UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 2. stopnja

Klemen Pavlič

Grafi deliteljev niča in totalni grafi kolobarjev

Magistrsko delo

Mentor: izr. prof. dr. David Dolžan

Ljubljana, 2014

Podpisani Klemen Pavlič izjavljam:

– da sem magistrsko delo z naslovom *Grafi deliteljev niča in totalni grafi kolobarjev* izdelal samostojno pod mentorstvom izr. prof. dr. Davida Dolžana in

– da Fakulteti za matematiko in fiziko Univerze v Ljubljani dovoljujem objavo elektronske oblike svojega dela na spletnih straneh.

Ljubljana, 20. 6. 2014 Podpis: ....

Zahvala

Zahvaljujem se mojemu mentorju, izr. prof. dr. Davidu Dolžanu, za usmeritev v to zanimivo področje matematike, kjer se prepletata teorija kolobarjev in teorija grafov, ter za vso pomoč in razlago pri razumevanju snovi, še posebej za nasvete glede kolobarjev brez enote.

Kazalo

Program dela

V magistrskem delu si oglejte grafe deliteljev niča in totalne grafe nad končnimi kolobarji in raziščite njihove lastnosti.

Grafi deliteljev niča in totalni grafi kolobarjev

Povzetek

Najprej spoznamo pojem Jacobsonovega radikala in ugotovimo nekaj njegovih lastnosti. Nato pokažemo, da ima graf deliteljev niča končnega komutativnega enotskega kolobarja (razen v primeru sedmih izjem) prerezno vozlišče natanko tedaj, ko ima vozlišče stopnje ena. V nadaljevanju se zato posvetimo študiju vozlišč stopnje ena. Nato pokažemo, da je za končni komutativni enotski glavni kolobar R usmerjeni graf deliteljev niča $\Gamma_d(\mathbb{M}_n(R))$ uravnotežen in Eulerjev. Klasificiramo tudi vse končne kolobarje, katerih neusmerjeni graf deliteljev niča je Eulerjev. Spoznamo še nekaj lastnosti totalnih grafov. Določimo končne komutativne enotske kolobarje z ravninskim totalnim grafom. Ogledamo si še barvanje povezav in Eulerjevost totalnih grafov končnih komutativnih enotskih kolobarjev.

The zero-divisor graphs and total graphs of rings

Abstract

We first introduce the definition of Jacobson radical and some of its properties. Let R be a finite commutative ring with identity. We show that, with only seven known exceptions, the zero-divisor graph of R has a cut vertex if and only if the graph has a degree one vertex. This naturally leads to an examination of the degree one vertices of zero-divisor graphs. After that we prove that if R is a finite commutative principal ideal ring with identity, then the directed zero-divisor graph $\Gamma_d(\mathbb{M}_n(R))$ is balanced and Eulerian. We proceed to describe all finite rings with Eulerian undirected zero-divisor graph. We prove some basic properties of the total graph of a ring. We classify all finite commutative rings with identity that have planar total graph. At the end we study edge chromatic number and Eulerian total graphs of finite commutative rings with identity.

Math. Subj. Class. (2010): 05C07, 05C10, 05C25, 05C15, 05C20, 05C45, 13A99, 13F10, 13H99, 13M99

Ključne besede: graf deliteljev niča, totalni graf, Eulerjev graf, ravninski graf, prerezno vozlišče, barvanje povezav

Keywords: zero-divisor graph, total graph, Eulerian graph, planar graph, cut vertex, edge coloring

1. Uvod

S študijem grafov deliteljev niča na kolobarjih je prvi začel I. Beck, za njim pa se je s tem področjem ukvarjalo še mnogo avtorjev. Vpeljali in obravnavali so pojem grafa deliteljev niča še za druge algebraične strukture. Definirali so tudi pojem totalnega grafa kolobarja, ki poveže delitelje niča in operacijo seštevanja v kolobarju. Izkaže se namreč, da se iz lastnosti grafa deliteljev niča in totalnega grafa lahko ugotovi marsikatero zanimivo lastnost kolobarja. To je seveda tudi razlog za njihov študij. Področje se mi zdi zanimivo tudi zato, ker lepo poveže teorijo kolobarjev in teorijo grafov. Prvič sem se z njim srečal ob pisanju diplomskega seminarja, kjer sem se ukvarjal z grafi deliteljev niča komutativnih enotskih kolobarjev. Odločil sem se, da bom v magisteriju temo še razširil. Tu se bomo zato ukvarjali tudi z bolj splošnimi kolobarji.

