oznako $V^\times(x)$, ki bo za izraz x označevala formulo $V(x) \wedge \exists y(yz \doteq 1 \wedge V(y))$. Formula $V^\times(x)$ bo torej označevala lastnost "biti obrnljiv element v valuacijskem kolobarju".

Lema 4.1 ([9, 4.6.0.1])**.** *Naj bo $(K, \mathcal{O})$ κ-nasičeno polje z valuacijo. Potem sta κ-nasičena tudi pripadajoča valuacijska grupa Γ in polje ostankov $\overline{K}$.*

Dokaz. Lemo bomo dokazali tako, da bomo najprej vsak stavek v jeziku urejenih abelovih grup in polj prevedli na stavek v jeziku polj z valuacijami.

Za formulo Φ v jeziku polj ostankov bomo z indukcijo definirali formulo Φ_r, ki bo označevala njen prevod v jezik valuacij:

(1) $(t_1 \doteq t_2)_r := V(t_1 - t_2) \wedge \neg V^\times(t_1 - t_2)$,
(2) $(\neg\Phi)_r := \neg\Phi_r$,
(3) $(\Phi_1 \wedge \Phi_2)_r := \Phi_{1r} \wedge \Phi_{2r}$,
(4) $(\forall x\Phi) := \forall x(V(x) \to \Phi_r)$.

Po konstrukciji je jasno, da ima formula Φ_r enake proste spremenljivke kot Φ. Lahko se prepričamo (edino, kar je treba storiti, je to, da prevedemo levo in desno stran iz formalnega v naravni jezik in se potem prepričamo o enakosti), da velja za vsako polje z valuacijo $(K, \mathcal{O})$ in pripadajoče polje ostankov $\overline{K}$ ekvivalenca $\widetilde{\overline{K}} \models \Phi(v_0/c_{\overline{a_0}}, \ldots, v_n/c_{\overline{a_n}}) \iff \widetilde{(K, \mathcal{O})} \models \Phi_r(v_0/c_{a_0}, \ldots, v_n/c_{a_n})$, kjer je Φ formula s prostimi spremenljivkami $v_0, \ldots, v_n$ in $a_i \in K$. Tu smo seveda naredili konstantno razširitev tako jezika polja ostankov kot tudi jezika polj z valuacijami s primernimi konstantnimi simboli.

Sedaj definiramo še prevod stavkov Φ v jeziku urejenih abelovih grup na formule Φ_g v jeziku polj z valuacijo:

(1) $(t_1 \doteq t_2)_g := \exists x(V^\times(x) \wedge xt_1 \doteq t_2)$,
(2) $(t_1 < t_2)_g := \exists x(V(x) \wedge \neg V^\times(x) \wedge xt_1 \doteq t_2)$,
(3) $(\neg\Phi)_g := \neg\Phi_g$,
(4) $(\Phi_1 \wedge \Phi_2)_g := \Phi_{1g} \wedge \Phi_{2g}$,
(5) $(\forall x\Phi) := \forall x(x \neq 0 \to \Phi_g)$.

Tukaj na urejeno abelovo grupo gledamo kot na kvocient multiplikativne grupe $K^\times$, kot smo ga definirali v dokazu izreka 2.12. Zato smo tudi uporabili multiplikativen zapis. Vidimo, da imata Φ in Φ_g enake proste spremenljivke. Enako kot zgoraj se lahko z indukcijo po konstrukciji formule Φ z enakimi prostimi spremenljivkami kot zgoraj prepričamo, da velja $\widetilde{\Gamma} \models \Phi(c_{a_0\mathcal{O}^\times}/v_0, \ldots, c_{a_0\mathcal{O}^\times}/v_n) \iff \widetilde{(K, \mathcal{O})} \models \Phi_g$ za vse $a_i \in K$.

Če je $\Sigma(x)$ tip $\overline{K}$, v čigar formulah nastopajo konstantni simboli $c_{\overline{a}}$ za $\overline{a} \in A \subseteq \overline{K}$, $|A| < \kappa$, potem je $\Sigma_r(x) := \{\Phi_r \mid \Phi \in \Sigma(x)\} \cup \{V(x)\}$ tip $(K, \mathcal{O})$, v katerem nastopajo konstantni simboli c_a, pripadajoči (glede na praslike kvocientne preslikave iz $\mathcal{O}$ v $\overline{K}$) $a \in \mathcal{O}$, ki jih je očitno prav tako manj kot κ. Po κ-nasičenosti $(K, \mathcal{O})$ sledi, da obstaja $a \in K$, ki izpolnjuje $\Sigma_r(x)$. Ta a mora biti vsebovan v $\mathcal{O}$, saj realizira formulo $V(x)$. Po definiciji formul Φ_r glede na Φ sledi, da $\overline{a} \in \overline{K}$ izpolnjuje $\Sigma(x)$. Ugotovili smo, da je tudi $\overline{K}$ κ-nasičeno.

V primeru urejenih abelovih grup sklepamo povsem analogno. □

Iz konstrukcije prevedbe formul iz jezika urejenih abelovih grup oz. polj v dokazu sledi, da iz elementarne ekvivalence polj z valuacijo sledi elementarna ekvivalenca pripadajočih valuacijskih grup in polj ostankov, pa tudi, da je valuacijska grupa oz. polje ostankov ultraprodukta polj z valuacijo elementarno ekvivalenten ultraproduktu pripadajočih valuacijskih grup oz. polj ostankov. Sedaj smo pripravljeni, da dokažemo izrek Ax-Kochen-Jeršov.

Izrek 4.2. *(Ax-Kochen, Jeršov)* [10] *Naj bo $(K, \mathcal{O})$ Henselovo polje z valuacijo s pripadajočo valuacijsko grupo Γ in poljem ostankov $\overline{K}$, ki ima karakteristiko 0. Če velja $(K, \mathcal{O}) \subseteq (K_1, \mathcal{O}_1)$ za polje z valuacijo $(K_1, \mathcal{O}_1)$ z urejeno abelovo grupo Γ_1 in poljem ostankov $\overline{K}_1$ in je:*

(1) *urejena abelova grupa Γ eksistencialno zaprta v Γ_1,*
(2) *polje $\overline{K}$ eksistencialno zaprto v $\overline{K}_1$,*

potem je polje z valuacijo $(K, \mathcal{O})$ eksistencialno zaprto v $(K_1, \mathcal{O}_1)$.

Dokaz. Ker sta pri henselizaciji polja z valuacijo dobljena valuacijska grupa in polje ostankov enaka, lahko brez izgube splošnosti predpostavimo, da je tudi $(K_1, \mathcal{O}_1)$ Henselovo (sicer ga nadomesimo z njegovo henselizacijo). Naj bo $\kappa := |K_1| \geq |K|$. Ker je jezik polj z valuacijami števen, po 3.25 obstaja κ^+-nasičena elementarna razširitev $(K, \mathcal{O})$, ki jo označimo s $(K_2, \mathcal{O}_2)$. Ker je $(K, \mathcal{O})$ Henselovo, to velja tudi za $(K_2, \mathcal{O}_2)$. Pokazali bomo, da je (v razširjenem jeziku polj z dodanimi konstantnimi simboli c_a za $a \in K$) strukturo $((K_1, \mathcal{O}_1), K)$ mogoče vložiti v $((K_2, \mathcal{O}_2), K)$. Po posledici 3.29 bo sledilo, da je $(K, \mathcal{O})$ eksistencialno zaprt v $(K_1, \mathcal{O}_1)$.

