ZORNOVA LEMA IN NJENA UPORABA

ŽIGA ZUPANČIČ

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

V članku je predstavljena Zornova lema in nekaj ekvivalentnih formulacij. Prikazana je njena uporaba v teoriji grup, kjer je dokazano, da lahko homomorfizme iz podgrup Abelovih grup v deljive grupe razširimo na celotno Abelovo grupo. V teoriji kolobarjev je s pomočjo Zornove leme pokazano, da vsak kolobar vsebuje maksimalni levi ideal in da je presek vseh praidealov komutativnega kolobarja enak množici vseh nilpotentnih elementov kolobarja. Dokazan je Cohenov izrek in njegova posplošitev. V nadaljevanju je dokazan izrek, ki pravi, da ima vsak neničelni modul nad obsegom bazo. Njegova posledica pravi, da ima vsak vektorski prostor nad poljem bazo. S pomočjo te posledice je pokazano, da v grupi z več kot dvema elementoma obstaja netrivialni avtomorfizem. Primer uporabe v teoriji grafov pa je dokaz izreka, da vsak povezan graf vsebuje vpeto drevo.

ZORN'S LEMMA AND SOME APPLICATIONS

In this article Zorn's lemma and some equivalent formulations are presented. An application in group theory is presented by proving that homomorphisms from subgroups of Abelian groups to divisible groups can be extended to the whole Abelian group. In ring theory Zorn's lemma implies the existence of maximal left ideals in rings. Also, it implies that the intersection of all prime ideals in a commutative ring is equal to the set of nilpotent elements of the ring. Cohen's theorem and it's generalization are also proved. Using Zorn's lemma, it is shown, that every nonzero module over a division ring has a basis. The consequence of that is that every vector space over a field has a basis. This corollary is used to prove that a group with more than two elements has a nontrivial automorphism. The use of Zorn's lemma in graph theory is shown when proving that every connected graph contains a spanning tree.

1. Uvod

Zornova lema (znana tudi kot Kuratowski-Zornova lema), ki jo lahko izpeljemo iz aksioma izbire, je pomembno orodje v mnogih vejah matematike. Neodvisno drug od drugega sta jo formulirala najprej Kazimierz Kuratowski (leta 1922), nato pa še Max Zorn (leta 1935), ki jo je predlagal kot nov aksiom. Poimenoval jo je John W. Tukey [8, stran 7] v svoji topološki knjigi leta 1941.

Ekvivalentna je med drugim tudi izreku Tihonova v topologiji in izreku o dobri urejenosti. Ekvivalenco razumemo v smislu, da če privzamemo aksiome Zermelo-Fraenkel (ZF) in eno od trditev, potem druge sledijo. Torej Zornovo lemo lahko uporabljamo, če privzamemo ZFC aksiome (Zermelo-Fraenkel aksiome in aksiom izbire), kar bomo, razen v drugem razdelku, kjer dokazujemo ekvivalence različnih formulacij, tudi storili.

2. Zornova lema in ekvivalentne formulacije

V tem razdelku definiramo pojme, ki jih potrebujemo v formulaciji Zornove leme. Najprej si oglejmo, kaj je delna urejenost na neki množici in kaj je delno urejena množica.

Definicija 1. *Relacija delne urejenosti* na množici A je relacija z oznako $\leq$, ki zadošča naslednjim pogojem:

1. za vsak $a \in A$ velja $a \leq a$ (refleksivnost),
2. za vsaka $a, b \in A$ iz $a \leq b$ in $b \leq a$ sledi $a = b$ (antisimetričnost),
3. za vse $a, b, c \in A$ iz $a \leq b$ in $b \leq c$ sledi $a \leq c$ (tranzitivnost).

Definicija 2. *Delno urejena množica* je par $(A, \leq)$ množice A in relacije delne urejenosti $\leq$, definirane na A.

Če je iz besedila razvidno, katero relacijo imamo v mislih, za delno urejeno množico $(A, \leq)$ pišemo le A.

V formulaciji Zornove leme potrebujemo tudi delno urejene množice, v katerih lahko primerjamo poljubna elementa. To nas pripelje do naslednje definicije.

Definicija 3. Naj bo $(A, \leq)$ delno urejena množica. Če za poljubna $a, b \in A$ velja $a \leq b$ ali $b \leq a$, pravimo, da je $(A, \leq)$ *linearno urejena množica*.

Za elementa a in b, za katera velja $a \leq b$ ali $b \leq a$, rečemo, da sta *primerljiva*.

Lema 1. *Naj bo A delno urejena množica. Če je $\{a_1, a_2, \ldots, a_n\} \subseteq A$ linearno urejena končna množica za neki $n \in \mathbb{N}$, potem obstaja tak $i \in \{1, 2, \ldots, n\}$, da je $a_j \leq a_i$ za $j = 1, 2, \ldots, n$.*

Dokaz. Lemo bomo dokazali z indukcijo na n. Za $n = 1$ lema očitno velja. Predpostavimo sedaj, da v $\{a_1, a_2, \ldots, a_{n-1}\}$ obstaja element a_i, da je $a_j \leq a_i$ za $j = 1, 2, \ldots, n-1$. Oglejmo si element a_n. Bodisi je $a_n \leq a_i$ in zato lema velja, ali pa je $a_i \leq a_n$. Tedaj je element a_n tak, da velja $a_j \leq a_n$ za $j = 1, 2, \ldots, n$, saj zaradi tranzitivnosti relacije delne urejenosti iz $a_j \leq a_i$ in $a_i \leq a_n$ namreč sledi $a_j \leq a_n$.

Naj bo sedaj A delno urejena množica. *Zgornja meja* podmnožice $B \subseteq A$ je tak element $a \in A$, da je $b \leq a$ za vsak $b \in B$. *Maksimalni element* množice A pa definiramo kot element $a \in A$, za katerega velja $b \leq a$ za vsak b, ki ga lahko primerjamo z a.

Zgornja meja neke podmnožice ne obstaja vedno in ni nujno, da je vsebovana v tej podmnožici. Če na primer vzamemo množico naravnih števil ter običajno relacijo urejenosti, ima vsaka končna podmnožica zgornjo mejo (največji element v njej), množica večkratnikov števila 2 pa zgornje meje nima. Tudi maksimalni element ne obstaja vedno. Primer je množica $\{q \in \mathbb{Q} \mid 1 \leq q^2 \leq 2\}$ z običajno relacijo urejenosti, kjer je kandidat za maksimalni element število $\sqrt{2}$, ki pa ni racionalno število. Naslednji zgled pa pokaže še, da če maksimalni element obstaja, ni nujno en sam.

Zgled 1. Naj bo $\mathcal{X} = \mathcal{P}(\mathbb{R}) \setminus \{\emptyset\}$ (torej potenčna množica množice realnih števil brez prazne množice). Na njej je definirana relacija delne urejenosti: za $A, B \in \mathcal{X}$ je $A \leq B$, če velja $B \subseteq A$. Očitno je relacija refleksivna in antisimetrična. Preverimo le tranzitivnost. Naj bodo $A, B, C \in \mathcal{X}$ ter naj velja $A \leq B$ in $B \leq C$. Iz definicije relacije sledi, da je $B \subseteq A$ in $C \subseteq B$, od tod pa $C \subseteq A$, kar pomeni $A \leq C$.

V $\mathcal{X}$ je vsaka enoelementna množica maksimalni element. To je res, saj je $\{x\} \in \mathcal{X}$ primerljiva z vsemi množicami, ki vsebujejo x, in je zato $\{x\} \subseteq A$ za vsak A, ki vsebuje x. V $\mathcal{X}$ torej obstaja neštevno mnogo maksimalnih elementov. To so tudi vsi maksimalni elementi, saj lahko iz vsake neprazne množice S z vsaj dvema elementoma izberemo en element (recimo mu s) in zato velja $S \leq \{s\}$.

Sedaj imamo vse potrebne definicije za formulacijo Zornove leme.

Izrek 2 (Zornova lema). *Naj bo A delno urejena množica. Če ima vsaka linearno urejena podmnožica množice A zgornjo mejo, potem A vsebuje maksimalen element.*

Zornova lema nam torej da le obstoj maksimalnega elementa, nič pa ne pove o njihovem številu. Zapisali bi jo lahko tudi za minimalne elemente (kjer bi vsaka linearno urejena podmnožica morala imeti spodnjo mejo), a je taka formulacija ekvivalentna tej v izreku 2, saj lahko relacijo delne urejenosti obrnemo (torej namesto $a \leq b$ sedaj velja $b \leq a$) in tako namesto maksimalnih elementov dokažemo obstoj minimalnih.

Lotimo se ekvivalentnih formulacij. Najprej bomo formulirali Aksiom izbire in dokazali njegovo ekvivalenco z Zornovo lemo [2].

Aksiom 1 (Aksiom izbire). Naj bo $(A_i)_{i\in\mathcal{I}}$ družina neprazniih množic. Potem obstaja taka funkcija $f : \mathcal{I} \to \bigcup_{i\in\mathcal{I}} A_i$, da je $f(i) \in A_i$ za vsak $i \in \mathcal{I}$.

Opomba 1. Funkcija f v zgornjem aksiomu se imenuje *funkcija izbire*.

Spodnji izrek nam pravzaprav zagotavlja, da lahko uporabljamo Zornovo lemo, če predpostavimo aksiome ZFC. Dokaz v [11].

Izrek 3. *Zornova lema je ekvivalentna aksiomu izbire.*

Tudi pomemben izrek v topologiji je ekvivalenten Zornovi lemi. V dokazu izreka Tihonova bomo sledili [10], v drugi smeri pa [6, strani 75-76].

Izrek 4 (Tihonov). *Neprazen produkt neprazniih prostorov $\prod_{i\in\mathcal{I}} X_i$ je kompakten natanko tedaj, ko je X_i kompakten za vsak $i \in \mathcal{I}$.*

Za dokaz izreka potrebujemo naslednjo lemo ter izrek Alexandra za podbaze, ki nam pove, da lahko kompaktnost preverjamo s pomočjo pokritij s podbazičnimi okolicami.