V tem delu se bomo najprej posvetili študiju kolobarjev in nekaterih njihovih lastnosti (posplošili bomo nekatere pojme in definicije iz [16]), nato pa bomo s pomočjo teh ugotovitev obravnavali nekatere lastnosti grafov deliteljev niča in totalnih grafov. V drugem razdelku bomo najprej posplošili pojem Jacobsonovega radikala na nekomutativne kolobarje in spoznali nekaj ekvivalentnih definicij in lastnosti tega radikala. Spoznali bomo tudi pojem polenostavnega in J-polenostavnega kolobarja in povezavo med tema dvema lastnostma. Na koncu bomo definirali še kvaziregularne elemente in z njihovo pomočjo karakterizirali Jacobsonov radikal v kolobarjih brez enote. V tretjem razdelku bomo pojem lokalnega kolobarja posplošili na nekomutativne kolobarje. Četrti razdelek je namenjen mnogim raznovrstnim lastnostim kolobarjev, ki jih bomo potrebovali pri dokazavanju v razdelkih, kjer se bomo ukvarjali z grafi. V petem razdelku se bomo posvetili idempotentnim elementom in SBI-kolobarjem. Glavna ugotovitev tega razdelka bo govorila o dvigu idempotentov iz $R/J(R)$ v R. V naslednjem razdelku bomo na hitro omenili osnovne kolobarje z deljenjem, nato pa bomo začeli obravnavati lastnosti grafov. V sedmem razdelku bomo najprej definirali grafe deliteljev niča, nato pa se bomo ukvarjali s prereznimi vozlišči. Glavni rezultat tega razdelka bo govoril o končnih komutativnih enotskih kolobarjih, katerih graf deliteljev niča ima vsaj tri vozlišča. Pokazali bomo, da ima graf deliteljev niča takega kolobarja prerezno vozlišče natanko tedaj, ko ima vozlišče stopnje ena ali pa je izomorfen enemu izmed sedmih posebnih kolobarjev. Ker so torej vozlišča stopnje ena pomembna pri iskanju prereznih vozlišč, se bomo v osmem razdelku ukvarjali z njimi. V devetem razdelku se bomo ukvarjali z bolj splošnimi grafi, saj bomo imeli opravka z usmerjenimi grafi deliteljev niča. Obravnavali bomo uravnoteženost in Eulerjevost usmerjenih grafov deliteljev niča kolobarjev matrik nad komutativnimi končnimi glavnimi enotskimi kolobarji. V desetem razdelku bomo pozornost namenili neusmerjenim Eulerjevim grafom deliteljev niča. Natančno bomo namreč klasificirali vse končne kolobarje s takim grafom. V enajstem razdelku bomo končno spoznali še pojem totalnega grafa. Ukvarjali se bomo predvsem s končnimi komutativnimi enotskimi kolobarji. Spoznali bomo, da lahko veliko povemo o totalnem grafu takega kolobarja, če ločimo primera, ko je kolobar lokalni in ko ni. V dvanajstem razdelku bomo nato s pomočjo prejšnjih ugotovitev določili končne komutativne enotske kolobarje z ravninskim totalnim grafom. Pri tem nam bo v veliko pomoč množica minimalnih praidealov kolobarja. V trinajstem razdelku si bomo ogledali barvanja povezav totalnega grafa, v zadnjem, štirinajstem, razdelku, pa bomo obravnavali še Eulerjevost totalnih grafov.

Uporabljal bom nekaj lem, ki sem jih dokazal že v diplomi (glej [16]), kjer lahko zainteresiran bralec najde njihove dokaze, kot tudi osnovne primere grafov deliteljev niča. Prav tako lahko tam najdemo razlago večine oznak, ki jih bomo uporabljali.

2. Jacobsonov radikal

Definicija 2.1. Naj bo R kolobar. Potem je *Jacobsonov radikal* $J(R)$ enak preseku vseh maksimalnih levih idealov kolobarja R.

Najprej opazimo, da v komutativnih kolobarjih zgornja definicija sovpada z definicijo iz [16], kjer je Jacobsonov radikal komutativnega kolobarja definiran kot presek vseh maksimalnih idealov.

Spomnimo se še nekaj definicij. Naj bo R kolobar in M levi R-modul. Pravimo, da je modul M *enostaven*, če je $M \neq 0$ in sta 0 in M edina R-podmodula modula M. Poleg tega pravimo še, da je modul M *polenostaven*, če je vsak R-podmodul modula M direktni sumand modula M.

Poglejmo si zdaj, kaj velja za elemente iz Jacobsonovega radikala.

Lema 2.2. *Naj bo R enotski kolobar, ki ni nujno komutativen. Potem so za $y \in R$ ekvivalentne naslednje trditve*

(1) *$y \in J(R)$,*
(2) *$1 - xy$ ima levi inverz za vsak $x \in R$,*
(3) *$yM = 0$ za vsak enostavni levi R-modul M.*

Dokaz. Dokažimo implikacijo (1) $\Rightarrow$ (2). Naj bo $y \in J(R)$. Denimo, da implikacija ne velja. Potem obstaja $x \in R$, da $1-xy$ nima levega inverza. Potem je $R(1-xy) \subsetneq R$ in $R(1-xy)$ je vsebovan v nekem maksimalnem levem idealu m. Ker pa je $1-xy \in R(1-xy) \subseteq m$, je $1-xy \in m$. Poleg tega je $y \in J(R) \subseteq m$ in zato je tudi $xy \in m$. Sledi $1 \in m$. Protislovje.

Dokažimo implikacijo (2) $\Rightarrow$ (3). Naj bo torej M enostavni levi R-modul. Naj bo $m \in M$ tak, da je $ym \neq 0$. Ker je M enostaven, mora biti torej $R \cdot ym = M$. Potem obstaja $x \in R$, da je $m = x \cdot ym$. To zvezo lahko prepišemo v $(1-xy)m = 0$. Po predpostavki ima $1-xy$ levi inverz in če zgornjo zvezo pomnožimo z njim, dobimo $m = 0$. Protislovje s predpostavko, da je $ym \neq 0$.