Po 4.1 sta tudi polje $\overline{K}_2$ in Γ_2, valuacijska grupa $(K_2, \mathcal{O}_2)$, κ^+-nasičeni. Po 3.29 velja:

- Strukturo $\overline{K_1}$ v jeziku polj, razširjenem s konstantami $\overline{K}$, lahko vložimo v $\overline{K_2}$ v istem jeziku. To sledi iz predpostavke, da je $\overline{K}$ eksistencialno zaprt v $\overline{K}_2$.
- Strukturo Γ_1 v jeziku polj, razširjenem s konstantami Γ, lahko vložimo v Γ_2 v istem jeziku.

To pomeni, da lahko razširimo vložitev $\tau : \overline{K} \to \overline{K}_2$ do vložitve $\tau_1 : \overline{K}_1 \to \overline{K}_2$, vložitev $\sigma : \Gamma \to \Gamma_2$ pa do vložitve $\sigma_1 : \Gamma_1 \to \Gamma_2$. Vse naštete preslikave so konstantne na $\overline{K}$ oz. Γ. Če $\overline{K}_1$ in Γ_1 izenačimo z njunima slikama glede na τ_1 oz. σ_1 (to lahko storimo zaradi njihove izomorfnosti in posledične elementarne ekvivalentnosti), lahko brez škode za splošnost predpostavimo, da velja $\overline{K}_1 \subseteq \overline{K}_2$ in $\Gamma_1 \subseteq \Gamma_2$. Sedaj imamo polja z valuacijami $(K, \mathcal{O}), (K_1, \mathcal{O}_1)$ in $(K_2, \mathcal{O}_2)$, za katera velja:

(1) $(K, \mathcal{O}), (K_1, \mathcal{O}_1)$ in $(K_2, \mathcal{O}_2)$ so Henselova,
(2) $(K, \mathcal{O}) \subseteq (K_1, \mathcal{O}_1)$ in $(K, \mathcal{O}) \subseteq (K_2, \mathcal{O}_2)$,
(3) $\overline{K} \subseteq \overline{K_1} \subseteq \overline{K_2}$,
(4) $\Gamma \subseteq \Gamma_1 \subseteq \Gamma_2$, pri čemer je Γ_1/Γ brez torzije.

Zadnji navedeni pogoj sledi iz v izreku predpostavljene eksistencialne zaprtosti Γ v Γ_2. Pa recimo, da obstaja tak $\gamma \in \Gamma_1 \setminus \Gamma$, da je $\delta := n\gamma \in \Gamma$. Potem velja $(\Gamma_1, \Gamma) \models \exists x\ nx = c_\delta$ in zato, po eksistencialni zaprtosti Γ v Γ_1, $(\Gamma, \Gamma) \models \exists x\ nx \doteq c_\delta$. Torej je $\delta = n\gamma'$ za nek $\gamma' \in \Gamma$, zato je $\gamma = \gamma' \in \Gamma$.

Pokazali bomo, da je pri navedenih pogojih vložitev $(K, \mathcal{O})$ v $(K_2, \mathcal{O}_2)$ mogoče razširiti do vložitve $\tau : (K_1, \mathcal{O}_1) \to (K_2, \mathcal{O}_2)$, torej take vložitve polj, ki bo ohranjala valuacijo. Z drugimi besedami, za dobljeni τ bo veljalo $v_2 \circ \tau = v_1$. Naj bo $(K', \mathcal{O}') \subseteq (K_1, \mathcal{O}_1)$ maksimalno tako polje z valuacijo, ki ga je mogoče vložiti v $(K_2, \mathcal{O}_2)$ in za katerega veljajo pogoji (1)-(4), kjer ima $(K', \mathcal{O}')$ vlogo $(K, \mathcal{O})$. Obstoj

takega polja z valuacijo sledi iz Zornove leme. Množica vseh takih polj z valuacijo je namreč neprazna, saj vsebuje $(K, \mathcal{O})$. Tu tudi implicitno uporabimo posledico Chevalleyevega izreka 2.40, po katerem lahko vsaki razširitvi polja priredimo tudi razširitev valuacije. Pokazali bomo, da je $(K', \mathcal{O}') = (K_1, \mathcal{O}_1)$. Pa recimo, da to ne velja. Ločili bomo tri primere. V vseh treh bomo s $(K', \mathcal{O}')$ označevali tudi vložitev tega polja v $(K_2, \mathcal{O}_2)$. Pripadajočo valuacijo, valuacijsko grupo in polje ostankov bomo označili z v', Γ' in $\overline{K'}$.

V prvem primeru predpostavimo, da velja $\overline{K'} \neq \overline{K_1}$. Najprej privzemimo, da obstaja $\overline{x_1} \in \overline{K_1} \setminus \overline{K'}$, ki je transcendenten nad $\overline{K'}$. Ker velja $\overline{K_1} \subseteq \overline{K_2}$, obstaja tak $x_2 \in \mathcal{O}_2$, da velja $\overline{x_1} = \overline{x_2}$. Iz 2.43 sledi, da sta transcendentni tudi razširitvi $K'(x_i) \mid K'$ za $i = 1, 2$. Po trditvi 2.52 za $i = 1, 2$ zato obstaja natanko določena valuacija v_i na $K'(x_i) \subseteq K_i$, ki na K' ohranja valuacijo v' in za katero je grupa ostankov enaka Γ', polje ostankov pa $\overline{K'}(\overline{x_1}) \cong \overline{K'}(\overline{x_2})$. Spomnimo, da za tak v_i velja $v_i(\sum_{j=0}^{n} a_j x^j) = \min_{0 \leq i \leq n} v_i(a_j)$. Sedaj lahko vložitev $K' \subseteq K_1$ v $K' \subseteq K_2$ razširimo do vložitve $\tau : K'(x_1) \to K_2$, in sicer tako, da je $\tau(a) = a$ za $a \in K'$ in $\tau(x_1) = x_2$. Slika τ je seveda $K'(x_2)$, za τ pa očitno velja $v_2 \circ \tau = v_1$. Sedaj polji $K'(x_1)$ in $K'(x_2)$ razširimo do njunih henselizacij. Te so po izreku 2.58 vsebovane v K_1 oz. K_2, zaradi njihove enoličnosti pa lahko vložitev τ razširimo še iz henselizacije $K'(x_1)$ na henselizacijo $K'(x_2)$. Izomorfna slika henselizacije polja je namreč očitno henselizacija izomorfne slike, pa tudi polji ostankov in urejeni abelovi grupi ostaneta enaki. Tudi razširjena vložitev ohranja vrednosti valuacij, kar sledi iz enoličnosti henselizacij. Tako smo dobili vložitev polja $(K', \mathcal{O}') \subsetneq (K'', \mathcal{O}'') \subseteq (K_1, \mathcal{O}_1)$ v $(K_2, \mathcal{O}_2)$, za katero velja (1)-(4), kjer ima $(K', \mathcal{O}')$ vlogo $(K, \mathcal{O})$. To pa je v nasprotju z maksimalnostjo $(K', \mathcal{O}')$.