Lema 5. *Naj bodo (X_i, τ_i) kompaktni prostori za vsak $i \in \mathcal{I}$, naj bo $X = \prod_{i\in\mathcal{I}} X_i$ prostor opremljen s produktno topologijo in naj bo $\pi_i : X \to X_i$ projekcija. Potem vsako odprto pokritje $\mathcal{U}$ prostora X, ki je sestavljeno iz elementov množice $\{\pi_i^{-1}(U) \mid U \in \tau_i, i \in \mathcal{I}\}$, vsebuje končno podpokritje.*

Dokaz. Naj bo $\mathcal{U} \subseteq \{\pi_i^{-1}(U) \mid U \in \tau_i, i \in \mathcal{I}\}$ pokritje prostora X. Definirajmo $\mathcal{V}_i = \{U \in \tau_i \mid \pi_i^{-1}(U) \in \mathcal{U}\}$. Pokažimo, da obstaja tak $i_0 \in \mathcal{I}$, da je $\mathcal{V}_{i_0}$ pokritje za X_{i_0}. Če tak $i_0 \in \mathcal{I}$ ne obstaja, potem za vsak $i \in \mathcal{I}$ obstaja neki $x_i \in X_i$, ki ni vsebovan v nobeni množici iz $\mathcal{V}_i$. Izberimo tak $e \in X$, da je $\pi_i(e) = x_i$ za vsak i. Element e torej ni vsebovan v nobeni množici iz $\mathcal{U}$, kar pa je v protislovju s predpostavko, da je $\mathcal{U}$ pokritje za X.

Torej lahko izberemo tak $i_0 \in \mathcal{I}$, da je $\mathcal{V}_{i_0}$ pokritje za X_{i_0}. Ker pa je (X_{i_0}, τ_{i_0}) kompakten, obstaja končno podpokritje $U_1, U_2 \ldots, U_k \in \mathcal{V}_{i_0}$, da je $X_{i_0} = \bigcup_{j=1}^{k} U_j$. Odprto pokritje za X je torej $\{\pi_{i_0}^{-1}(U_j) \mid j = 1, 2, \ldots, k\}$.

Opomba 2. V dokazu smo pri izbiri $e \in X$ uporabili aksiom izbire.

Izrek 6 (Izrek Alexandra za podbaze). *Naj bo (X, τ) topološki prostor in naj bo $\mathcal{P}$ podbaza topologije τ. Če ima vsaka družina množic iz podbaze $\mathcal{P}$, ki pokrije X, končno poddružino, ki prav tako pokrije X, potem je X kompakten.*

Dokaz. Naj bo $\mathcal{P}$ podbaza za τ in naj za vsako pokritje X z množicami iz $\mathcal{P}$ obstaja končno podpokritje. Denimo, da X ni kompakten.

Množico vseh odprtih pokritij prostora X, ki nimajo končnega podpokritja, označimo z $\mathcal{F}$ in jo delno uredimo z inkluzijo. Množica $\mathcal{F}$ ni prazna, saj X ni kompakten. Naj bo $\{E_\alpha\}$ poljubna linearno urejena podmnožica množice $\mathcal{F}$. Pokažimo, da je $E = \bigcup_\alpha E_\alpha$ njena zgornja meja. Očitno je E pokritje za X, saj je unija pokritij. Pokazati moramo še, da ne obstaja neko končno podpokritje. Naj bo $\{U_1, U_2, \ldots, U_k\}$ neka končna podmnožica E. Potem za vsak $i \in \{1, 2, \ldots, k\}$ obstaja α_i, da je $U_i \in E_{\alpha_i}$. Ker je $\{E_\alpha\}$ linearno urejena, je tudi $\{E_{\alpha_1}, E_{\alpha_2}, \ldots, E_{\alpha_k}\} \subseteq \{E_\alpha\}$ linearno urejena in po lemi 1 sledi, da obstaja E_{α_0}, da je $E_{\alpha_i} \subseteq E_{\alpha_0}$ za vsak $i = 1, 2, \ldots, k$. To pomeni, da E_{α_0} vsebuje vse U_i, $i = 1, 2, \ldots, k$ in zato ne morejo biti pokritje za X, saj ne obstaja končno podpokritje pokritja E_{α_0}. Torej je E zgornja meja linearno urejene množice $\{E_\alpha\}$.

Po Zornovi lemi obstaja maksimalni element $\mathcal{M}$ množice $\mathcal{F}$. Pokažimo, da je $S := \mathcal{M} \cap \mathcal{P}$ pokritje za X. Če to ni res, obstaja $x_0 \in X$, ki ne pripada nobeni množici iz S. Ker je $\mathcal{M}$ pokritje za X, obstaja $O \in \mathcal{M}$, da je $x_0 \in O$. Obstajajo $V_1, V_2, \ldots, V_n \in \mathcal{P}$, da je $x_0 \in \bigcap_{j=1}^{n} V_j \subseteq O$, saj je $\mathcal{P}$ podbaza topologije. Nobena od množic V_j (za $j = 1, 2, \ldots n$) ni v $\mathcal{M}$, saj bi bil potem x_0 element neke množice iz S. Zaradi maksimalnosti $\mathcal{M}$, za vsak $j \in \{1, 2, \ldots, n\}$, družina množic $\mathcal{M} \cup \{V_j\}$ vsebuje končno podpokritje za X. Označimo $X = V_j \cup U_j$, kjer je U_j končna unija množic iz $\mathcal{M}$. Sledi

$$X = \bigcap_{j=1}^{n} (V_j \cup U_j) \subseteq \bigcap_{j=1}^{n} V_j \cup \bigcup_{j=1}^{n} U_j \subseteq O \cup \bigcup_{j=1}^{n} U_j,$$

kar pa je v protislovju z dejstvom, da $\mathcal{M}$ ne vsebuje končnega podpokritja. Torej je S pokritje za X.

Ker je S vsebovana v $\mathcal{P}$, po predpostavki obstaja končno podpokritje za X. Ker pa je S vsebovana tudi v $\mathcal{M}$, končno podpokritje ne obstaja, kar nas pripelje do protislovja s predpostavko, da X ni kompakten.

Pokažimo sedaj, da je izrek Tihonova ekvivalenten Zornovi lemi. Če predpostavimo, da Zornova lema velja, izrek Tihonova hitro sledi iz izreka Alexandra za podbaze in prejšnje leme. V drugo smer pa bomo pravzaprav dokazali aksiom izbire, a ker je ekvivalenten Zornovi lemi, bomo dokazali, da velja tudi ta. Konstruirali bomo primeren produkt kompaktnih prostorov, iz njegove kompaktnosti pa bo sledil obstoj funkcije izbire.

Izrek 7. *Zornova lema je ekvivalentna izreku Tihonova.*

Dokaz. Najprej predpostavimo, da velja Zornova lema, in označimo $X = \prod_{i \in \mathcal{I}} X_i$. Naj bo $\pi_i : X \to X_i$ projekcija za vsak $i \in \mathcal{I}$. Podbaza produktne topologije na X je družina

$$\mathcal{P} = \{\pi_i^{-1}(U) \mid U \in \tau_i, i \in \mathcal{I}\}.$$

Po lemi 5 vsako odprto pokritje prostora X z množicami iz $\mathcal{P}$ vsebuje končno podpokritje. Po izreku 6 sledi, da je X kompakten.

Če je X kompakten, sledi, da so za vsak $i \in \mathcal{I}$ tudi $\pi_i(X) = X_i$ kompaktni, saj so zvezne slike kompaktnega prostora.

Pokažimo še, da iz izreka Tihonova sledi Zornova lema. Predpostavimo, da velja izrek Tihonova. Pravzaprav bomo pokazali, da potem velja aksiom izbire, a ker sta z Zornovo lemo ekvivalentna, velja tudi ta. Naj bo $(X_\alpha)_{\alpha \in \Lambda}$ družina nepraznih množic.

Najprej bomo definirali družino topoloških prostorov, za katere bomo pokazali, da so kompaktni. Po izreku Tihonova bo sledilo, da je tudi njihov produkt kompakten. Od tod bomo sklepali, da je produkt $\prod_{\alpha \in \Lambda} X_\alpha$ neprazen.

Naj bo ∞ neka točka, ki ni v nobenem X_α, in naj bo $Y_\alpha = X_\alpha \cup \{\infty\}$ topološki prostor s topologijo $\tau_\alpha = \{\emptyset, \{\infty\}, X_\alpha, Y_\alpha\}$ za vsak $\alpha \in \Lambda$. Prostor je očitno kompakten, saj imamo le končno mnogo odprtih množic, torej je vsako odprto pokritje končno.

Označimo z Y produkt prostorov $\prod_{\alpha \in \Lambda} Y_\alpha$ in ga opremimo s produktno topologijo. Po izreku Tihonova je produkt Y kompakten. Za vsak $\alpha \in \Lambda$ naj bo Z_α tista podmnožica prostora Y, ki vsebuje vse točke, katerih α koordinata leži v X_α. Množica Z_α je zaprta v Y, saj je X_α zaprta v Y_α.

Naj bo $\Delta \subset \Lambda$ končna podmnožica. Končen presek $\bigcap_{\alpha \in \Delta} Z_\alpha$ je neprazen, saj lahko izberemo $x_\alpha \in X_\alpha$ za $\alpha \in \Delta$ (končno izbir) ter nastavimo $x_\alpha = \infty$ za $\alpha \in \Lambda \setminus \Delta$. Pokažimo, da je presek

$\bigcap_{\alpha\in\Lambda} Z_\alpha$ neprazen. Če to ni res, potem je

$$Y = \left(\bigcap_{\alpha\in\Lambda} Z_\alpha\right)^c = \bigcup_{\alpha\in\Lambda} Z_\alpha^c.$$

Torej je $\{Z_\alpha^c\}_{\alpha\in\Lambda}$ odprto pokritje za Y, saj so Z_α zaprte množice. Iz kompaktnosti sledi, da obstaja končno podpokritje $\{Z_\alpha^c\}_{\alpha\in\Gamma}$, kar pomeni $\bigcap_{\alpha\in\Gamma} Z_\alpha = \emptyset$. Tako pridemo do protislovja, saj smo prej pokazali, da je presek $\bigcap_{\alpha\in\Delta} Z_\alpha$ neprazen za vsako končno podmnožico $\Delta \subset \Lambda$.