Dokažimo še implikacijo (3) $\Rightarrow$ (1). Naj bo m poljuben maksimalni levi ideal. Potem je R/m enostavni levi R -modul. Po predpostavki je potem $y \cdot (R/m) = 0$, kar implicira, da je $y \in m$. Ker je bil zgoraj m poljuben, je potem $y \in J(R)$. □

Spomnimo se, da je za poljubni levi R-modul M anihilator M definiran kot $\mathrm{ann}(M) = \{r \in R : rM = 0\}$. To je očitno ideal kolobarja R. Če sta $a, b \in \mathrm{ann}(M)$ in $r \in R$, potem je jasno $a + b, ra \in \mathrm{ann}(M)$, prav tako pa je $ar \in \mathrm{ann}(M)$, saj je $ar \cdot M = a \cdot rM \subseteq aM = 0$.

Naj bo zdaj I levi ideal kolobarja R. Za R-modul M lahko vzamemo kar R/I. Potem je $\mathrm{ann}(M) = \{r \in R : r \cdot R/I = 0\} = \{r \in R : rR \subseteq I\}$.

Zdaj lahko zapišemo takojšnjo posledico zgornje leme in zgoraj zapisanega.

Posledica 2.3. *Naj bo R enotski kolobar. Potem je Jacobsonov radikal $J(R) = \cap\, \mathrm{ann}(M)$, kjer presek teče po vseh enostavnih levih R-modulih. Sledi še, da je $J(R)$ ideal v R.*

S pomočjo te posledice lahko dokažemo še naslednjo karakterizacijo Jacobsonovega radikala. Pri tem z $U(R)$ označimo množico vseh obrnljivih elementov kolobarja R.

Lema 2.4. *Naj bo R enotski kolobar. Potem sta za $y \in R$ ekvivalentni trditvi*

(1) $y \in J(R)$,
(2) $1 - xyz \in U(R)$ *za vsaka* $x, z \in R$.

Dokaz. Dokažimo najprej implikacijo (2) $\Rightarrow$ (1). Ker (2) velja za vsak z, velja tudi za $z = 1$. Potem je $1 - xy \in U(R)$ za vsak $x \in R$ in po lemi 2.2 je $y \in J(R)$.

Dokažimo še (1) $\Rightarrow$ (2). Naj bo $y \in J(R)$ in $x, z \in R$. Ker je po posledici 2.3 $J(R)$ ideal, je $yz \in J(R)$. Zato po lemi 2.2 obstaja $u \in R$, da je $u(1 - xyz) = 1$. Od tod sledi, da ima u desni inverz. Ker je po posledici 2.3 tudi $xyz \in J(R)$, ima po lemi 2.2 element $u = 1 + u(xyz)$ še levi inverz. Sledi, da je $u \in U(R)$ in posledično $1 - xyz \in U(R)$. □

Posledica 2.5. *Naj bo R enotski kolobar. Potem je Jacobsonov radikal $J(R)$ največji levi ideal $I \subseteq R$, ki zadošča $1 + I \subseteq U(R)$.*

Dokaz. Sledi iz posledice 2.3 in leme 2.4. □

Posledica 2.6. *Naj bo R enotski kolobar in I ideal v R, ki zadošča $I \subseteq J(R)$. Potem je $J(R/I) = J(R)/I$.*

Dokaz. Sledi s pomočjo ekvivalence med (1) in (2) v lemi 2.2. □

Na tem mestu lahko omenimo Jacobsonovo polenostavnost. Pravimo, da je kolobar R *Jacobsonovo polenostaven* (oziroma *J-polenostaven*), če je $J(R) = 0$. Primerov takih kolobarjev ni težko najti, saj je za poljuben enotski kolobar R kvocientni kolobar $R/J(R)$ J-polenostaven kolobar. Na ta način lahko vsakemu enotskemu kolobarju priredimo J-polenostaven kolobar. Izkaže se, da imata kolobar in pripadajoči J-polenostavni kolobar nekatere lastnosti skupne, zato je včasih bolj smiselno obravnavati pripadajoči J-polenostavni kolobar.

Lema 2.7. *Naj bo R enotski kolobar. Potem imata R in $R/J(R)$ iste enostavne leve module. Prav tako velja, da je $x \in R$ levo obrnljiv (obrnljiv) v R natanko tedaj, ko je $\overline{x} = x + J(R) \in \overline{R} = R/J(R)$ levo obrnljiv (obrnljiv) v $\overline{R} = R/J(R)$.*