Sedaj predpostavimo, da obstaja $\overline{x} \in \overline{K_1} \setminus \overline{K'}$, ki je algebraičen nad $\overline{K'}$. Naj bo $\overline{p} \in \overline{K'}[x]$ minimalen enični polinom za x. Ker ima $\overline{K_1}$ karakteristiko nič, je $\overline{x}$ enostavna ničla $\overline{p}$[2]. Ker je $(K_1, \mathcal{O}_1)$ Henselovo, potem obstaja tak $x_1 \in \mathcal{O}_1$, da je x_1 ničla p in $\overline{x_1} = \overline{x}$. Brez škode za splošnost privzamemo, da ima p isto stopnjo kot $\overline{p}$, sicer izbrišemo vodilni koeficient, ki je v $\mathcal{M}'$. Če valuacijo v_1 omejimo na $K'(x_1)$, je pripadajoča valuacijska grupa izomorfna Γ', polje ostankov pa $\overline{K'}(\overline{y})$. To sledi iz enačbe $ef \leq n$ v izreku 2.46 in dejstva, da je stopnja razširitve $[\overline{K'}(\overline{x_1}) : \overline{K'}]$ enaka $[K'(x_1) : K']$. Enak sklep naredimo v sliki $K' \subseteq K_2$. Ker je tudi K_2 Henselovo, obstaja $x_2 \in K_2$, ki je enostavna ničla p v K_2. Enako kot zgoraj v_2 omejimo na $K_2(x_2)$ in dobimo vložitev $\tau : K'(x_1) \to K'(x_2)$, ki je kot razširitev vložitve $(K', \mathcal{O}')$ konstantna na $(K, \mathcal{O})$. Tako kot prej je $\tau(a) = a$ za vsak $a \in K'$ in $\tau(x_1) = x_2$. Ker sta x_1 in x_2 obe enostavni ničli istega polinoma p, je vložitev dobro definirana in ohranja vrednosti valuacij. Če namesto $K'(x_i)$ za $i = 1, 2$ vzamemo njuni henselizaciji v K_1 oz. K_2, se dobljena vložitev enolično razširi, s čimer spet pridemo v protislovje s predpostavko o maksimalnosti $(K', \mathcal{O}')$ kot polja, ki izpolnjuje (1)-(4) v vlogi $(K, \mathcal{O})$. Prišli smo do sklepa, da mora veljati $\overline{K'} = \overline{K_1}$.

V drugem primeru predpostavimo, da velja $\overline{K'} = \overline{K_1}$ in $\Gamma' \neq \Gamma_1$. Naj bo $\gamma \in \Gamma_1 \setminus \Gamma'$ in $x \in K_1$ tak, da je $v_1(x) = \gamma$. Ker je Γ_1/Γ' po predpostavki brez torzije, je $\Gamma' \oplus \mathbb{Z}\gamma$ direktna vsota. Potem po trdtivi 2.51 obstaja enolična razširitev valuacije v' na K', da je $v'(a_n x^n + \cdots a_1 x + a_0) = \min_{0 \leq i \leq n}(v(a_i) + i\gamma)$. Za $(K'(x), \mathcal{O}_1')$, kjer je $\mathcal{O}_1' = K'(x) \cap \mathcal{O}_1$, po isti trditvi velja, da je pripadajoča grupa ostankov enaka $\Gamma' \oplus \mathbb{Z}\gamma$, polje ostankov pa je očitno enako $\overline{K_1} = \overline{K}$. Ker je $\Gamma' \oplus \mathbb{Z}\gamma$ taka razširitev Γ', da je indeks $[\Gamma' \oplus \mathbb{Z}\gamma : \Gamma']$ neskončen, po 2.43 sledi, da je $x \in K_1$ transcendenten nad

[2]Spomnimo, da so vsa polja s karakteristiko nič perfektna.

K'. Da pridemo do protislovja z maksimalnostjo vložitve $(K', \mathcal{O}')$, bomo $(K'(x), \mathcal{O}'')$ razširili do polja z valuacijo $(K'', \mathcal{O}'')$, da bo za pripadajočo valuacijsko grupo Γ'' veljalo, da je Γ_1/Γ'' brez torzijskega dela.

Predpostavimo, da za Γ_1', valuacijsko grupo $(K'(x), \mathcal{O}_1')$ velja, da ima Γ_1/Γ_1' element končnega reda. Potem obstajata tak $\delta \in \Gamma_1 \setminus \Gamma_1'$ in praštevilo q, da je $q\delta \in \Gamma_1'$. Izberimo $a \in K'(x)$, da velja $v_1'(a) = q\delta$ in $y \in K_1^\times$, da je $v_1(y) = \delta$. Tu je v_1' valuacija, ki pripada na $(K'(x), \mathcal{O}_1')$. Potem je $v_1(y^q a^{-1}) = q\delta - q\delta = 0$, torej je $y^q a^{-1} \in \mathcal{O}_1^\times$. Ker je po predpostavki $\overline{K_1} = \overline{K'} = \overline{K'(x)}$, obstaja tak $c \in K'(x)$, da je $\bar{c} = \overline{y^q a^{-1}}$ oz. $\overline{y^q a^{-1} c^{-1}} = \bar{1}$. Ker je karakteristika $\overline{K_1}$ enaka nič, ima zato polinom $x^q - \overline{y^q a^{-1} c^{-1}} \in \overline{K_1}$ enostavno ničlo $\bar{1}$ v $\overline{K_1}$. Ker je K_1 Henselovo, obstaja ničla z polinoma $x^q - y^q a^{-1} c^{-1}$ v K_1. Za z velja $z^q = y^q a^{-1} c^{-1} \in O_1^\times$, zato je tudi $z \in \mathcal{O}_1^\times$. Zato velja $ac = (yz^{-1})^q$ in ker sta a, c po predpostavki vsebovana v $K'(x)$, sledi, da je $K'(x, yz^{-1})$ algebraična razširitev K'. Pripadajoča valuacijska grupa vsebuje $v_1(yz^{-1}) = v_1(y) - v_1(z) = \delta$. Tako smo dobili razširitev $(K'(x), \mathcal{O}_1')$ na polje z valuacijo $(K'(x, yz^{-1}), \mathcal{O}_1'')$, $\mathcal{O}_1'' = \mathcal{O}_1 \cap K'(x, yz^{-1})$, čigar valuacijska grupa Γ_1'' vsebuje δ. Neformalno lahko sklepamo, da ima Γ_1/Γ_1'' najmanj en torzijski element manj kot Γ_1/Γ_1'. Ta postopek ponavljamo, dokler ne pridemo do razširitve $(K'(x), \mathcal{O}_1') \subseteq (K'', \mathcal{O}'') \subsetneq (K_1, \mathcal{O}_1)$, za katero je Γ_1/Γ'' brez torzije. Tu uporabimo transfinitno indukcijo, pri kateri moramo postopek ponoviti kvečjemu $|\Gamma_1/\Gamma_1'|$ - krat.