Ker je $\prod_{\alpha\in\Lambda} X_\alpha$ ravno presek $\bigcap_{\alpha\in\Lambda} Z_\alpha$ in ker je ta presek neprazen, je tudi $\prod_{\alpha\in\Lambda} X_\alpha$ neprazen.

3. Uporaba v teoriji grup

V tem razdelku si bomo ogledali uporabo Zornove leme v teoriji grup na primeru spodnjega izreka.

Izrek 8. *Naj bo D deljiva grupa, A Abelova grupa in $B \subset A$ njena podgrupa. Homomorfizem $f : B \to D$ lahko razširimo do homomorfizma $\widetilde{f} : A \to D$.*

Najprej definirajmo deljivost Abelovih grup.

Definicija 4. Abelova grupa $(G, +)$ je *deljiva*, če za vsak $n \in \mathbb{N}$ in vsak $g \in G$ obstaja $h \in G$, da velja $nh = g$.

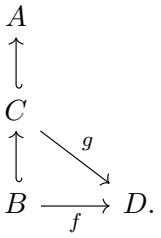
V dokazu bomo potrebovali tudi naslednjo lemo, ki pove, kakšne oblike so podgrupe aditivne grupe celih števil.

Lema 9. *Podmnožica P aditivne grupe $(\mathbb{Z}, +)$ je njena podgrupa natanko tedaj, ko je $P = n\mathbb{Z}$ za neki $n \in \mathbb{N} \cup \{0\}$.*

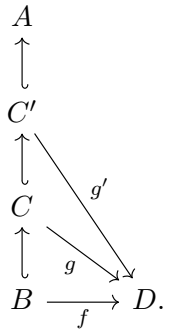
Dokaz. Pokažimo najprej, da je $P = n\mathbb{Z}$ podgrupa $\mathbb{Z}$. Naj bosta nz_1 in nz_2 iz P za neka $z_1, z_2 \in \mathbb{Z}$. Ker je $nz_1 - nz_2 = n(z_1 - z_2)$ iz P, je P podgrupa $\mathbb{Z}$.

Sedaj privzemimo, da je P podgrupa $\mathbb{Z}$. Če je $P = \{0\}$, smo končali. Sicer pa P vsebuje neko neničelno celo število p, torej tudi $-p$. V P označimo z n element, ki je najmanjši izmed naravnih števil. Potem so tudi $nz \in P$ za $z \in \mathbb{Z}$. Torej je $n\mathbb{Z} \subseteq P$. Pokažimo še inkluzijo v drugo smer. Element $k \in P$ lahko zapišemo kot $k = qn + r$ za neka $q \in \mathbb{Z}$ in $0 \le r \le n-1$. Sledi $r = k - qn \in P$, kar pa pomeni, da je $r = 0$, saj bi sicer zaradi pogoja $0 \le r \le n-1$ v P obstajalo manjše naravno število od n. Torej je $k = qn \in n\mathbb{Z}$ in zato $P \subseteq n\mathbb{Z}$.

Dokaz (izreka). Definirajmo S kot množico parov (C, g), kjer je C podgrupa grupe A, za katero velja, da je B njena podgrupa, g pa homomorfizem iz C v D, za katerega je $g|_B = f$, kot je prikazano na spodnjem diagramu.



Množico delno uredimo: za $(C, g), (C', g')$ iz S je $(C, g) \leq (C', g')$, če je $C \subseteq C'$ in $g'|_C = g$.



Vidimo, da S ni prazna, saj je $(B, f) \in S$. S pomočjo Zornove leme bomo dokazali obstoj maksimalnega elementa (M, h), za katerega bomo pokazali, da je $M = A$. Torej bo h ravno homomorfizem, ki ga želimo, saj je $h|_B = f$.

Vzemimo poljubno linearno urejeno podmnožico $\{(C_\alpha, g_\alpha)\}_{\alpha\in\Lambda}$ in pokažimo, da obstaja zgornja meja. Naj bo $C := \bigcup_{\alpha\in\Lambda} C_\alpha$ ter preverimo, da je to podgrupa A. Za $c_1, c_2 \in C$ obstajata C_{α_1} in C_{α_2}, da je $c_i \in C_{\alpha_i}$. Brez škode za splošnost lahko predpostavimo $c_1, c_2 \in C_{\alpha_2}$ (linearna urejenost). Sledi $c_1 - c_2 \in C_{\alpha_2} \subseteq C$. Definirajmo še preslikavo $g : C \to D$ za $x \in C_\alpha$ s predpisom $g(x) = g_\alpha(x)$. Preveriti moramo, da je dobro definirana. Naj bo x element C_β in C_γ. Zaradi linearne urejenosti je $(C_\beta, g_\beta) \leq (C_\gamma, g_\gamma)$ ali $(C_\gamma, g_\gamma) \leq (C_\beta, g_\beta)$. Brez škode za splošnost naj bo $(C_\beta, g_\beta) \leq (C_\gamma, g_\gamma)$. Torej je $x \in C_\beta \subseteq C_\gamma$ ter $g_\gamma|_{C_\beta} = g_\beta$, kar pomeni $g_\beta(x) = g_\gamma(x)$. Preslikava g je homomorfizem, saj sta poljubna $x, y \in C$ elementa istega C_δ za neki δ (zaradi linearne urejenosti), torej je

$$g(x + y) = g_\delta(x + y) = g_\delta(x) + g_\delta(y) = g(x) + g(y).$$

Ker za vse $\alpha \in \Lambda$ velja, da je $g_\alpha|_B = f$, je $g|_B = f$. Od tod sledi, da je (C, g) element S in tako zgornja meja množice $\{(C_\alpha, g_\alpha)\}_{\alpha\in\Lambda}$.

Uporabimo Zornovo lemo, ki nam zagotovi obstoj maksimalnega elementa (M, h) v S. S protislovjem bomo pokazali, da je $M = A$ tako, da bomo skonstruirali neki element množice S, ki je strogo večji od (M, h), kar nas bo pripeljalo do protislovja z maksimalnostjo (M, h). Najprej preverimo, da obstaja ustrezna podgrupa grupe A, nato pa, da obstaja razširitev homomorfizma h na to podgrupo.

Če $M \neq A$, potem obstaja $a \in A$, ki ni v M. Preverimo, da je $\langle M, a\rangle = M + \mathbb{Z}a$ podgrupa A. Naj bosta $m_1 + z_1a$ in $m_2 + z_2a$ iz $\langle M, a\rangle$. Potem je tudi $(m_1 + z_1a) - (m_2 + z_2a) = (m_1 - m_2) + (z_1 - z_2)a \in \langle M, a\rangle$. Očitno je B njena podgrupa, saj je B podgrupa M.

Za razširitev homomorfizma h na $\langle M, a\rangle$ si pomagajmo s podgrupo $\{k \in \mathbb{Z} \mid ka \in M\}$ grupe $\mathbb{Z}$, ki je po lemi 9 enaka $\{0\}$ ali $n\mathbb{Z}$ za neki $n \in \mathbb{N}$. Če je enaka $\{0\}$, potem je zapis $m + ka$ za $m \in M$ ter $k \in \mathbb{Z}$ za poljubni element iz $\langle M, a\rangle$ enoličen, saj $na \notin M$ za vse $n \in \mathbb{N}$. Homomorfizem $h' : \langle M, a\rangle \to D$, določen s predpisom $h'(m + za) = h(m)$, je torej dobro definiran in velja $h'|_M = h$. V primeru, ko pa je $\{k \in \mathbb{Z} \mid ka \in M\}$ enaka $n\mathbb{Z}$ za neki $n \in \mathbb{N}$, pa je na element M. Če želimo h razširiti do homomorfizma $h' : \langle M, a\rangle \to D$, mora veljati $nh'(a) = h'(na) = h(na)$. Ker je D deljiva grupa, obstaja $d \in D$, da je $nd = h(na)$. Torej nastavimo $h'(a) = d$ in predpis preslikave h' definiramo kot

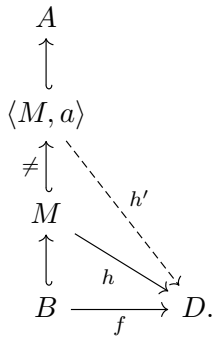
$$h'(m + ka) = h(m) + kd.$$

Preverimo, da je h' dobro definirana. Naj bo $m_1 + z_1a = m_2 + z_2a \in \langle M, a\rangle$. Pokazali bomo, da je $h'(m_1 + z_1a) = h'(m_2 + z_2a)$. Velja $(z_1 - z_2)a = m_2 - m_1 \in M$, torej je $z_1 - z_2 \in \{k \in \mathbb{Z} \mid ka \in$

$M\} = n\mathbb{Z}$. Zapišemo lahko $z_1 = z_2 + nw$ za neki $w \in \mathbb{Z}$. Računamo:

$$\begin{aligned} h'(m_1 + z_1 a) &= h(m_1) + z_1 d = h(m_1) + z_2 d + w(nd) \\ &= h(m_1) + z_2 d + w h'(na) = h'(m_1 + wna) + z_2 d \\ &= h'(m_1 + (z_1 - z_2)a) + z_2 d = h'(m_1 + z_1 a - z_2 a) + z_2 d \\ &= h(m_2 + z_2 a - z_2 a) + z_2 d = h'(m_2 + z_2 a). \end{aligned}$$

Vidimo, da je preslikava dobro definirana, s preprostim računom in uporabo dejstva, da je h homomorfizem, pa lahko preverimo, da je h' homomorfizem.



Sledi $(M, h) \leq (\langle M, a\rangle, h')$, M pa je prava podgrupa $\langle M, a\rangle$, kar nas pripelje do protislovja z maksimalnostjo (M, h). Torej je $M = A$.