Dokaz. Naj bo M enostavni R-modul. Naj bosta $x \in M, \overline{r} \in \overline{R}$. Definiramo $\overline{r}x = rx$. Denimo, da je $\overline{r} = \overline{s}$. Velja $\overline{r} = \overline{s} \Leftrightarrow r - s \in J(R) \Leftrightarrow (r - s)M = 0$ za vsak enostavni R-modul M (lema 2.2). To pomeni, da je $rx = sx$ za vsak $x \in M$, torej je to dobro definirano delovanje. Enostavno se preveri, da s to operacijo M postane $\overline{R}$-modul. Denimo, da obstaja $N \subsetneq M$ $\overline{R}$-modul. N postane R-podmodul, če definiramo $rx = \overline{r}x, r \in R, x \in N$. Ker je M enostavni R-modul, pa je $N = \{0\}$. Zato je M enostavni $\overline{R}$-modul. Naj bo M enostavni $\overline{R}$-modul. Potem M postane R-modul, če definiramo $rx = \overline{r}x, r \in R, x \in M$ (preprost račun). Naj bo $N \subsetneq M$ R-modul. Ker je delovanje R definirano preko delovanja $\overline{R}$, je N tudi $\overline{R}$-podmodul. Ker je M enostavni $\overline{R}$-modul, je $N = \{0\}$. Sklenemo, da imata R in $\overline{R}$ res iste enostavne module. Če ima x levi inverz y, je jasno, da je $\overline{y}$ levi inverz $\overline{x}$. Pokazati moramo torej le še, da iz obstoja levega inverza elementa $\overline{x}$ sledi obstoj levega inverza elementa x. Naj bo $y \in R$ tak, da je $\overline{yx} = \overline{1}$. Potem je $1 - yx \in J(R)$. To je ekvivalentno temu, da je $yx \in 1 + J(R) \subseteq U(R)$. Potem obstaja $u \in R$, da je $u \cdot yx = 1$ in je uy levi inverz elementa x. Analogno dokažemo za desno obrnljivost. □

Pravimo, da je kolobar R *polenostaven*, če je levi R-modul R polenostaven. Poleg tega velja še naslednja lema.

Lema 2.8. *Za vsak kolobar R sta ekvivalentni trditvi*

(1) *R je polenostaven,*
(2) *R je J-polenostaven in levo artinski.*

Zainteresirani bralec lahko dokaz najde v [13, Izrek 4.14], tu pa ga bomo izpustili. Ker zgornja lastnost očitno velja tudi za končne kolobarje, bomo to na primernih mestih s pridom uporabili.

Končni polenostavni kolobarji imajo še eno zelo zanimivo lastnost. Po [15, Trditev 1.6] namreč sledi, da ima vsak končni polenostavni kolobar multiplikativno enoto. Na tem mestu je primerno, da se spomnimo še Wedderburnovega izreka.

Izrek 2.9 (Wedderburn)**.** *Naj bo R polenostavni kolobar. Tedaj je $R \cong \mathbb{M}_{n_1}(D_1) \times \cdots \times \mathbb{M}_{n_r}(D_r)$, kjer so D_i obsegi in n_i pozitivna števila. Pri tem je število r enolično določeno, prav tako pa so do vrstnega reda natančno določeni pari $\{(n_i, D_i)\}_{i=1}^r$.*

Opomba 2.10. Dokaz izreka bomo izpustili, saj ga lahko najdemo v skoraj vsaki knjigi iz nekomutativne algebre, na primer v [13, Izrek 3.5]. Po zgoraj napisanem sledi, da izrek velja za vsak končni kolobar R, ki zadošča pogoju $J(R) = 0$. Velja še, da so v primeru končnega kolobarja obsegi iz izreka kar polja.

Vrnimo se sedaj k Jacobsonovemu radikalu.

Lema 2.11. *Naj bo $\{I_j\}_{j=1}^m$ neki končni nabor levih idealov kolobarja R. Če je vsak izmed njih nilpotenten, potem je tudi ideal $I_1 + \cdots + I_m$ nilpotenten.*

Dokaz. Obravnavali bomo samo primer, ko je $m = 2$, v splošnem namreč dokaz zaključimo z indukcijo. Naj bosta I_1, I_2 dva nilpotentna leva ideala. Naj bo $n \in \mathbb{N}$ najmanjši tak, da je $I_1^n = 0$ in $I_2^n = 0$. Označimo z $L = I_1 + I_2$. Trdimo, da je $L^{2n} = 0$. Pokazati moramo, da je produkt $2n$ elementov $(x_1+y_1)\cdots(x_{2n}+y_{2n}), x_i \in I_1, y_i \in I_2$ enak 0. Ta produkt razpišemo. Vsak sumand bo produkt $2n$ členov, pri čemer jih bo vsaj n iz I_1 ali vsaj n iz I_2. Ker sta I_1 in I_2 leva ideala in ker je $I_1^n = 0 = I_2^n$, so vsi sumandi enaki 0 in zato je zgornji produkt enak 0. Sledi $L^{2n} = 0$. □

Pravimo, da je ideal I *nil ideal*, če so vsi njegovi elementi nilpotentni. To pomeni, da za vsak $x \in I$ obstaja tak $n \in \mathbb{N}$, da je $x^n = 0$. Jasno je, da je vsak nilpotentni ideal tudi nil ideal, obratna implikacija pa ne velja. Analogno definiramo še pojem enostranskega nil ideala.