Sedaj želimo pokazati, da lahko $(K'', \mathcal{O}'')$ vložimo v $(K_2, \mathcal{O}_2)$. Ker je slednje po predpostavki $|K_1|^+$-nasičeno in velja $|K''| \leq |K_1|$, bo dovolj, če pokažemo, da lahko vsako končno razsežno razširitev polja $K^* \mid K'(x)$, $K^* \subseteq K''$ vložimo v K_2. V to se prepričamo tako, če zadnji stavek prevedemo v jezik logike in vidimo, da take končne razširitve polj $K^* \mid K'(x)$ ustrezajo končno generiranim $\mathcal{K}_{K'(x)}$-podstrukturam $((K'', \mathcal{O}''), K'(x))$ in uporabimo 3.29. Še več - ker je vsaka končno razsežna razširitev K rezultat končno mnogo razširitev K z enim elementom, se lahko omejimo na primer, ko je $K^* = K'(x, y)$ za nek $y \in K''$, algebraičen nad $K'(x)$. Potem za Γ^*, valuacijsko grupo $(K^*, \mathcal{O}^*)$, velja $[\Gamma^* : \Gamma' \oplus \mathbb{Z}\gamma] < \infty$. Spomnimo, da je $\gamma = v_1(x)$. Γ^* ne more biti direktna vsota oblike $\Gamma' \oplus \mathbb{Z}\gamma \oplus \mathbb{Z}\gamma'$, saj bi za $\gamma' \in \Gamma_1$ moral obstajati n, da je $n\gamma' \in \Gamma' \oplus \mathbb{Z}\gamma$, torej bi za nek $m \in \mathbb{Z}$, $\delta \in \Gamma$ veljalo $n\gamma' = \delta + m\gamma$ in zato $n\gamma' - m\gamma \in \Gamma'$. Če ne velja $n\gamma' = m\gamma$, pridemo v nasprotje s predpostavko, da je Γ_1/Γ' brez torzije. V nasprotnem primeru dobimo $\gamma' \in \mathbb{Z}\gamma$ ali $\gamma \in \mathbb{Z}\gamma'$. Sklepamo lahko torej, da je Γ^* oblike $\Gamma' \oplus \mathbb{Z}\gamma_1$ za nek $\gamma_1 \in \Gamma_1$. Izberimo $x_1 \in K^*$, za katerega velja $v_1(x_1) = \gamma_1$. Potem je $(K^*, \mathcal{O}^*)$ neposredna razširitev $(K'(x_1), \mathcal{O}_1')$, kjer je $\mathcal{O}_1' := \mathcal{O}_1 \cap K'(x_1)$. Valuacijski grupi sta namreč enaki, vsa polja ostankov pa so izomorfna $\overline{K'} = \overline{K_1}$. Na $(K'(x_1), \mathcal{O}_1')$ lahko, spet po 2.51, definiramo valuacijo $v_1'(a_n x_1^n + \ldots + a_0) := \min_{0 \leq i \leq n}\{v(a_i) + i\gamma_1\}$. Pripadajoča valuacijska grupa je tako $\Gamma' \oplus \mathbb{Z}\gamma_1$.

Sedaj naj bo $x_2 \in K_2$ tak, da velja $v_2(x_2) = \gamma_1$ (tak $x_2 \in K_2$ obstaja, ker je $\Gamma_1 \subseteq \Gamma_2$). Ker po enoličnosti razširitve v na $K'(x_2)$ po 2.51 sledi, da je $v_2(a_m x_2^n + \cdots a_0) = \min_{0 \leq i \leq n}\{v(a_i) + i\gamma_1\}$, lahko vložitev K' v K_2 razširimo do vložitve $K'(x_1)$ v K_2, ki ohranja vrednost valuacije - tako kot prej naj bo $\tau(a) = a$ za vsak $a \in K$ in $\tau(x_1) = x_2$. Tu smo implicitno uporabili dejstvo, da je po 2.43 $x_i \in K_i$ transcendenten nad K' za $i = 1, 2$.

Tako kot prej izomorfizrm, ki slika $K'(x_1)$ v $K'(x_2)$, razširimo do izomorfizma njunih henselizacij. Ker je po 2.60 henselizacija $(K'(x_1), \mathcal{O}_1')$ maksimalna neposredna algebraična razširitev $(K'(x_1), \mathcal{O}_1')$, skepamo, da vsebuje K^*. Povedali smo že namreč, da je $(K^*, \mathcal{O}^*)$ neposredna razširitev $(K'(x_1), \mathcal{O}_1')$. Ker je $K^* = K'(x, y)$

algebraičen nad K', zaradi česar je algebraičen tudi nad $K'(x_1)$. Sledi, da lahko $(K^*, \mathcal{O}^*)$ kot podpolje henselizacije $(K'(x_1), \mathcal{O}_1')$ vložimo v $(K_2, \mathcal{O}_2)$ tako, da za vložitev τ velja $v_2 \circ \tau = v_1$.

Premislili smo, da lahko $(K'', \mathcal{O}'')$ vložimo v $(K_2, \mathcal{O}_2)$. Da pridemo do protislovja s predpostavko o maksimalnosti K', tako kot zgoraj spet preidemo iz $(K'', \mathcal{O}'')$ na njegovo henselizacijo. Tako smo ugovorili, da mora veljati $\Gamma' = \Gamma_1$.

V tretjem primeru pa predpostavimo $\overline{K'} = \overline{K_1}$, $\Gamma' = \Gamma_1$ in $K' \neq K_1$. Posebej velja, da je $(K_1, \mathcal{O}_1)$ neposredna razširitev $(K', \mathcal{O}')$.

Zaradi maksimalnosti $(K', \mathcal{O}')$ lahko predpostavimo, da je Henselovo, sicer vzamemo njegovo henselizacijo. Ker je po 2.60 henselizacija maksimalna algebraična neposredna razširitev, za vsak $x_1 \in K_1 \setminus K'$ velja, da je transcendenten. Pokazali bomo, da tudi v tem primeru pridemo do protislovja.

Naj bo $x_1 \in K_1$ torej transcendenten nad K'. Najprej pokažimo, da obstaja tak $x_2 \in K_2$, da za vsak $a \in K'$ velja $v_1(a - x_1) = v_2(a - x_2)$. Naj bo za vsak $a \in K'$ $x_a \in K'$ tak, da je $v_1(a - x_1) = v_1(x_a) = v_2(x_a)$. Tak $x_a \in K'$ obstaja, ker je $\Gamma' = \Gamma_1$.

Definiramo množico $\mathcal{L}_{K'}$-formul s prosto spremenljivko x:

$$\Sigma(x) := \{V^\times((c_a - x)c_{x_a^{-1}}) \mid a \in K'\}.$$

Želimo poiskati tak $x_2 \in K_2$, ki bo izpolnjeval $\Sigma(x)$. Za njega bo namreč za vsak $a \in K'$ veljalo :

$$(a - x_2)x_a^{-1} \in \mathcal{O}_2^\times \Rightarrow v_2(a - x_2) = v_2(x_a) = v_1(a - x_1).$$

Ker je $|K'| \leq |K_1|$, K_2 pa je $|K_1|^+$ nasičeno, bo dovolj preveriti, da za vsako končno podmožico $\Sigma(x)$ obstaja nek $y \in K_2$, ki jo izpolnjuje.

Z drugimi besedami, za vsak končen nabor $a_1, \ldots, a_n \in K'$ želimo poiskati tak $y \in K_2$, da velja $v_1(a_i - x_1) = v_1(x_{a_i}) = v_2(x_{a_i}) = v_2(a_i - y)$ za $1 \leq i \leq n$.