4. Uporaba v teoriji kolobarjev

Oglejmo si še nekaj primerov uporabe Zornove leme na idealih in modulih. Kolobarje definiramo tako, da vsebujejo enoto za množenje. V nekomutativnih kolobarjih definiramo leve ideale na naslednji način.

Definicija 5. Naj bo K kolobar. Množica $I \subseteq K$ je *levi ideal* kolobarja K, če velja:

1. I je podgrupa za seštevanje,
2. za vse $k \in K$ in $a \in I$ je $ka \in I$.

Na analogen način definiramo desne ideale (v točki (2) mora veljati $ak \in I$). V komutativnih kolobarjih definiciji sovpadata, objektu I pa pravimo *ideal kolobarja* K, ter označimo $I \triangleleft K$.

Definicija 6. Naj bo K kolobar in I njegov levi ideal. Če ne obstaja tak levi ideal J, da bi veljalo $I \subsetneq J \subsetneq K$ ter $I \neq K$, potem je I *maksimalen levi ideal* kolobarja K.

Sedaj imamo pripravljene vse definicije in se lahko lotimo prvega izreka.

Izrek 10. *Vsak neničelni kolobar vsebuje maksimalni levi ideal.*

Dokaz. Naj bo K neničelni kolobar. Definirajmo S kot množico vseh pravih levih idealov kolobarja K. Na njej definiramo relacijo delne urejenosti z inkluzijo (za $A, B \in S$ velja $A \leq B$, če $A \subseteq B$). Ker je $\{0\}$ levi ideal in ker je kolobar neničeln, je S neprazna.

Da lahko uporabimo Zornovo lemo, moramo pokazati, da ima vsaka linearno urejena podmnožica množice S zgornjo mejo. Naj bo torej $T \subseteq S$ linearno urejena. Pokazali bomo, da je

$$Z = \bigcup_{A \in T} A$$

zgornja meja za množico T. Najprej pokažimo, da je to levi ideal. Naj bosta x in y iz Z. Velja $x \in I_\alpha$ ter $y \in I_\beta$ za neka $I_\alpha, I_\beta \in T$. Ker je T linearno urejena, je $I_\alpha \leq I_\beta$ ali $I_\beta \leq I_\alpha$. Brez škode za splošnost lahko privzamemo $I_\alpha \leq I_\beta$, zato je tako x kot y v I_β in ker je I_β levi ideal, velja $x - y \in I_\beta$. Torej je Z podgrupa za seštevanje. Pokazati moramo še, da za vse $k \in K$ in $x \in Z$ velja $kx \in Z$. Ker je I_α levi ideal, je $kx \in I_\alpha$ za vse $k \in K$. Torej je Z res levi ideal kolobarja K, ker pa vsebuje vse leve ideale iz linearno urejene množice T, je to zgornja meja te množice, če leži v S (če je pravi levi ideal). Denimo, da ni. Potem Z vsebuje enoto. Ker je Z unija levih idealov iz T, mora obstajati levi ideal $I \in T$, ki vsebuje enoto. Po definiciji množice S pa tak levi ideal ne obstaja, kar nas pripelje do protislovja.

Po Zornovi lemi sledi, da ima S maksimalni element. Torej obstaja maksimalni levi ideal kolobarja K.

Enako bi dokazali, da vsak neničelni kolobar vsebuje kak maksimalni desni ideal. Za neničelne komutativne kolobarje torej velja, da vsebujejo maksimalne ideale. V nadaljevanju bomo potrebovali kvocientne kolobarje, definirane v [9, III. poglavje]. Preslikavi $\pi : K \to K/I$, definirani s predpisom

$$\pi(a) = a + I,$$

pravimo kanonični epimorfizem kolobarjev. Zanjo velja $\ker(\pi) = I$ [9, stran 104].

Oglejmo si naslednjo posledico izreka 10.

Posledica 11. *Vsak pravi ideal neničelnega komutativnega kolobarja je vsebovan v maksimalnem idealu.*

Dokaz. Naj bo K neničelni komutativen kolobar in $I \lhd K$ njegov pravi ideal. Tedaj je kvocientni kolobar K/I neničeln in komutativen. Po izreku 10 torej obstaja maksimalni ideal M kolobarja K/I. Naj bo $\pi : K \to K/I$ kanonični epimorfizem. Pokažimo, da je $\pi^{-1}(M)$ maksimalni ideal kolobarja K, ki vsebuje ideal I. Ker je $\pi(0) \in M$, $\pi^{-1}(M)$ gotovo vsebuje I. Množica $\pi^{-1}(M)$ je ideal, saj je praslika ideala, maksimalnost $\pi^{-1}(M)$ pa sledi iz izreka o korespondenci idealov [1, izrek 2.3.5].

Spomnimo se definicije praideala. Ideal $I \lhd K$ je *praideal* kolobarja K, če je pravi ideal in za poljubna $x, y \in K$ iz $xy \in I$ sledi $x \in I$ ali $y \in I$. Definirajmo še multiplikativno množico.

Definicija 7. Neprazni podmnožici $\mathcal{S}$ kolobarja K rečemo *multiplikativna množica*, če za poljubna $x, y \in \mathcal{S}$ velja, da je tudi produkt xy element $\mathcal{S}$.

S preprostima računoma preverimo naslednjo lemo, ki jo bomo potrebovali v izreku 13.

Lema 12. *Naj bo K kolobar in $I, J \lhd K$ njegova leva ideala. Potem je tudi $I + J := \{x + y \mid x \in I, y \in J\}$ levi ideal kolobarja K.*

Dokaz. Preverimo, da je podgrupa za seštevanje. Naj bodo $x_1, x_2 \in I$ in $y_1, y_2 \in J$. Velja:

$$(x_1 + y_1) - (x_2 + y_2) = (x_1 - x_2) + (y_1 - y_2) \in I + J,$$

saj je seštevanje komutativno in asociativno.

Naj bodo sedaj $x \in I$, $y \in J$ ter $k \in K$. Velja

$$k(x + y) = kx + ky \in I + J.$$

Sedaj se lahko lotimo izreka.

Izrek 13. *Naj bo $\mathcal{S}$ multiplikativna množica komutativnega kolobarja K in $0 \notin \mathcal{S}$. Glede na relacijo inkluzije obstaja maksimalni element množice $\{I \lhd K \mid I \cap \mathcal{S} = \emptyset\}$. Ta maksimalni element je praideal.*

Dokaz. Označimo $A = \{I \lhd K \mid I \cap \mathcal{S} = \emptyset\}$ in jo delno uredimo z relacijo inkluzije. Pokažimo, da maksimalni element množice obstaja. Množica A je neprazna, saj vsebuje $\{0\}$. Preverimo, da ima vsaka linearno urejena podmnožica množice A zgornjo mejo. Naj bo $\{I_\alpha\}_{\alpha\in\Lambda}$ poljubna linearno urejena množica. Pokažimo, da je $I = \bigcup_{\alpha\in\Lambda} I_\alpha$ zgornja meja. Da je I ideal, vemo iz dokaza izreka 10, gotovo pa vsebuje vse I_α. Očitno je tudi, da je $I \cap \mathcal{S} = \emptyset$, saj je presek $I_\alpha \cap \mathcal{S}$ prazen za vsak $\alpha \in \Lambda$. Torej je $I \in A$ zgornja meja in Zornova lema nam zagotavlja obstoj maksimalnega elementa.

Označimo s P maksimalni element množice A, ki je pravi ideal kolobarja K, saj velja $P \cap \mathcal{S} = \emptyset$. Preverimo, da je P praideal. Naj bosta x in y poljubna elementa v K in naj bo $xy \in P$. Pokažimo, da je $x \in P$ ali $y \in P$. Če to ni res, potem sta $(x) + P$ in $(y) + P$ po lemi 12 ideala, ki sta oba strogo večja od P, torej ne ležita v A. To pomeni, da obstajata s_1 in s_2 iz $\mathcal{S}$, da je $s_1 \in (x) + P$ ter $s_2 \in (y) + P$. Torej lahko zapišemo

$$s_1 = ax + p_1 \text{ in } s_2 = by + p_2$$

za neke $a, b \in K$ ter $p_1, p_2 \in P$. Če s_1 in s_2 zmnožimo, dobimo

$$s_1 s_2 = (ax + p_1)(by + p_2) = abxy + axp_2 + byp_1 + p_1p_2.$$

Ker je P ideal in je $xy \in P$, je $abxy + axp_2 + byp_1 + p_1p_2 \in P$, torej $s_1s_2 \in P$. Ker pa je množica $\mathcal{S}$ multiplikativna, velja $s_1s_2 \in \mathcal{S}$, kar pa nas pripelje do protislovja. Torej je $x \in P$ ali $y \in P$, kar pomeni, da je P praideal, ki ne vsebuje nobenega elementa množice $\mathcal{S}$.

Definirajmo *nilpotentni element* r kolobarja K kot element, za katerega velja $r^n = 0$ za neki $n \geq 1$. Naslednja posledica nam pove, da če vemo, da neki element leži v vsakem praidealu, potem mora biti neka njegova potenca enaka 0.

Posledica 14. *Presek vseh praidealov v komutativnem kolobarju je množica vseh nilpotentnih elementov kolobarja.*

Dokaz. Naj bo K komutativni kolobar. Najprej pokažimo, da presek praidealov vsebuje množico nilpotentnih elementov kolobarja. Naj bo P poljuben praideal in r neki nilpotenten element (torej $r^n = 0$ za neki $n \geq 1$). Velja, da je $r^n \in P$. Ker je P praideal, je $r \in P$ ali $r^{n-1} \in P$. Torej je $r \in P$ ali $r^{n-2} \in P$. Nadaljujemo in dobimo $r \in P$.

Pokažimo sedaj, da množica vseh nilpotentnih elementov kolobarja vsebuje presek praidealov, torej, da so v preseku vseh praidealov le nilpotentni elementi. Pravzaprav bomo pokazali, da element, ki ni nilpotenten, ne leži v nekem praidealu. Naj bo r poljuben element, ki ni nilpotenten (torej $r^n \neq 0$ za vsak $n \geq 1$). Potem je množica $\mathcal{S} := \{r^m \mid m \in \mathbb{N}\}$ multiplikativna in po izreku 13 obstaja praideal P, za katerega je $P \cap \mathcal{S} = \emptyset$. Torej $r \notin P$.