Lema 2.12. *Naj bo R enotski kolobar. Če je $I \subseteq R$ levi (desni) nil ideal, potem je $I \subseteq J(R)$.*

Dokaz. Naj bo $y \in I$. Ker je I levi ideal, je za vsak $x \in R$ tudi $xy \in I$ in posledično je xy nilpotenten. Obstaja torej $n \in \mathbb{N}$, da je $(xy)^n = 0$. Oglejmo si sedaj element $1 - xy$. Ta ima inverz $\sum_{j=0}^{\infty}(xy)^j = \sum_{j=0}^{n-1}(xy)^j$. Po lemi 2.2 je torej $y \in J(R)$. Dokaz je podoben tudi v primeru, ko je I desni nil ideal, le da si pomagamo z lemo 2.4. □

Ker je vsak nilpotentni ideal očitno tudi nil ideal, nam zgornja lema pove, da $J(R)$ vsebuje vse nilpotentne leve ideale. V primeru artinskih kolobarjev pa lahko povemo še več. Pokazali bomo, da mora biti v tem primeru $J(R)$ kar nilpotenten.

Izrek 2.13. *Naj bo R levo artinski enotski kolobar. Potem je $J(R)$ največji nilpotentni levi ideal.*

Dokaz. Po komentarju pred izrekom zadošča dokazati, da je $J(R)$ nilpotenten. Ker je R levo artinski, obstaja naravno število k, da je $J(R)^k = J(R)^{k+1} = I$. Trdimo, da je $I = 0$. Denimo nasprotno, da $I \neq 0$. Poglejmo si množico $\mathcal{S}$ levih idealov K v R, ki zadoščajo pogoju $I \cdot K \neq 0$. Množica $\mathcal{S}$ je neprazna, saj vsebuje I. Ker je R levo artinski, ima $\mathcal{S}$ minimalni element K_0. Naj bo zdaj $a \in K_0$ tak element, da je $I \cdot a \neq 0$. Potem je $I \cdot (Ia) = I^2 a = Ia \neq 0$. Ker pa je K_0 minimalen, mora biti $Ia = K_0$. To pomeni, da je $a = ya$ za neki $y \in I \subseteq J(R)$. To zvezo lahko prepišemo v $(1 - y)a = 0$. Ker je $y \in J(R)$, ima po lemi 2.2 element $1 - y$ levi inverz. To pomeni, da je $a = 0$. Protislovje. Sledi, da je $J(R)^k = 0$. □

Če združimo lemo 2.12 in izrek 2.13, dobimo naslednjo posledico.

Posledica 2.14. *V levo artinskem enotskem kolobarju je vsak levi nil ideal nilpotenten.*

Do sedaj smo ves čas govorili le o enotskih kolobarjih. Poiščimo še karakterizacijo Jacobsonovega radikala v kolobarjih brez enote. V ta namen bomo najprej uvedli pojem kvaziregularnega elementa. Pred tem pa moramo definirati še operacijo $\circ$. Naj bo R kolobar (lahko je nekomutativen in brez enote). Za $x, y \in R$ definiramo $x \circ y = x + y - xy$. Z lahkoto preverimo, da je ta operacija asociativna, kar pomeni, da je za poljubne $x, y, z \in R$ izpolnjena enakost $x \circ (y \circ z) = (x \circ y) \circ z$. Očitno velja še $x \circ 0 = 0 \circ x = x$, kar pomeni, da je 0 enota za operacijo $\circ$. Pri tem je $x \circ y = y \circ x$ natanko tedaj, ko je $xy = yx$.

Definicija 2.15. Naj bo R kolobar.

(1) Element $x \in R$ je *levo kvaziregularen*, če obstaja $y \in R$, da je $y \circ x = 0$. Element $x \in R$ je *desno kvaziregularen*, če obstaja $z \in R$, da je $x \circ z = 0$. Element $x \in R$ je *kvaziregularen*, če je levo kvaziregularen in desno kvaziregularen. Pri tem elementu y rečemo *levi kvaziinverz*, elementu z pa *desni kvaziinverz.*
(2) Levi ideal I kolobarja R je *kvaziregularen*, če je vsak element $x \in I$ levo kvaziregularen.
(3) Desni ideal I kolobarja R je *kvaziregularen*, če je vsak element $x \in I$ desno kvaziregularen.

Naslednja lema govori o kvaziregularnosti v enotskem kolobarju.

Lema 2.16. *Naj bo R enotski kolobar.*

(1) *Element $x \in R$ je levo (desno) kvaziregularen natanko tedaj, ko ima $1 - x$ levi (desni) inverz v R.*
(2) *Element $x \in R$ je kvaziregularen natanko tedaj, ko je $1 - x \in U(R)$.*
(3) *Če je I levi ali desni ideal, ki je kvaziregularen, potem je vsak element $x \in I$ kvaziregularen.*

Dokaz. Dokazali bomo vsako točko leme posebej. Začnimo kar s prvo.