Naj bo $a \in \{a_1, \ldots, a_n\}$ tak, da je $v_1(a - x_1) = \max_{1 \leq i \leq n} v_1(a_i - x_1)$, in naj bodo $b_i \in K'$ taki, da je $v_1(b_i) = v_1(a_i - x_1)$ za $1 \leq i \leq n$. Naj bo $b := b_i$, kjer za i velja $v_1(a_i - x_1) = v_1(a - x_1)$. Očitno je $v_1(\frac{a-x_1}{b}) = 0$, in ker je $\overline{K_1} = \overline{K'}$, obstaja tak $c \in K'$, da je $\bar{c} = \overline{\frac{a-x_1}{b}}$, iz česar sledi $v_1(\frac{a-x_1}{b} - c) > 0$ (saj je $\overline{\frac{a-x_1}{b} - c} = 0$), torej je $v_1(x_1 - a - bc) > v_1(b) = v_1(x_1 - a)$. Definiramo $y := a + bc \in K'$. Za y in vsak $1 \leq i \leq n$ velja $v_1(x_1 - y) > v_1(x_1 - a) \geq v_1(x_1 - a_i)$. Sledi $v_1(y - a_i) = v_1((x_1 - y) - (x_1 - a_i)) = v_1(x_1 - a_i)$ za vsak i. Ker je $y \in K' \subseteq K_2$, smo našli tak $y \in K_2$, ki zadošča enakostim $v_2(a_i - y) = v_1(a_i - x_1) = v_1(b_i)$ za $1 \leq i \leq n$.

Kot smo razmislili, obstaja tak $x_2 \in K_2$, da velja $v_2(a - x_2) = v_1(a - x_1)$ za vsak $a \in K'$. Najprej, ker je $(K', \mathcal{O}')$ Henselovo, enako kot zgoraj sklepamo, da je x_2 transcendenten nad K' v K_2. Edino, na kar moramo biti pozorni da lahko naredimo ta sklep, je, da ni slučajno v K'. Toda če bi bil, bi veljalo $\infty = v_2(x_2 - x_2) = v_1(x_2 - x_1)$, iz česar bi sledilo $x_1 = x_2 \in K'$, kar pa ne drži. Zato lahko podobno kot zgoraj definiramo τ, vložitev $K'(x_1)$ v K_2 s $\tau(a) = a$ za $a \in K'$ in $\tau(x_1) = x_2$. Pokazati moramo še, da je $v_2 \circ \tau = v_1$. Dovolj bo, če pokažemo, da je $v_1(f(x_1)) = v_2(f(x_2))$ za vsak polinom $f \in K'[x]$. Dokazovali bomo z indukcijo po stopnji polinomov. Za linearne polinome enakost velja po zgornji konstrukciji.

Pa recimo, da velja enakost za vse polinome v $K'[x_1]$ stopnje kvečjemu $n - 1$. Naj bo $f \in K'[x_1]$ stopnje n. Po indukcijski predpostavki in aditivnosti valuacije produkta lahko predpostavimo, da je f nerazcepen v K'. Naj bo $F := K'[x_1]/(f)$ polje, ki je kot vektorski prostor nad K' je izomorfno $V := K' \oplus K'x_1 \oplus \cdots K'x_1^{n-1} \subseteq K'[x_1]$. Naj bo $v : K'[x_1] \to \Gamma' \cup \{\infty\}$ zožitev valuacije v_1 na $K'[x_1]$. Če jo zožimo na V (kot podmnožico $K'[x_1]$) in če to zožitev komponiramo s K'-izomorfizmom

vektorskih polj F in V', dobimo preslikavo $v : F \to \Gamma' \cup \{\infty\}$, ki zadošča $v(0) = \infty$ in $v(p+q+(f)) \geq \min\{v(p+(f)), v(q+(f))\}$ za vse $p, q \in K'[x_1]$.

Če velja še $v(pq+(f)) = v(p+(f)) + v(q+(f))$ za vse $p, q \in K'[x_1]$, je v valuacija na F. Ker je $\infty > [F : K'] = n > 1$, K' pa Henselovo polje s karakteristiko nič in zato končno razvejano, F ne more biti neposredna razširitev, in ker sta pripadajoči valuacijski grupi enaki, sledi, da je $\overline{F}$ prava razširitev $\overline{K} = \overline{K(x_1)}$, kar pa ni mogoče. Sklepamo, da obstajata dva taka polinoma $p, q \in K'[x_1]$ stopnje manj kot n, da velja $v(pq+(f)) \neq v(p+(f)) + v(q+(f))$. Naj bo r enolično določen polinom stopnje manj kot n, da je $pq = fs + r$, $s \in K'[x_1]$. Torej je $r + (f) = pq + (f)$ in tako dobimo $v(r+(f)) \neq v(p+(f)) + v(q+(f))$. Če se premaknemo nazaj v $K'[x_1]$, iz zgornje evklidske enačbe sledi $v_1(f) = \min\{v_1(p)+v_1(q), v_1(r)\} - v_1(s)$. Vsi polinomi na desni strani imajo stopnjo, manjšo od n, zato lahko sklepamo (če ves postopek ponovimo za $K'[x_2] \subseteq K_2$):

$$\begin{aligned} v_1(f(x_1)) &= \min\{v_1(g(x_1)) + v_1(h(x_1)), v_1(r(x_1))\} - v_1(s(x_1)) \\ &= \min\{v_2(g(x_2)) + v_2(h(x_2)), v_2(r(x_2))\} - v_1(s(x_2)) = v_2(f(x_2)). \end{aligned}$$

Druga neenakost zgoraj velja po indukcijski predpostavki glede na stopnjo polinoma. Z indukcijo smo pokazali, da je $v_2 \circ \tau = v_1$. Ker smo s tem zopet prišlo do protislovja s predpostavljeno maksimalnostjo vložitve $(K', \mathcal{O}')$ v K_2, ki izpolnjuje (1)-(4) v vlogi $(K, \mathcal{O})$, je dokaz izreka tako končan. □

Izrek 4.3 ([9, izrek 4.6.2])**.** *(Ax-Kochen, Jeršov) Naj bosta $(K_1, \mathcal{O}_1)$ in $(K_2, \mathcal{O}_2)$ Henselovi polji z elementarno ekvivalentnima poljema ostankov $\overline{K}_1$ in $\overline{K}_2$ ter elementarno ekvivalentnima valuacijskima grupama Γ_1 in Γ_2. Če je karakteristika polj ostankov enaka 0, potem sta tudi $(K_1, \mathcal{O}_1)$ in $(K_2, \mathcal{O}_2)$ elementarno ekvivalentna.*

Dokaz. Ker je jezik polj z valuacijo števen, po izreku Löwenheim–Skolem - navzdol obstajata števni elementarni podstrukturi $(K_i', \mathcal{O}_i') \preceq (K_i, \mathcal{O}_i)$ za $i = 1, 2$. Predpostavimo lahko, da sta $(K_i, \mathcal{O}_i)$ $\aleph_1$-nasičeni za $i = 1, 2$, sicer namesto njiju obravnavamo elementarno $\aleph_1$-nasičeni elementarni razširitvi $(K_i', \mathcal{O}_i')$, ki obstaja po 3.25 in sta elementarno ekvivalentni $(K_i, \mathcal{O}_i)$. Potem bomo spet s pomočjo izreka Löwenheim–Skolem - navzdol skonstruirali naraščajočo verigo polj z valuacijo

$$(K_i^{(0)}, \mathcal{O}_i^{(0)}) \subseteq (K_i^{(1)}, \mathcal{O}_i^{(1)}) \subseteq \ldots \subseteq (K_i^{(n)}, \mathcal{O}_i^{(n)}) \subseteq \ldots \subseteq (K_i, \mathcal{O}_i),$$

kjer bodo $(K_i^{(n)}, \mathcal{O}_i^{(n)})$ za $i = 1, 2$, $n \in \mathbb{N}_0$ števna Henselova polja. Za vsak n bo obstajal izomorfizem $\sigma^{(n)} : (K_1^{(n)}, \mathcal{O}_1^{(n)}) \to (K_2^{(n)}, \mathcal{O}_2^{(n)})$, ki bo za $n \geq 1$ razširitev $\sigma^{(n-1)}$. Prav tako bo veljalo za vsak $n \geq 1$:

(1) $(K_1^{(2n-1)}, \mathcal{O}_1^{(2n-1)}) \preceq (K_1, \mathcal{O}_1)$,
(2) $(K_2^{(2n)}, \mathcal{O}_2^{(2n)}) \preceq (K_2, \mathcal{O}_2)$,
(3) $(\overline{K}_1, (\overline{a})_{a \in \mathcal{O}_1^{(n)}}) \equiv (\overline{K}_2, (\overline{\sigma^{(n)}(a)})_{a \in \mathcal{O}_1^{(n)}})$,
(4) $(\Gamma_1, (v_1(a))_{a \in K_1^{(n)}}) \equiv (\Gamma_2, (v_2(\sigma^{(n)}(a)))_{a \in K_1^{(n)}})$.