Tudi naslednji izrek se nanaša na praideale komutativnega kolobarja, še prej pa se spomnimo, kdaj so ideali komutativnega kolobarja končno generirani. Ideal I nad komutativnim kolobarjem K je končno generiran, če obstaja končna podmnožica $\{h_1, h_2, \ldots, h_m\} \subseteq I$, da je $I = Kh_1 + Kh_2 + \cdots + Kh_m$, kar krajše zapišemo $I = (h_1, h_2, \ldots, h_m)$. Sedaj se lahko lotimo izreka.

Izrek 15 (Cohen). *Če so vsi praideali komutativnega kolobarja končno generirani, potem so vsi ideali kolobarja končno generirani.*

Dokaz. Naj bo K komutativen kolobar. Pokazali bomo nasprotno, torej, če obstaja ideal, ki ni končno generiran, potem obstaja praideal v kolobarju K, ki ni končno generiran. Ta praideal bomo iskali kot maksimalni element neke množice, katere elementi niso končno generirani.

Definirajmo torej S kot množico vseh idealov kolobarja K, ki niso končno generirani. Množica S ni prazna, saj predpostavljamo, da obstaja neki ideal, ki ni končno generiran. Uredimo S z inkluzijo in si oglejmo poljubno linearno urejeno podmnožico $\{I_\alpha\}_{\alpha\in\Lambda}$. Definirajmo $I = \bigcup_{\alpha\in\Lambda} I_\alpha$ in pokažimo, da je zgornja meja. Podobno kot v dokazu izreka 10 pokažemo, da I je ideal, ki očitno vsebuje vse I_α. Preveriti moramo še, da I ni končno generiran, torej, da je element S. Pa denimo, da I je končno generiran, kar zapišemo kot $I = (x_1, x_2, \ldots, x_n)$ za neki $n \in \mathbb{N}$. Obstajajo taki $\alpha_1, \alpha_2, \ldots, \alpha_n$, da so $x_i \in I_{\alpha_i}$ za $i = 1, 2, \ldots, n$. Ker je $\{I_{\alpha_1}, I_{\alpha_2}, \ldots, I_{\alpha_n}\} \subseteq \{I_\alpha\}_{\alpha\in\Lambda}$ linearno urejena, po lemi 1 obstaja I_{α_j} za neki $j \in \{1, 2, \ldots, n\}$, za katerega je $\{x_1, x_2, \ldots, x_n\} \subseteq I_{\alpha_j}$. Torej velja $I \subseteq I_{\alpha_j}$, kar pravzaprav pomeni $I = I_{\alpha_j}$, saj je I unija vseh I_α. Od tod sledi, da je tudi I_{α_j} končno generiran, kar nas pripelje do protislovja. Torej I ni končno generiran.

Zornova lema nam zagotovi obstoj maksimalnega elementa množice S, ki ga označimo s P. Ta ni končno generiran in je ideal kolobarja K. Pokažimo, da je tudi praideal. Očitno je P pravi ideal, saj bi bil sicer končno generiran z 1. Preverimo še, da iz $xy \in P$ sledi $x \in P$ ali $y \in P$. Če temu ni tako, potem je $(x) + P$ ideal (to nam pove lema 12), ki vsebuje P in je od njega različen. Torej $(x) + P \notin S$, saj je P maksimalen za S, kar pomeni, da je $(x) + P$ končno generiran. Zapišemo lahko

$$(x) + P = (r_1, r_2, \ldots, r_k) \text{ za neki } k \in \mathbb{N} \text{ in neke } r_1, r_2, \ldots, r_k \in K.$$

Za vsak $i = 1, 2, \ldots, k$ lahko $r_i \in (x) + P$ zapišemo v obliki

$$r_i = a_i x + p_i \text{ za neka } a_i \in K \text{ in } p_i \in P.$$

Potem velja, da je r_i element ideala $(x, p_1, p_2, \ldots, p_k)$ za $i = 1, 2, \ldots, k$. Sledi, da je

$$(x) + P = (x, p_1, p_2, \ldots, p_k),$$

saj so tudi vsi $p_i \in (x) + P$.

Naj bo $p \in P$ poljuben element. Ker velja $P \subset (x) + P$, lahko zapišemo

$$p = c_0 x + c_1 p_1 + c_2 p_2 + \cdots + c_k p_k, \tag{1}$$

kjer so c_i elementi K za $i = 0, 1, \ldots, k$. Velja, da je $c_0 x = p - \sum_{i=1}^{k} c_i p_i \in P$, kar pomeni, da element c_0 leži v $J = \{r \in K \mid rx \in P\}$. Preverimo, da je J ideal. Naj bosta j_1 in j_2 iz J. Potem sta $j_1 x$ in $j_2 x$ iz P, torej je tudi $j_1 x - j_2 x = (j_1 - j_2)x$ iz P. Sledi, da je $j_1 - j_2 \in J$, kar pomeni, da je J podgrupa za seštevanje. Za $k \in K$ ter $j \in J$ velja, da sta elementa jx ter kjx v P. Torej je kj element J in J je res ideal. Očitno je $P \subseteq J$, saj za $q \in P$ velja, da je $qx \in P$, ker je P ideal in zato $q \in J$. Ker velja $xy \in P$, je $y \in J$. Od tod vidimo, da je $P \neq J$, saj y ni element P. Ideal J je torej končno generiran, saj je P maksimalen v množici idealov, ki niso končno generirani. Iz enačbe (1) sledi $p \in xJ + \sum_{i=1}^{k} Kp_i$, kar pomeni, da je $P \subseteq xJ + \sum_{i=1}^{k} Kp_i$. Velja tudi, da je $xJ \subseteq P$ in $\sum_{i=1}^{k} Kp_i \subseteq P$. Od tod sledi

$$P = xJ + \sum_{i=1}^{k} Kp_i,$$

kar pomeni, da je P končno generiran, saj je J končno generiran. To nas pripelje do protislovja s predpostavko $x \notin P$ in $y \notin P$. Veljati mora $x \in P$ ali $y \in P$, od koder sledi, da je P praideal, ki ni končno generiran.

Naslednji izrek bo posplošitev izreka 15 na module nad kolobarji. Oba izreka sta predstavljena, saj moramo proti koncu dokaza naslednjega izreka pokazati še nekaj dodatnih stvari. Moduli nad kolobarji so pravzaprav posplošitve vektorskih prostorov nad polji. Če bi bil kolobar tudi polje, bi namreč dobili ravno vektorski prostor. Še formalno definirajmo, kaj je modul nad kolobarjem.

Definicija 8. Naj bo K kolobar. Abelova grupa $(M,+)$, skupaj z operacijo $\cdot : K \times M \to M$, je *levi modul* nad kolobarjem K, če za vse $a, b \in K$ in $x, y \in M$ velja:

1. $a \cdot (x+y) = a \cdot x + a \cdot y$,
2. $(a+b) \cdot x = a \cdot x + b \cdot x$,
3. $(ab) \cdot x = a \cdot (b \cdot x)$,
4. $1 \cdot x = x$.

Operacijo $\cdot : K \times M \to M$ imenujemo *množenje s skalarjem*. Ker se bomo ukvarjali le z levimi moduli, jim bomo v nadaljevanju rekli kar moduli. Potrebovali bomo naslednjo definicijo.

Definicija 9. Naj bo M modul nad K in N podgrupa M. Če je za vse $n \in N$ in $k \in K$ produkt kn element N, potem je N *podmodul* modula M.

Naj bo sedaj K kolobar, $\mathfrak{a} \triangleleft K$ njegov ideal in M modul nad K. Potem označimo z $\mathfrak{a}M$ množico vseh končnih vsot produktov elementov iz $\mathfrak{a}$ in M, torej

$$\mathfrak{a}M = \left\{ \sum_{i=1}^{n} a_i m_i \mid a_i \in \mathfrak{a}, m_i \in M, n \in \mathbb{N} \right\}.$$

Lema 16. *Množica $\mathfrak{a}M$ je podmodul modula M.*

Dokaz. Pokažimo, da je $\mathfrak{a}M$ podgrupa za seštevanje grupe M. Naj bosta $x, y \in \mathfrak{a}M$. Zapišemo lahko $x = \sum_{i=1}^{n_1} a_i g_i$ in $y = \sum_{i=1}^{n_2} b_i h_i$, kjer so $a_i, b_i \in \mathfrak{a}$ in $g_i, h_i \in M$. Preveriti moramo, da je $x - y \in \mathfrak{a}M$. Velja $-b_i \in \mathfrak{a}$, saj je $\mathfrak{a}$ podgrupa za seštevanje, torej je

$$x - y = \sum_{i=1}^{n_1} a_i g_i - \sum_{i=1}^{n_2} b_i h_i = \sum_{i=1}^{n_1} a_i g_i + \sum_{i=1}^{n_2} (-b_i) h_i \in \mathfrak{a}M.$$

Naj bo $k \in K$. Potem je

$$kx = k \sum_{i=1}^{n} a_i g_i = \sum_{i=1}^{n} (k a_i) g_i,$$

ker pa je $\mathfrak{a}$ ideal, je $ka_i \in \mathfrak{a}$ za vsak i. Od tod sledi, da je $kx \in \mathfrak{a}M$, kar pomeni, da je $\mathfrak{a}M$ podmodul M.

Definirajmo pojem anihilatorja, ki ga bomo nato uporabili v dokazu izreka 18.

Definicija 10. Naj bo M modul nad kolobarjem K in S neprazna podmnožica M. *Anihilator* množice S je množica

$$\mathrm{Ann}_K(S) = \{k \in K \mid ks = 0 \text{ za vse } s \in S\}.$$

Pokažimo naslednjo lemo, povezano z anihilatorji.