(1) Naj bo x levo kvaziregularen. Potem obstaja tak $y \in R$, da je $y \circ x = y + x - yx = 0$. To je ekvivalentno temu, da velja $1 = 1 - y - x + yx = (1 - y)(1 - x)$. To pomeni, da ima element $1 - x$ levi inverz. Pokažimo še obrat. Naj bo $z(1 - x) = 1$ za neki $z \in R$. Zapišimo z kot $z = 1 - y$ za neki $y \in R$ (vzamemo lahko $y = 1 - z$). Potem je $1 = z(1 - x) = (1 - y)(1 - x) = 1 - y - x + yx$. To implicira $y \circ x = 0$, torej je x levo regularen. Podobno dokažemo trditev še za desno kvaziregularne elemente.
(2) Sledi iz točke (1) in definicije kvaziregularnega elementa.

(3) Naj bo I levi ideal, ki je kvaziregularen (za desne ideale je dokaz podoben). Naj bo $x \in I$. Po definiciji je x levo kvaziregularen. To pomeni, da obstaja $y \in R$, ki zadošča $y + x - yx = y \circ x = 0$. Ker je I levi ideal, iz enakosti $y = yx - x$ sledi $y \in I$. To pomeni, da je y levo kvaziregularen element. Potem obstaja $z \in R$, da je $z \circ y = 0$. Potem je $z = z \circ 0 = z \circ (y \circ x) = (z \circ y) \circ x = 0 \circ x = x$. Sledi $x = z$ in zato je $x \circ y = y \circ x = 0$. To pa ravno pomeni, da je x kvaziregularen.

□

Tretja točka leme nam pove, zakaj ni potrebno govoriti o levo kvaziregularnih levih idealih in desno kvaziregularnih desnih idealih.

Lema 2.17. *Vsak nilpotentni element je kvaziregularen.*

Dokaz. Naj bo x nilpotentni element in naj bo $n \in \mathbb{N}$ najmanjše število, ki zadošča $x^n = 0$. Potem je element $-x - x^2 - \cdots - x^{n-1}$ kvaziinverz elementa x. □

Posledica 2.18. *Vsak nil ideal je kvaziregularen.*

Sedaj lahko podamo še eno definicijo Jacobsonovega radikala.

Definicija 2.19. Naj bo R kolobar. Potem je $J(R)$ kvaziregularen levi ideal, ki vsebuje vse druge kvaziregularne leve ideale kolobarja R.

Opazimo, da ta definicija spominja na lemo 2.12. Iz zgornje definicije po posledici 2.18 namreč sledi, da $J(R)$ vsebuje vse leve nil ideale. Zapišimo naslednjo lemo.

Lema 2.20. *Naj bo R enotski kolobar. Tedaj je*

$$J(R) = \{x \in R | rx \text{ je levo kvaziregularen za vsak } r \in R\}.$$

Dokaz. Naj bo $x \in J(R)$. Ker je po zgornji definiciji $J(R)$ kvaziregularen levi ideal, je x tudi iz množice na desni strani enačaja. Naj bo $x \in R$ tak, da je rx levo kvaziregularen za vsak $r \in R$. Potem je Rx kvaziregularen levi ideal. Po zgornji definiciji je $Rx \subseteq J(R)$. Ker je R enotski, je $x \in J(R)$. □

Primerjajmo ugotovitve leme 2.2 z ugotovitvami leme 2.16 in leme 2.20. Vidimo, da zgornja definicija v primeru, ko imamo enotski kolobar, sovpada z že znanimi karakterizacijami Jacobsonovega radikala.

Spomnimo se še ene definicije. Naj bo R kolobar in $e \in R$ idempotent. Potem kolobarju eRe pravimo *kotni kolobar*. Opazimo še, da je e njegova enota.

Pokažimo naslednjo lemo, ki bo povezala Jacobsonov radikal in kotne kolobarje.

Lema 2.21. *Naj bo R enotski kolobar in naj bo $e = e^2$ neki idempotent kolobarja R. Tedaj velja $J(eRe) = J(R) \cap eRe = eJ(R)e$.*

Dokaz. Naj bo najprej $r \in J(eRe)$. Da bo $r \in J(R) \cap eRe$, zadošča videti, da je $r \in J(R)$. Po lemi 2.2 je dovolj, če pokažemo, da ima za vsak $y \in R$ element $1 - yr$ levi inverz v R. Gremo najprej v eRe. Tam po lemi 2.2 obstaja b, da je $b(e - (eye)r) = e$. Ker sta $b, r \in eRe$, lahko zapišemo $b(e - eyer) = be(1 - y(er)) = b(1-yr)$. Velja torej zveza $b(1-yr) = e$. Od tu dobimo $yr = yre = yrb(1-yr)$. Na obeh straneh prištejemo $1-yr$ in dobimo $1 = yr+(1-yr) = yrb(1-yr)+(1-yr) = (yrb+1)(1-yr)$, kar ravno pomeni, da je element $1+yrb$ levi inverz elementa $1-yr$.

Naj bo zdaj $r \in J(R) \cap eRe$. Potem je očitno $r \in eJ(R)e$.

Naj bo torej še $r \in eJ(R)e$. Radi bi videli, da je $r \in J(eRe)$. Po lemi 2.2 spet zadošča videti, da ima za vsak $y \in eRe$ element $e - yr$ levi inverz v eRe. Ker je

$J(R)$ po posledici 2.3 ideal, je $r \in eJ(R)e \subseteq J(R)$. Po lemi 2.2 obstaja $x \in R$, da je $x(1-yr)=1$. Potem velja $e = e1e = ex(1-yr)e = ex(e-yr) = exe(e-yr)$ in posledično ima $e-yr$ levi inverz exe. □

3. Lokalni kolobarji

Definicija 3.1. Pravimo, da je neničelni kolobar R *lokalen*, če ima natanko en maksimalni levi ideal.