Tu z v_i za $i = 1, 2$ kot ponavadi definiramo valuacijo, ki pripada $(K_1, \mathcal{O}_1)$. Potem bomo definirali $K_1' := \cup_{n \in \mathbb{N}} K_1^{(n)}$, $K_2' := \cup_{n \in \mathbb{N}} K_2^{(n)}$ in $\sigma' := \cup_{n \in \mathbb{N}} \sigma^{(n)}$. $\sigma' : K_1' \to K_2'$ bo izomorfizem. Poleg tega bo iz $(K_1^{(2n-1)}, \mathcal{O}_1^{(2n-1)}) \preceq (K_1, \mathcal{O}_1)$ za vse $n \geq 1$ sledilo, da je K_1' elementarna podstruktura K_1[3], K_2' pa, podobno, elementarna podstruktura K_2. Iz tega bo takoj sledila elementarna ekvivalenca $(K_1, \mathcal{O}_1) \equiv (K_2, \mathcal{O}_2)$.

[3]Elementarna ekvivalenca K_1' in K_1 bo sledila iz $K_1^{(1)} \preceq K_1$ in $K_1^{(1)} \preceq K_1'$.

Za $n = 0$ bomo definirali $K_1^{(0)} = K_2^{(0)} = \mathbb{Q}$ in $\sigma^{(0)} = id_{\mathbb{Q}}$. Ker je karakteristika polj ostankov enaka nič, so, kot smo že premislili v poglavju o Henselovih poljih, elementi $\mathbb{Q}^\times$ obrnljivi v $\mathcal{O}_1^{(0)}$ oz. $\mathcal{O}_2^{(0)}$. Potem sta dobljeni valuaciji trivialni. Iz tega sledi, da je $(K_i^{(0)}, \mathcal{O}_i^{(0)} = \mathbb{Q})$ Henselovo polje z valuacijo za $i = 1, 2$[4]. Poleg tega iz $\mathrm{char}(K_1) = \mathrm{char}(K_2) = 0$ sledi $\mathbb{Q} \subseteq K_1$ in $\mathbb{Q} \subseteq K_2$.

Za $n = 1$ naj bo $(K_1^{(1)}, \mathcal{O}_1^{(1)})$ števna elementarna podstruktura $(K_1, \mathcal{O}_1)$, ki vsebuje $(K_1^{(0)}, \mathcal{O}_1^{(0)})$ in obstaja po 3.23. Ker je $K_1^{(1)}$ števno, sta števna tudi $\Gamma_1^{(1)}$ in $\overline{K_1^{(1)}}$. Velja tudi $\overline{K_1}^{(1)} \equiv \overline{K_1} \equiv \overline{K_2}$ in $\Gamma_1^{(1)} \equiv \Gamma_1 \equiv \Gamma_2$. Ker sta $\overline{K_2}$ in Γ_2 $\aleph_1$-nasičena po 4.1, iz 3.28 sledi, da lahko $\overline{K_1}^{(1)}$ elementarno vložimo v $\overline{K_2}$, $\Gamma_1^{(1)}$ pa v Γ_2. Pripadajoči vložitvi označimo z $\sigma_r^{(1)} : \overline{K_1}^{(1)} \to \overline{K_2}$ in $\sigma_g^{(1)} : \Gamma_1^{(1)} \to \Gamma_2$. Ker je $\Gamma_1^{(0)} = \{0\}$ in $\Gamma_1^{(1)} = \mathbb{Q}$, je njun kvocient očitno brez torzije.

Premislimo, da lahko identično preslikavo $\sigma^{(0)} : (K_1^{(0)}, \mathcal{O}_1^{(0)}) \to (K_2^{(0)}, \mathcal{O}_2^{(0)}) \subseteq (K_2, \mathcal{O}_2)$ razširimo do vložitve $\sigma^{(1)} : (K_1^{(1)}, \mathcal{O}_1^{(1)}) \to (K_2, \mathcal{O}_2)$. Velja namreč:

- $(K_1^{(0)}, \mathcal{O}_1^{(0)}), (K_1^{(1)}, \mathcal{O}_1^{(1)}), (K_2, \mathcal{O}_2)$ so Henselova polja z valuacijo.
- Velja $(K_1^{(0)}, \mathcal{O}_1^{(0)}) \subseteq (K_1^{(1)}, \mathcal{O}_1^{(1)})$ in $(K_1^{(0)}, \mathcal{O}_1^{(0)}) \subseteq (K_2, \mathcal{O}_2)$. Tu tako kot v 4.2 $(K_1^{(0)}, \mathcal{O}_1^{(0)})$ izenačimo z njegovo vložitvijo v $(K_2, \mathcal{O}_2)$.
- $(K_2, \mathcal{O}_2)$ je $\aleph_1 = |K_1^{(0)}|^+$-nasičen.
- Zaradi obstoja vložitev $\sigma_r^{(1)} : \overline{K_1}^{(1)} \to \overline{K_2}$ in $\sigma_g^{(1)} : \Gamma_1^{(1)} \to \Gamma_2$ lahko brez škode za splošnost predpostavimo, da je $\{0\} = \Gamma_1^{(0)} \subseteq \Gamma_1^{(1)} \subseteq \Gamma_2$ in $\mathbb{Q} = \overline{K_1^{(0)}} \subseteq \overline{K_1^{(1)}} \subseteq \overline{K_2}$, saj ima $\overline{K_1^{(1)}}$ tako kot $\overline{K_1}$ karakteristiko nič.
- $\Gamma_1^{(1)}/\Gamma_1^{(0)}$ je brez torzijskega dela.

Če dobro pomislimo, smo se znašli nekje na začetku dokaza 4.2, od koder naprej lahko pokažemo, da obstaja vložitev $(K_1^{(1)}, \mathcal{O}_1^{(1)})$ v $(K_2, \mathcal{O}_2)$, ki ohranja vrednost valuacij. Bralcu bomo prihranili ponovitve vseh podrobnosti. Torej obstaja vložitev $\sigma^{(1)} : (K_1^1, \mathcal{O}_1^{(1)}) \to (K_2, \mathcal{O}_2)$. Naj bo $(K_2^{(1)}, \mathcal{O}_2^{(1)})$ $\sigma^{(1)}$-izomorfna slika $(K_1^{(1)}, \mathcal{O}_1^{(1)})$ v $(K_2, \mathcal{O}_2)$.