Lema 17. *Naj bodo A_i podmoduli modula M za $i = 1, 2, \ldots, n$. Potem je*

$$\mathrm{Ann}_K(A_1 + A_2 + \cdots + A_n) = \bigcap_{i=1}^{n} \mathrm{Ann}_K(A_i).$$

Dokaz. Naj bo $k \in \bigcap_{i=1}^{n} \mathrm{Ann}_K(A_i)$. Torej je $ka_i = 0$ za vsak $a_i \in A_i$ in od tod sledi $ka_1 + ka_2 + \cdots + ka_n = k(a_1 + a_2 + \cdots + a_n) = 0$. Torej je k element $\mathrm{Ann}_K(A_1 + A_2 + \cdots + A_n)$. Obratna smer je očitna.

Spomnimo se še, da je modul M nad kolobarjem K končno generiran, če obstaja končna podmnožica $\{g_1, g_2, \ldots, g_n\} \subseteq M$, da je $M = Kg_1 + Kg_2 + \cdots + Kg_n$, kar krajše zapišemo $M = (g_1, g_2, \ldots, g_n)$.

Izrek 18. *Naj bo M končno generiran modul nad komutativnim kolobarjem K. Če je za vsak praideal $\mathfrak{p}$ podmodul $\mathfrak{p}M$ končno generiran, potem je vsak podmodul M končno generiran.*

Dokaz. Tako kot v izreku 15 bomo pokazali nasprotno, torej, če M vsebuje kak podmodul, ki ni končno generiran, potem tudi $\mathfrak{p}M$ ni za neki praideal $\mathfrak{p}$.

Naj bo K kolobar in M končno generiran modul nad K. Definirajmo S kot množico podmodulov modula M, ki niso končno generirani, ter jo delno uredimo z relacijo inkluzije. Po predpostavki je S neprazna. Preverimo, da ima vsaka linearno urejena podmnožica $\{I_\alpha\}_{\alpha\in\Lambda}$ zgornjo mejo v S.

Unija $I = \bigcup_{\alpha\in\Lambda} I_\alpha$ očitno vsebuje vse I_α. Pokažimo, da je I podmodul M. Za $x, y \in I$ obstajata $I_1, I_2 \in \{I_\alpha\}_{\alpha\in\Lambda}$, da je $x \in I_1$ in $y \in I_2$. Zaradi linearne urejenosti brez škode za splošnost predpostavimo $I_1 \leq I_2$, torej $x, y \in I_2$. Od tod sledi $x - y \in I_2 \subseteq I$, kar pomeni, da je I podgrupa za seštevanje. Naj bo $k \in K$ ter $z \in I$. Ponovno obstaja $I_0 \in \{I_\alpha\}_{\alpha\in\Lambda}$, da je $z \in I_0$, torej $kz \in I_0 \subseteq I$. Sledi, da je I podmodul. Preveriti moramo še, da ni končno generiran, torej, da je element S. Če bi bil, bi lahko zapisali $I = (g_1, g_2, \ldots, g_n)$ za neki $n \in \mathbb{N}$. Obstajajo taki I_{α_i}, da velja $g_i \in I_{\alpha_i}$ za vse $i = 1, 2, \ldots, n$. Po lemi 1 obstaja I_{α_j} za neki $j \in \{1, 2, \ldots, n\}$, ki vsebuje vse I_{α_i}, torej $g_1, g_2, \ldots, g_n \in I_{\alpha_j}$. Od tod sledi $I \subseteq I_{\alpha_j}$. Ker pa je I unija $\{I_\alpha\}_{\alpha\in\Lambda}$, je $I = I_{\alpha_j}$, kar pa nas pripelje do protislovja, saj to pomeni, da je I_{α_j} končno generiran. Vsaka linearno urejena podmnožica torej ima zgornjo mejo.

Iz Zornove leme sledi, da obstaja maksimalni element množice S, ki ga označimo z N. Očitno $N \neq M$, saj $M \notin S$, ker je končno generiran. Vsak podmodul modula M, ki strogo vsebuje N, je torej končno generiran. V dveh korakih bomo pokazali, da obstaja tak praideal $\mathfrak{p}$, da $\mathfrak{p}M$ ni končno generiran. Najprej, da je $\mathfrak{p} := \mathrm{Ann}_K(M/N)$ praideal kolobarja K, nato pa, da $\mathfrak{p}M$ ni končno generiran.

Za $\mathfrak{p}$ velja

$$\begin{aligned}\mathfrak{p} = \mathrm{Ann}_K(M/N) &= \{k \in K \mid k(m+N) = 0 + N, m \in M\} \\ &= \{k \in K \mid km + N = 0 + N, m \in M\} \\ &= \{k \in K \mid km \in N, m \in M\} \\ &= \{k \in K \mid kM \subseteq N\}.\end{aligned}$$

Opazimo, da $\mathfrak{p} \neq K$, saj bi bil sicer $M \subseteq N$, vemo pa $N \subsetneq M$. Denimo, da $\mathfrak{p}$ ni praideal. Naj bo $xy \in \mathfrak{p}$ za neka elementa $x, y \in K \setminus \mathfrak{p}$. To pomeni

$$xyM \subseteq N,\ xM \not\subseteq N \text{ in } yM \not\subseteq N.$$

Od tod sledi, da $xM + N$ strogo vsebuje N, kar pomeni, da je končno generiran. Naj bodo $xm_i + n_i$ za $m_i \in M$ in $n_i \in N$ generatorji modula $xM + N$, $i = 1, 2, \ldots, l$. Potem lahko vsak element $a \in xM + N$ zapišemo kot $a = \sum_{i=1}^{l} k_i(xm_i + n_i)$, torej je

$$xM + N = \sum_{i=1}^{l} K(xm_i + n_i) = \sum_{i=1}^{l} Kxm_i + \sum_{i=1}^{l} Kn_i.$$

Poljuben $n \in N \subset xM + N$ lahko tako zapišemo v obliki:

$$\begin{aligned} n &= k_1xm_1 + k_2xm_2 + \cdots + k_lxm_l + k_1'n_1 + k_2'n_2 + \cdots + k_l'n_l \\ &= x(k_1m_1 + k_2m_2 + \cdots + k_lm_l) + k_1'n_1 + k_2'n_2 + \cdots + k_l'n_l, \end{aligned} \tag{2}$$

kjer so $k_i, k_i' \in K$.

Definirajmo L kot množico $\{m \in M \mid xm \in N\}$ in pokažimo, da je podmodul M. Za $l_1, l_2 \in L$ velja, da je $xl_1, xl_2 \in N$, od koder dobimo $xl_1 - xl_2 = x(l_1 - l_2) \in N$. Sledi, da je L podgrupa za seštevanje, saj je $l_1 - l_2 \in L$. Naj bosta $k \in K$ ter $l_0 \in L$ poljubna elementa. Torej je $xl_0 \in N$. Ker je N modul, je $kxl_0 \in N$, zaradi komutativnosti je $xkl_0 \in N$. Od tod sledi $kl_0 \in L$ in L je res podmodul M. Ker po enačbi (2) vemo, da je $x(k_1m_1 + k_2m_2 + \cdots + k_lm_l)$ element N, je $k_1m_1 + k_2m_2 + \cdots + k_lm_l \in L$.

Za $n \in N$ velja $xn \in N$, torej je $n \in L$. To pomeni, da je $N \subseteq L$. Velja tudi $yM \subseteq L$, saj je $xyM \subseteq N$, ker pa vemo $yM \not\subseteq N$, sledi, da je N strogo vsebovana v L. Tako smo pokazali, da je L končno generiran podmodul. Iz enačbe (2) sledi

$$N \subseteq xL + \sum_{i=1}^{l} Kn_i.$$

Z upoštevanjem definicije L in dejstva, da je N podmodul, dobimo

$$N = xL + \sum_{i=1}^{l} Kn_i,$$

kar pa nas pripelje do protislovja, saj je desna stran očitno končno generirana. Torej je $\mathfrak{p}$ praideal.

Lotimo se še zadnjega dela dokaza, kjer bomo pokazali, da $\mathfrak{p}M$ ni končno generiran. Ker je M končno generiran, obstajajo $e_1, e_2, \ldots, e_t$, da je $M = Ke_1 + Ke_2 + \cdots + Ke_t$. Vidimo, da množica $\{e_i + N \mid i = 1, 2, \ldots, t\}$ generira M/N, saj lahko poljuben $a \in M$ zapišemo kot $a = g_1e_1 + g_2e_2 + \cdots + g_te_t$ za neke $g_1, g_2, \ldots, g_t \in K$, od koder dobimo

$$\begin{aligned} a + N &= g_1e_1 + g_2e_2 + \cdots + g_te_t + N \\ &= (g_1e_1 + N) + (g_2e_2 + N) + \cdots + (g_te_t + N) \\ &= g_1(e_1 + N) + g_2(e_2 + N) + \cdots + g_t(e_t + N). \end{aligned}$$

Zapišemo lahko $M/N = K(e_1 + N) + K(e_2 + N) + \cdots + K(e_t + N)$ in od tod ter iz leme 17 sledi

$$\begin{aligned} \mathfrak{p} &= \mathrm{Ann}_K(M/N) \\ &= \mathrm{Ann}_K(K(e_1 + N) + K(e_2 + N) + \cdots + K(e_t + N)) \\ &= \bigcap_{i=1}^{t} \mathrm{Ann}_K(K(e_i + N)) \\ &= \bigcap_{i=1}^{t} \{k' \in K \mid k'ke_i \in N, k \in K\}. \end{aligned}$$

Pokažimo, da je $\mathfrak{p}$ enak enemu izmed $\mathrm{Ann}_K(K(e_i+N))$. Če to ni res, potem za vsak $i \in \{1, 2, \ldots, t\}$ obstaja element $a_i \in \mathrm{Ann}_K(K(e_i + N))$, ki ni element $\mathfrak{p}$. Produkt $a_1a_2 \cdots a_t$ pa je element vseh $\mathrm{Ann}_K(K(e_i + N))$, saj je

$$a_1a_2 \cdots a_{i-1}a_{i+1} \cdots a_t \cdot (a_iK(e_i + N)) \subseteq N.$$

Ker je $\mathfrak{p}$ praideal, to pomeni, da je $a_1 \in \mathfrak{p}$ ali $a_2a_3 \cdots a_t \in \mathfrak{p}$. Ker a_1 po predpostavki ne leži v $\mathfrak{p}$, velja $a_2a_3 \cdots a_t \in \mathfrak{p}$. Tako nadaljujemo in po $t-1$ korakih dobimo $a_t \in \mathfrak{p}$, kar nas pripelje do protislovja. Torej je $\mathfrak{p}$ enak $\mathrm{Ann}_K(K(e_j + N))$ za neki $j \in \{1, 2, \ldots, t\}$.