Takoj opazimo, da je komutativni kolobar lokalen, če ima natanko en maksimalni ideal. Naslednja lema pove, da lahko lokalni kolobar definiramo tudi prek maksimalnih desnih idealov.

Lema 3.2. *Naj bo R enotski kolobar. Naslednje trditve so ekvivalentne*

(1) *R ima natanko en maksimalni levi ideal,*
(2) *R ima natanko en maksimalni desni ideal,*
(3) *$\overline{R} = R/J(R)$ je obseg,*
(4) *$R \setminus U(R)$ je ideal kolobarja R,*
(5) *$R \setminus U(R)$ je aditivna grupa,*
(6) *za vsak $n \in \mathbb{N}$ iz predpostavke $a_1 + \cdots + a_n \in U(R)$ sledi, da je neki $a_i \in U(R)$,*
(7) *iz $a+b \in U(R)$ sledi, da je $a \in U(R)$ ali $b \in U(R)$.*

Dokaz. Dokažimo najprej implikacijo (1) $\Rightarrow$ (3). Po (1) sledi, da je $J(R)$ edini maksimalni levi ideal. Potem $R/J(R)$ nima pravih levih idealov. Naj bo $\overline{0} \neq \overline{a} \in \overline{R}$. Potem je levi ideal $\overline{R}\overline{a}$ enak bodisi $\overline{0}$ bodisi $\overline{R}$. Prva možnost odpade, ker ima R enoto. Sledi $\overline{R}\overline{a} = \overline{R}$. Zato obstaja $\overline{b} \in \overline{R}$, da je $\overline{b}\overline{a} = \overline{1}$. Ker je tudi $\overline{R}\overline{b} = \overline{R}$, obstaja $\overline{c} \in \overline{R}$, da je $\overline{c}\overline{b} = \overline{1}$. Potem je $\overline{a} = \overline{c}$ in $(\overline{a})^{-1} = \overline{b}$. Sledi, da je $\overline{R} = R/J(R)$ obseg.

Dokažimo implikacijo (3) $\Rightarrow$ (1). Vemo, da je $J(R)$ vsebovan v vsakem maksimalnem levem idealu m. Ker je $R/J(R)$ obseg, mora biti $m = J(R)$ in zato je R lokalni kolobar.

Analogno dokažemo (2) $\Leftrightarrow$ (3).

Pokažimo sedaj implikacijo (3) $\Rightarrow$ (4). Po lemi 2.7 je $x \in R$ obrnljiv natanko tedaj, ko je obrnljiv $\overline{x} \in R/J(R)$. Po (3) je $R/J(R)$ obseg, torej je vsak element $x \notin J(R)$ obrnljiv element v R in je zato $x \in U(R)$. Sledi torej, da je $R \setminus U(R) = J(R)$, kar je po posledici 2.3 ideal.

Implikacija iz (4) $\Rightarrow$ (5) je očitna, saj je vsak ideal tudi aditivna grupa.

Prav tako sta očitni implikaciji (5) $\Rightarrow$ (6) in (6) $\Rightarrow$ (7).

Dokažimo še implikacijo (7) $\Rightarrow$ (3). Naj bo torej $a \in R \setminus J(R)$. Potem obstaja maksimalni ideal m, za katerega velja $a \notin m$. Potem je $m + R \cdot a = R$ zaradi maksimalnosti m. To pomeni, da lahko zapišemo $1 = x + ba$ za neki $x \in m$ in $b \in R$. Ker je $1 \in U(R)$ in $x \notin U(R)$, je po (7) $ba \in U(R)$. Po lemi 2.7 je $\overline{ba} \in U(R/J(R))$. Sledi torej, da ima $\overline{a}$ levi inverz v $R/J(R)$. Ker je $J(R)$ enak tudi preseku maksimalnih desnih idealov, lahko podobno dokažemo še, da ima $\overline{a}$ desni inverz v $R/J(R)$. Sledi, da je $\overline{a} \in U(R/J(R))$. To pomeni, da je $(R/J(R)) \setminus \{0\}$ multiplikativna grupa in posledično je $R/J(R)$ obseg. □

Naslednja lema govori o idempotentih v lokalnih kolobarjih.

Lema 3.3. *Naj bo R lokalni enotski kolobar. Potem R nima netrivialnih idempotentov (edina idempotenta sta torej 0 in 1).*

Dokaz. Denimo da R vsebuje neki netrivialni idempotent e. Označimo z $f = 1-e$. Ker pa je $e + f = 1 \in U(R)$, je po lemi 3.2 $e \in U(R)$ ali $f \in U(R)$. Ker velja še $ef = e(1-e) = 0$, je $e = 0$ ali $f = 0$. To implicira, da je $e = 0$ ali $e = 1$. Protislovje. □

Zanimivo pa je to, da v artinskih kolobarjih velja tudi obrat.