V zgornjih točkah smo predpostavili, da velja $\overline{K_1^{(1)}} \subseteq \overline{K_2}$, iz česar sledi $\overline{a} = \overline{\sigma^{(1)}(a)}$ za vsak $a \in \mathcal{O}_1^{(1)}$. Ker v splošnem namesto $\overline{K_1^{(1)}} \subseteq \overline{K_2}$ velja, da obstaja vložitev $\sigma_r^{(1)} : \overline{K_1^{(1)}} \to \overline{K_2}$, sledi $\sigma_r^{(1)}(\overline{a}) = \overline{\sigma^{(1)}(a)}$ za vsak $a \in \mathcal{O}_1^{(1)}$. Torej je $\sigma_r^{(1)}(\overline{K_1^{(1)}}) = \overline{K_2^{(1)}}$. $\sigma_r^{(1)}$ je, sklepamo, izomorfizem med $\overline{K_1^{(1)}}$ in $\overline{K_2^{(1)}}$. Ker sta polji $\overline{K_1^{(1)}} = \{\overline{a} \mid a \in \mathcal{O}_1^{(1)}\} \subseteq \overline{K_1}$ in $\overline{K_2^{(1)}} = \{\overline{a} \mid a \in \mathcal{O}_2^{(1)}\} = \{\overline{a} \mid a \in \sigma^{(1)}(\mathcal{O}_1^{(1)})\} \subseteq \overline{K_1}$ izomorfni in ker po predpostavki velja $\overline{K_1} \equiv \overline{K_2}$, sledi pogoj (3) iz začetka naloge za $n = 1$.

Iz dokaza 4.2 sledi $v_1 = v_2 \circ \sigma^{(1)}$. Upoštevati moramo, da je to posledica predpostavke $\Gamma_1^{(1)} \subseteq \Gamma_2$. V splošnem namesto tega velja, da obstaja vložitev $\sigma_g^{(1)} : \Gamma_1^{(1)} \to \Gamma_2$, zato lahko sklepamo, da velja $\sigma_g^{(1)} \circ v_1 = v_2 \circ \sigma^{(1)}$. Iz povedanega sledi, da velja $\sigma_g^{(1)}(\Gamma_1^{(1)}) = \Gamma_2^{(1)}$. Sklepamo, da je $\sigma_g^{(1)}$ izomorfizem med $\Gamma_1^{(1)}$ in $\Gamma_2^{(1)}$. Ker sta $\Gamma_1^{(1)} = v_1(K_1^{(1)}) \subseteq \Gamma_1$ in $\Gamma_2^{(1)} = v_2(K_2^{(1)\times}) = v_2(\sigma^{(1)}(K_1^{(1)}\times)) \subseteq \Gamma_2$ izomorfni in ker velja $\Gamma_1 \equiv \Gamma_2$, sledi, da za $n = 2$ sledi pogoj (4) iz začetka naloge.

Iz izpolnjenih pogojev (3) in (4) posebej sledi:

- $(\overline{K_1}, (\overline{x})_{\overline{x} \in \overline{K_1^{(1)}}}) \equiv (\overline{K_2}, (\sigma_r^{(1)}(\overline{x}))_{\overline{x} \in \overline{K_1^{(1)}}})$ in

[4]Velja namreč $\overline{K_i^{(0)}} = K_i^{(0)}$. Glej (3) v 2.57

- $(\Gamma_1, (\gamma)_{\gamma\in\Gamma_1^{(1)}}) \equiv (\Gamma_2, (\sigma_g^{(1)}(\gamma))_{\gamma\in\Gamma_1^{(1)}})$.

Sedaj naj bo $(K_2^{(2)}, \mathcal{O}_2^{(2)})$ števna elementarna podstruktura $(K_2, \mathcal{O}_2)$, ki vsebuje $(K_2^{(1)}, \mathcal{O}_2^{(1)})$. Njen obstoj zopet sledi iz 3.23. Potem iz zgornjih dveh točk takoj sledi:

- $(\overline{K_1}, (\overline{x})_{\overline{x}\in\overline{K_1^{(1)}}}) \equiv (\overline{K_2^{(2)}}, (\sigma_r^{(1)}(\overline{x}))_{\overline{x}\in\overline{K_1^{(1)}}})$ in
- $(\Gamma_1, (\gamma)_{\gamma\in\Gamma_1^{(1)}}) \equiv (\Gamma_2^{(2)}, (\sigma_g^{(1)}(\gamma))_{\gamma\in\Gamma_1^{(1)}})$.

Ker sta po 4.1 $\overline{K_1}$ in Γ_1 $\aleph_1$-nasičeni strukturi, po 3.28 obstajata elementarni vložitvi $\tau_r^{(2)} : \overline{K_2^{(2)}} \to \overline{K_1}$ in $\tau_g^{(2)} : \Gamma_2^{(2)} \to \Gamma_1$. Vidimo, da sta $\tau_r^{(2)}$ in $\tau_g^{(2)}$ razširitvi $(\sigma_r^{(1)})^{-1}$ in $(\sigma_g^{(1)})^{-1}$ na $\overline{K_2^2}$ oz. $\Gamma_2^{(2)}$.

Sedaj vidimo, da velja naslednje:

- $(K_2^{(1)}, \mathcal{O}_2^{(1)}), (K_2^{(2)}, \mathcal{O}_2^{(2)}), (K_1, \mathcal{O}_1)$ so Henselova polja z valuacijo.
- Velja $(K_2^{(1)}, \mathcal{O}_2^{(1)}) \subseteq (K_2^{(2)}, \mathcal{O}_2^{(2)})$ in $(K_2^{(1)}, \mathcal{O}_2^{(1)}) \subseteq (K_1, \mathcal{O})$.
- $(K_1, \mathcal{O}_1)$ je $\aleph_1 = |K_2^{(1)}|^+$-nasičen.
- Zaradi obstoja vložitev $\tau_r^{(2)} : \overline{K_2}^{(2)} \to \overline{K_1}$ in $\tau_g^{(2)} : \Gamma_2^{(2)} \to \Gamma_1$ lahko brez škode za splošnost predpostavimo, da je $\Gamma_2^{(1)} \subseteq \Gamma_2^{(2)} \subseteq \Gamma_1$ in $\overline{K_2^{(1)}} \subseteq \overline{K_2^{(2)}} \subseteq \overline{K_1}$.
- $\Gamma_2^{(2)}/\Gamma_2^{(1)}$ je brez torzije. To podobno kot v dokazu 4.2 sledi iz $\Gamma_2^{(1)} \equiv \Gamma_2^{(2)}$.