Prepričajmo se, da $e_j \notin N$. Če to ne bi bilo res, bi bil tudi $ke_j \in N$, za vsak $k \in K$, saj je N modul. To pa bi pomenilo, da je $\mathfrak{p}$ enak K, kar pa vemo, da ni res. Torej $e_j \notin N$ in $Ke_j \not\subset N$. Od tod sledi, da $Ke_j + N$ vsebuje N, a nista enaka, kar pomeni, da je $Ke_j + N$ končno generiran. Denimo, da je $\{k_ie_j + b_i \mid i = 1, 2, \ldots, d, k_i \in K, b_i \in N\}$ množica generatorjev za $Ke_j + N$. Element $a \in N \subset Ke_j + N$ lahko za neke $r_i \in K$ zapišemo kot

$$a = \sum_{i=1}^{d} r_i(k_ie_j + b_i) = \left(\sum_{i=1}^{d} r_ik_i\right) e_j + \sum_{i=1}^{d} r_ib_i.$$

Ker je $\sum_{i=1}^{d} r_ib_i \in N$, je tudi $\left(\sum_{i=1}^{d} r_ik_i\right) e_j \in N$. To pomeni, da je $\left(\sum_{i=1}^{d} r_ik_i\right)$ element $\mathfrak{p}$. Torej je

$$N \subseteq \mathfrak{p}e_j + \sum_{i=1}^{d} Kb_i.$$

Ker so v $\mathfrak{p}$ taki elementi k iz K, da je $ke_j \in N$, velja tudi obratna inkluzija. Dobimo

$$N = \mathfrak{p}e_j + \sum_{i=1}^{d} Kb_i \subseteq \mathfrak{p}M + \sum_{i=1}^{d} Kb_i \subseteq N + N = N,$$

od koder sledi $N = \mathfrak{p}M + \sum_{i=1}^{d} Kb_i$. Ker N ni končno generiran, tudi $\mathfrak{p}M$ ni.

Za posebni primer $M = K$ v izreku 18 dobimo Cohenov izrek.

5. Uporaba na bazah

S pomočjo Zornove leme bomo tekom tega razdelka pokazali, da ima vsak neničelni modul nad obsegom bazo. Posledica tega je, kot bomo videli, da ima vsak neničelni vektorski prostor bazo. Linearno neodvisnost množice v definiciji 11 razumemo tako, da nobena **končna** podmnožica nima netrivialne linearne kombinacije, ki je enaka 0. Definirajmo bazo modula nad kolobarjem.

Definicija 11. Naj bo M netrivialen modul nad kolobarjem K. Linearno neodvisna podmnožica $\mathcal{B} \subseteq M$ je *baza modula* M, če vsak element iz M lahko zapišemo kot končno linearno kombinacijo elementov iz $\mathcal{B}$.

Torej tudi, če je baza neskončna, nas zanimajo le končne linearne kombinacije baznih elementov. Za podmnožico P modula M, za katero velja, da lahko vsak element iz M zapišemo kot končno linearno kombinacijo elementov iz P, pravimo, da *razpenja* M. Spomnimo še, da je *obseg* tak kolobar, v katerem ima vsak neničelni element inverz za množenje. Sedaj si lahko ogledamo izrek, ki govori o obstoju baze modula nad obsegom.

Izrek 19. *Vsak neničelni modul nad obsegom ima bazo.*

Dokaz. Naj bo M neničelni modul nad obsegom $\mathcal{O}$. S pomočjo Zornove leme bomo bazo dobili kot maksimalni element neke množice. Definirajmo torej S kot množico vseh linearno neodvisnih podmnožic modula M. Naj bo $m \in M$ poljuben neničeln element. Ker je $\{m\}$ linearno neodvisna množica, S ni prazna. Množico S delno uredimo z relacijo inkluzije. Očitno velja, da je vsaka neprazna podmnožica linearno neodvisne množice tudi sama linearno neodvisna, zato so, če je A element S, tudi vse neprazne podmnožice A elementi S.

Preverimo pogoj za uporabo Zornove leme. Naj bo $\{I_\alpha\}_{\alpha\in\Lambda}$ linearno urejena podmnožica množice S. Za zgornjo mejo se ponuja unija $I := \bigcup_{\alpha\in\Lambda} I_\alpha$, ki vsebuje vse elemente $\{I_\alpha\}_{\alpha\in\Lambda}$, torej je od njih večja. S pomočjo linearne urejenosti bomo preverili, da je vsaka končna podmnožica I linearno neodvisna. Naj bodo $v_1, v_2, \ldots, v_k \in I$. Obstajajo take množice $I_{\alpha_1}, I_{\alpha_2}, \ldots, I_{\alpha_k}$, da je $v_i \in I_{\alpha_i}$ za $i = 1, 2, \ldots, k$. Po lemi 1 obstaja I_{α_j} za neki $j \in \{1, 2, \ldots, k\}$, da so $I_{\alpha_i} \leq I_{\alpha_j}$ za vse i. Torej so $v_1, v_2, \ldots, v_k \in I_{\alpha_j}$, kar pomeni, da so linearno neodvisni. Množica I je tako zgornja meja in Zornovo lemo lahko uporabimo.

Sledi, da obstaja neki maksimalni element $\mathcal{B}$ množice S. To je linearno neodvisna podmnožica modula M, ki ni vsebovana v nobeni večji linearno neodvisni podmnožici modula M. Pokazati moramo še, da $\mathcal{B}$ razpenja M.

Naj bo N množica vseh končnih linearnih kombinacij elementov iz $\mathcal{B}$, torej so v N elementi oblike $\sum_{i=1}^{l} \lambda_i b_i$ za $l \geq 1, \lambda_i \in \mathcal{O}$ in $b_i \in \mathcal{B}$. Pokažimo, da je $N = M$. Če to ni res, potem obstaja neki element $m_0 \in M \setminus N$. Videli bomo, da je $\mathcal{B} \cup \{m_0\}$ linearno neodvisna množica, ki vsebuje $\mathcal{B}$, a ji ni enaka. To nas bo pripeljalo do protislovja z maksimalnostjo $\mathcal{B}$.

Če $\mathcal{B} \cup \{m_0\}$ ni linearno neodvisna, potem obstaja končna linearna kombinacija $\sum_{i=1}^{l} \lambda_i b_i$ elementov iz $\mathcal{B} \cup \{m_0\}$, ki je enaka 0, a vsi koeficienti λ_i niso enaki 0. Ker so elementi $\mathcal{B}$ linearno neodvisni, je za neki $i_0 \in \{1, 2, \ldots, l\}$ element b_{i_0} enak m_0, koeficient λ_{i_0} pa je neničeln. Tako lahko zapišemo

$$\lambda_{i_0} m_0 = -\sum_{\substack{i=1 \\ i\neq i_0}}^{l} \lambda_i b_i.$$

Ko obe strani z leve pomnožimo z $\lambda_{i_0}^{-1}$, dobimo

$$m_0 = \sum_{\substack{i=1 \\ i\neq i_0}}^{l} (-\lambda_{i_0}^{-1}\lambda_i) b_i,$$

kar pa je element iz N. Tako smo prišli do protislovja, saj po predpostavki $m_0 \notin N$. Torej $N = M$ in $\mathcal{B}$ je baza M.

Izrek 19 velja za module nad obsegi, ne pa tudi za module nad kolobarji, saj v kolobarju nima vsak element inverza in dokaz se ustavi, ko želimo priti do protislovja s predpostavko $m_0 \notin N$. Oglejmo si posledico izreka 19.

Posledica 20. *Vsako linearno neodvisno podmnožico neničelnega modula nad obsegom lahko razširimo do baze modula.*

Dokaz. Naj bo $\mathcal{L}$ linearno neodvisna podmnožica. Bazo, ki vsebuje $\mathcal{L}$, bomo našli kot maksimalni element množice S, v kateri so linearno neodvisne podmnožice, ki vsebujejo $\mathcal{L}$. Ker je $\mathcal{L} \in S$, množica S ni prazna. Delno jo uredimo z relacijo inkluzije. Podobno kot v dokazu 19 pokažemo, da je pogoj za uporabo Zornove leme izpolnjen. Unija elementov linearno urejene podmnožice pa gotovo vsebuje $\mathcal{L}$, saj jo vsebuje vsak element. Torej po Zornovi lemi obstaja maksimalna linearno neodvisna množica $\mathcal{B}$, ki vsebuje $\mathcal{L}$, za katero na enak način kot v dokazu 19 pokažemo, da je baza.

Pokažimo še, da lahko iz množice, ki razpenja neki neničelni modul nad obsegom, dobimo bazo.

Posledica 21. *Vsaka množica, ki razpenja neničelni modul nad obsegom, vsebuje bazo tega modula.*

Dokaz. Naj bo $\mathcal{R}$ neka množica, ki razpenja neničelni modul M nad obsegom $\mathcal{O}$. Označimo z S množico vseh linearno neodvisnih podmnožic množice $\mathcal{R}$. Očitno S ni prazna, saj je $\{r\}$ linearno

neodvisna podmnožica $\mathcal{R}$ za poljuben neničeln $r \in \mathcal{R}$. Množico S delno uredimo z relacijo inkluzije. Preverimo, da ima vsaka linearno urejena podmnožica $\{I_\alpha\}_{\alpha\in\Lambda}$ množice S zgornjo mejo. Kandidat za zgornjo mejo je unija $I = \bigcup_{\alpha\in\Lambda} I_\alpha$, ki očitno vsebuje vse I_α. Argument, da je linearno neodvisna, je enak kot v dokazu izreka 19.

Zornova lema nam zagotavlja obstoj vsaj enega maksimalnega elementa množice S, ki ga označimo z $\mathcal{B}$. To je linearno neodvisna podmnožica $\mathcal{R}$, za katero moramo preveriti še, da razpenja modul M. Ker množica $\mathcal{R}$ razpenja M, je dovolj pokazati, da je vsak element iz $\mathcal{R}$ v množici, ki je razpeta z $\mathcal{B}$. Če neki $r_0 \in \mathcal{R}$ ni v množici, ki je razpeta z $\mathcal{B}$, potem je $\mathcal{B} \cup \{r_0\}$ linearno neodvisna podmnožica $\mathcal{R}$, ki strogo vsebuje $\mathcal{B}$. To je v protislovju z maksimalnostjo $\mathcal{B}$, ki je torej baza modula M.

Izrek 19 in njegovi posledici so splošnejše trditve od naslednje, ki isto pove za vektorske prostore.

Posledica 22. *Za neničelni vektorski prostor V nad poljem velja:*

1. *obstaja baza prostora V,*
2. *vsako linearno neodvisno podmnožico vektorskega prostora V lahko dopolnimo do baze,*
3. *vsaka množica, ki razpenja vektorski prostor V, vsebuje bazo tega prostora.*

Dokaz. Če je obseg v izreku 19 in njegovih posledicah komutativen, dobimo ravno polje in s tem vektorski prostor nad poljem.

Dokaz trditev iz posledice 22 v končno razsežnih vektorskih prostorih ne potrebuje Zornove leme. Trditev, da ima vsak neničelni vektorski prostor bazo, je pravzaprav ekvivalentna Zornovi lemi [3], česar pa ne bomo dokazali.

Oglejmo si še zanimivo posledico dejstva, da ima vsak neničelni vektorski prostor bazo. Potrebovali bomo pojem *avtomorfizma grupe*, ki je definiran kot bijektivni homomorfizem iz grupe G v grupo G. Spomnimo se še *centra grupe*, ki je množica tistih elementov grupe, ki komutirajo z vsemi elementi grupe. Za center grupe G uporabljamo oznako $Z(G)$.

Posledica 23. *V grupi z več kot dvema elementoma obstaja netrivialni avtomorfizem.*

Dokaz. Če grupa G ni Abelova, lahko najdemo element $a \in G \setminus Z(G)$. Potem je notranji avtomorfizem $\varphi(g) = aga^{-1}$ netrivialen, saj obstaja $g_0 \in G$, za katerega velja $ag_0 \neq g_0a$, torej $\varphi(g_0) = ag_0a^{-1} \neq g_0$.

Če pa je grupa G Abelova, uporabimo aditiven zapis in spet lahko ločimo dva primera. Najprej obravnavajmo možnost, ko obstaja element, ki ni sam svoj inverz. Preslikava $\varphi(g) = -g$ je potem netrivialen avtomorfizem. Če pa je vsak element sam svoj inverz, potem velja $x = -x$ oziroma $2x = 0$. Torej je G vektorski prostor nad poljem $\mathbb{Z}_2$. Iz posledice 22 sledi, da obstaja baza $\{b_\alpha\}_{\alpha\in\Lambda}$ vektorskega prostora G. Če imamo vsaj 2 bazična elementa, recimo b_β in b_γ, lahko definiramo preslikavo φ, ki ju zamenja, ostale pa pusti pri miru. To je netrivialen avtomorfizem, saj je $\varphi(b_\beta) = b_\gamma \neq b_\beta$. Če je v bazi le en element, recimo b_δ, dobimo grupo z elementoma 0 in b_δ, katere edini avtomorfizem pa je trivialen.

6. Uporaba v teoriji grafov

V tem razdelku si bomo ogledali uporabo Zornove leme v teoriji grafov. *Graf* je urejen par množice vozlišč in množice povezav. Vsaka povezava je dvoelementna podmnožica množice vozlišč. Pogosto označujemo z $V(G)$ množico vozlišč in z $E(G)$ množico povezav grafa G. *Pot* v grafu definiramo kot

zaporedje različnih vozlišč $u_0u_1u_2\cdots u_n$, kjer so $\{u_i, u_{i+1}\}$ v množici povezav za vsak $i \in \{0, 1, \ldots n-1\}$. Podobno definiramo tudi *cikel*, le da je začetno vozlišče enako končnemu, torej imamo zaporedje $u_0u_1u_2\cdots u_nu_0$. Za graf G pravimo, da je *povezan*, če med poljubnima vozliščema $v_1, v_2 \in V(G)$ obstaja pot. *Drevo* definiramo kot povezan graf brez ciklov.

Naj bosta sedaj G in H grafa. Pravimo, da je H *podgraf* grafa G, če velja $V(H) \subseteq V(G)$ in $E(H) \subseteq E(G)$. Če sta množici vozlišč enaki, potem je H *vpet podgraf* grafa G, če pa je H tudi drevo, potem mu rečemo *vpeto drevo*. Ker je drevo povezan graf, za nepovezane grafe vpeto drevo ne obstaja (saj grafu še odvzamemo povezave).

Sedaj se lahko s pomočjo [5, stran 198] lotimo izreka za povezane grafe.

Izrek 24. *Vsak povezan graf vsebuje vpeto drevo.*

Dokaz. Naj bo G povezan graf. Definirajmo S kot množico vseh podgrafov grafa G, ki so drevesa. Delno jo uredimo na naslednji način: za $T_1, T_2 \in S$ je $T_1 \leq T_2$ natanko tedaj, ko velja $V(T_1) \subseteq V(T_2)$ in $E(T_1) \subseteq E(T_2)$. Množica S ni prazna, saj je $(\{v\}, \emptyset)$ drevo za $v \in G$.

Oglejmo si neko linearno urejeno podmnožico $\{T_\alpha\} \subseteq S$. Trdimo, da je $T_0 = (\bigcup_\alpha V(T_\alpha), \bigcup_\alpha E(T_\alpha))$ zgornja meja te podmnožice. Očitno je $T_\alpha \leq T_0$ za vsak α, preveriti moramo le, da je T_0 drevo (da je povezan in nima ciklov). Ker je $V(T_0) = \bigcup_\alpha V(T_\alpha)$ obstajata taka T_{α_1} in T_{α_2} iz $\{T_\alpha\}$, da je $v_1 \in T_{\alpha_1}$ ter $v_2 \in T_{\alpha_2}$. V večjem izmed T_{α_1} in T_{α_2} obstaja pot med v_1 in v_2, zato obstaja tudi v T_0. Sledi, da je T_0 povezan.

S protislovjem pokažimo, da T_0 nima ciklov. Naj bo $c_1c_2\ldots c_nc_1$ neki cikel v T_0. Obstaja $C = \{T_{\alpha_1}, T_{\alpha_2}, \ldots, T_{\alpha_n}\} \subseteq \{T_\alpha\}$, da je $c_i \in T_{\alpha_i}$ za $i = 1, 2, \ldots, n$. Po lemi 1 obstaja T_{α_k}, ki je večji ali enak od vseh elementov v C. Torej velja $c_1, c_2, \ldots, c_n \in T_{\alpha_k}$, kar pomeni, da tak cikel ne obstaja, saj je T_{α_k} drevo.

Po Zornovi lemi obstaja maksimalni element M množice S. Ker je M v S, je M drevo. Če M ne bi vseboval vseh vozlišč grafa G, bi obstajalo vozlišče $v \in V(G)$, ki ne bi bilo v $V(M)$. Ker je G povezan, obstaja pot od vozlišča v do nekega vozlišča $u \in V(M)$. Če sledimo tej poti v smeri od v proti u, slej ko prej naletimo na sosednji vozlišči $v_0 \in V(G)\backslash V(M)$ in $u_0 \in V(M)$. Označimo z M^* graf, za katerega velja $V(M^*) = V(M) \cup \{v_0\}$ in $E(M^*) = E(M) \cup \{v_0u_0\}$. Torej je $M \leq M^*$, kar pa je v protislovju z dejstvom, da je M maksimalni element. Sledi, da je M vpeto drevo grafa G.

LITERATURA

[1] R. B. Ash, *Basic Abstract Algebra: For Graduate Students and Advanced Undergraduates*, Dover Books on Mathematics, Dover Publications, 2006.

[2] G. Bergman, *The Axiom of Choice, Zorn's lemma, and all that*, [ogled 15. 7. 2018], dostopno na `http://math.slu.edu/~srivastava/AC.pdf`.

[3] A. Blass, *Existence of bases implies the axiom of choice*, v: Axiomatic set theory (Boulder, Colo., 1983), Amer. Math. Soc., Providence, 1984, str. 31-33.

[4] K. Conrad, *Zorn's Lemma and Some Applications*, [ogled 15. 7. 2018], dostopno na `http://www.math.uconn.edu/~kconrad/blurbs/zorn1.pdf`.

[5] R. Diestel, *Graph Theory*, 3rd ed., Springer-Verlag, Berlin, Heidelberg, New York, 2006.

[6] J. L. Kelley, *The Tychonoff Product Theorem Implies the Axiom of Choice*, Fundamenta Mathematicae **37** (1950) 75-76; dostopno tudi na `http://eudml.org/doc/213229`.

[7] P. Pavešić, *Splošna topologija*, Izbrana poglavja iz matematike in računalništva **43**, DMFA – založništvo, Ljubljana, 2008.

[8] J. W. Tukey, *Convergence and Uniformity in Topology*, (AM-2): Volume 2, Annals of Mathematics Studies, Princeton University Press, New Jersey, 1941.

[9] I. Vidav, *Algebra*, Mladinska knjiga, Ljubljana, 1972.

[10] C. Wildman, *A Proof of Tychonoff's Theorem*, [ogled 15. 7. 2018], dostopno na `http://www.math.ucsd.edu/~cwildman/qualprep/tychonoff.pdf`.

[11] Ž. Zupančič, *Zornova lema in njena uporaba*, delo diplomskega seminarja, Fakulteta za matematiko in fiziko, Univerza v Ljubljani, 2017; dostopno tudi na `https://repozitorij.uni-lj.si/Dokument.php?id=110423`.