Podobno kot zgoraj sklepamo, da lahko $(K_2^2, \mathcal{O}_2^{(2)})$ vložimo v $(K_1, \mathcal{O}_1)$ s $\tau^{(2)}$, kjer $\tau^{(2)}$ ohranja vrednost valuacij. Naj bo $(K_1^{(2)}, \mathcal{O}_1^{(2)})$ slika $(K_2^{(2)}, \mathcal{O}_2^{(2)})$ v K_1. Podobno kot prej sklepamo, da velja $v_1 \circ \tau^{(2)} = \tau_g^{(2)} \circ v_2$ in $\tau_r^{(2)}(\overline{a}) = \overline{\tau^{(2}(a)}$ in da sta zato $\tau_r^{(2)} : \overline{K_2^{(2)}} \to \overline{K_1^{(2)}}$ in $\tau_g^{(2)} : \Gamma_2^{(2)} \to \Gamma_1^{(2)}$ izomorzifma polj oziroma valuacijskih abelovih grup. Če definiramo $\sigma^{(2)} = (\tau^{(2)})^{-1}$, $\sigma_r^{(2)} = (\tau_r^{(2)})^{-1}$ in $\sigma_g^{(2)} = (\tau_g^{(2)})^{-1}$, tako kot zgoraj za $n = 2$ veljata pogoja (3) in (4) in zato posebej:

- $(\overline{K_1}, (x)_{x\in\overline{K_1^{(2)}}}) \equiv (\overline{K_2}, (\sigma_r^{(2)}(x))_{x\in\overline{K_1^{(2)}}})$ in
- $(\Gamma_1, (\gamma)_{\gamma\in\Gamma_1^{(2)}}) \equiv (\Gamma_2, (\sigma_g^{(2)}(\gamma))_{\gamma\in\Gamma_1^{(2)}})$.

Sedaj postopek ponovimo za vsako naravno število n. Če je n sod, dobimo vložitev $\sigma^{(n+1)} : (K_1^{(n+1)}, \mathcal{O}_1^{(n+1)}) \to (K_2, \mathcal{O}_2)$. Ta vložitev bo inducirala izomorfizem $\sigma^{(n+1)} : (K_1^{(n+1)}, \mathcal{O}_1^{(n+1)}) \to (K_2^{(n+1)}, \mathcal{O}_2^{(n+1)})$. Ta izomorfizem pa nam da izomorfizem polj ostankov $\sigma_r^{(n+1)} : \overline{K_1^{(n+1)}} \to \overline{K_2^{(n+1)}}$ in valuacijskih grup $\sigma_g^{(n+1)} : \Gamma_1^{(n+1)} \to \Gamma_2^{(n+1)}$.

Če je n lih, pa dobimo vložitev $\tau^{(n+1)} : (K_2^{(n+1)}, \mathcal{O}_2^{(n+1)}) \to (K_1, \mathcal{O}_1)$, ki inducira izomorfizem $\tau^{(n+1)} = (\sigma^{(n+1)})^{-1} : (K_2^{(n+1)}, \mathcal{O}_2^{(n+1)}) \to (K_1^{(n+1)}, \mathcal{O}_1^{(n+1)})$. Izomorfizem $\sigma^{(n+1)}$ podobno kot v zgornjem primeru da izomorfizem polj ostankov in valuacijskih grup.

Dobili smo iskano zaporedje in s tem dokazali izrek. □

Opomba 4.4. Predpostavka $\mathrm{char}(\overline{K_1}) = \mathrm{char}(\overline{K_2}) = 0$ v izreku je potrebna. Če si namreč ogledamo polji z valuacijo $\mathbb{Z}_p((t))$ in $\mathbb{Q}_p$ za neko praštevilo p, vidimo, da sta valuacijski grupi obe enaki $\mathbb{Z}$, polji ostankov pa sta v obeh primerih $\mathbb{Z}_p$, ki ima karakteristiko p. Kljub temu $\mathbb{Z}_p((t))$ in $\mathbb{Q}_p$ nista elementarno ekvivalentni, saj je karakteristika prvega enaka p, karatkeristika drugega pa nič.

Sedaj se spomnimo dveh polj z valuacijami, ki smo ju spoznali na koncu prejšnjega poglavja: $(K_1, \mathcal{O}_1) := \cap_{p\in\mathbb{P}}\mathbb{Q}_p/\mathcal{P}$ in $(K_2, \mathcal{O}_2) := \cap_{p\in\mathbb{P}}\mathbb{Z}_p((t))/\mathcal{P}$, kjer je bil $\mathcal{P}$

ultrafilter nad filtrom kokončnih množic na množici praštevil $\mathbb{P}$. Zgoraj smo premislili, da je valuacijska grupa ultraprodukta enaka ultraproduktu valuacijskih grup. Pripadajoči valuacijski grupi Γ_1 in Γ_2 sta torej enaki ultraproduktu števno mnogo kopij $\mathbb{Z}$, ta struktura pa je, kot smo prav tako že razmislili, elementarno ekvivalentna $\mathbb{Z}$. Polji ostankov $\overline{K_1}$ in $\overline{K_2}$ sta v obeh primerih enaka ultraproduktu $\overline{K} := \cap_{p\in\mathbb{P}}\mathbb{Z}_p$. Razmislimo, da je $\mathrm{char}(\overline{K}) = 0$. Pa recimo, da ni. Potem obstaja tako praštevilo p, za katerega velja $\overline{K} \models p \cdot 1 = 0$. To pomeni, da je $\{q \in \mathbb{P} \mid \mathbb{Z}_q \models p \cdot 1 = 0\} \in \mathcal{P}$. Toda $p \cdot 1$ velja natanko v enem polju iz ultraprodukta - $\mathbb{Z}_p$. Ker je $\mathcal{P}$ ultrafilter, ki je razširitev filtra kokončnih množic, v $\mathcal{P}$ ni nobene končne množice. V posebnem nima nobenega singeltona. Torej je $\mathrm{char}(\overline{K}) = 0$. Sedaj vidimo, da so izpolnjene vse predpostavke izreka Ax-Kochen-Jeršov, s pomočjo katerega lahko naredimo spodnji zaključek.

Izrek 4.5. *Ultraprodukta polj z valuacijo $\cap_{p\in\mathbb{P}}\mathbb{Q}_p/\mathcal{P}$ in $\cap_{p\in\mathbb{P}}\mathbb{Z}_p((t))/\mathcal{P}$, kjer je $\mathcal{P}$ ultrafilter nad filtrom kokončnih množic, sta elementarno ekvivalentna.*

Povedano drugače: vsaka izjava v jeziku polj z valuacijo, ki velja v $\mathbb{Q}_p$ za vsa razen končno mnogo praštevil $p \in \mathbb{P}$, velja v $\mathbb{Z}_p((t))$ za vsa razen končno mnogo praštevil $p \in \mathbb{P}$.

Literatura

[1] R. B. Ash, *A Course in Algebraic Number Theory*, Dover publications, New York, 2003.

[2] J. Ax, S.Kochen, *Diophantine problems over local fields I.*, American Journal of Mathematics **87** (1965) 605–630.

[3] N. Bourbaki, *Commutative algebra. Chapters 1-7*, Springer, Berlin, 1989.

[4] A. J. Engler, A. Prestel, *Valued fields*, Springer Monographs in Mathematics, Springer, Berlin, 2005.

[5] J. Globevnik, *Analiza I*, DMFA - založništvo, 2016.

[6] K. Hrbaček, T. Jech, *Introduction to Set Theory*, M. Dekker, New York, 1999.

[7] Ju. L. Jeršov, *On the elementary theory of maximal normed fields*, Algebra i Logika, **4** (1965) 47–48.

[8] G. Kemper, *A course in commutative algebra*, Springer, Berlin, 2011.

[9] A. Prestel, C. Delzell, *Mathematical Logic and Model Theory*, Springer, London, 2011.

[10] A. Prestel, F. V. Kuhlmann, *On places of algebraic function fields*, Journal für die reine und angewandte Mathematik **353** (1984) 181–195.

[11] M. Reid, *Undergraduate Commutative Algebra*, Cambridge University Press, Cambridge, 1995.

[12] W. Rautenberg, *A Concise Introduction to Mathematical Logic*, Springer, Berlin, 2005.