Lema 3.4. *Naj bo R desno artinski enotski kolobar. Potem je R lokalni natanko tedaj, ko nima netrivialnih idempotentov.*

Opomba 3.5. Za dokaz implikacije v levo potrebujemo teorijo nerazcepnih modulov, zato se bomo temu dokazu tu izognili. Zainteresiran bralec ga lahko najde v [13, Posledica 19.19]

4. Še malo o kolobarjih

Lema 4.1. *Naj bo R končni nenilpotentni kolobar brez enote. Potem lahko zapišemo $R \cong R_1 \oplus R_2 \oplus \cdots \oplus R_m$, kjer je $m \geq 1, |R_i| = p_i^{\alpha_i}, i = 1, 2, \ldots, m$ in so $p_1, p_2, \ldots, p_m$ različna praštevila. Trdimo še, da obstaja $1 \leq j \leq m$, da R_j vsebuje neničelni nilpotentni element.*

Dokaz. Prvi del trditve sledi iz razcepa končnih abelovih grup, potrebno je preveriti le usklajenost množenja. To naredimo tako kot v [16, Lema 2.3].

Dokažimo torej, da obstaja neničelni nilpotent. Trditev zadošča dokazati za nerazcepni kolobar R moči $|R| = p^n$ za neko praštevilo p in naravno število n. Zadošča pokazati, da je Jacobsonov radikal $J(R) \neq 0$, saj je ta nilpotenten tudi v kolobarjih brez enote, kar bomo dokazali sedaj. Vložimo naš kolobar R v enotski kolobar $\mathbb{Z}_{p^n} \times R$, kjer je množenje definirano kot $(k, a) \cdot (l, b) = (kl, kb + la + ab)$, kjer sta $k, l \in \mathbb{Z}_{p^n}$ ter $a, b \in R$. Oglejmo si, kakšni so maksimalni levi ideali $\mathbb{Z}_{p^n} \times R$. Najprej opazimo, da je kolobar $\mathbb{Z}_{p^n}$ lokalni kolobar. Sledi, da je njegov edini maksimalni ideal $p\mathbb{Z}_{p^n}$. Jasno je tudi, da je $p\mathbb{Z}_{p^n} \times R$ maksimalni levi ideal enotskega kolobarja $\mathbb{Z}_{p^n} \times R$. Poglejmo si še, kakšni so maksimalni levi ideali v $\mathbb{Z}_{p^n} \times R$, ki imajo na drugi komponenti pravi maksimalni levi ideal m_i. Če je množica $\mathbb{Z}_{p^n} \times m_i$ levi ideal kolobarja $\mathbb{Z}_{p^n} \times R$ (problem je pri zaprtosti za množenje z elementi $\mathbb{Z}_{p^n} \times R$), potem je to zagotovo maksimalni levi ideal. Če pa to ni levi ideal, moramo imeti na prvi komponenti neki ideal I kolobarja $\mathbb{Z}_{p^n}$. Tedaj je levi ideal $I \times m_i$ vsebovan v maksimalnem idealu $p\mathbb{Z}_{p^n} \times R$. V obeh primerih dobimo, da je $\{0\} \times J(R) \subseteq J(\mathbb{Z}_{p^n} \times R)$. Ker je slednji nilpotenten, je tudi $J(R)$ nilpotenten (glej definicijo množenja v $\mathbb{Z}_{p^n} \times R$).

Če bi bil $J(R) = 0$, bi bil R po lemi 2.8 polenostaven in zato po Wedderburnovem izreku 2.9 izomorfen direktni vsoti matrik nad polji. To je v nasprotju s tem, da R nima enote. □

Vpeljimo sedaj še pojem levega in desnega anihilatorja. Množica $l_R(x) = \{y \in R | yx = 0\}$ je *levi anihilator* elementa x. Analogno definiramo $r_R(x) = \{y \in R | xy = 0\}$ kot *desni anihilator* elementa x. Podobno definiramo anihilator poljubne množice. Pripomnimo še, da je anihilator elementa x potem ravno $\mathrm{ann}_R(x) = \{y \in R | yx = xy = 0\} = l_R(x) \cap r_R(x)$.

Lema 4.2. *Naj bo R končni enotski kolobar. Naj bo $a \in R$ element, za katerega velja $l_R(a) = 0$ oziroma $r_R(a) = 0$. Potem ima a levi oziroma desni inverz. Če oba inverza obstajata, sta enaka.*

Dokaz. Opazujmo preslikavo $x \mapsto xa$. Ker je $l_R(a) = 0$, je ta preslikava bijektivna. To pomeni, da obstaja $a_L \in R$, tako da je $a_L a = 1$, torej je a_L levi inverz a. Analogno dokažemo, da obstaja desni inverz. Če obstajata oba, velja

$$a_L = a_L(aa_D) = (a_L a)a_D = a_D,$$

torej je levi inverz a_L enak desnemu inverzu a_D. □

Zgornja lema nam pove, da za vsak element a v končnem enotskem kolobarju R velja, da je a bodisi desni delitelj niča (če je $l_R(a) \neq 0$) bodisi ima levi inverz (če je $l_R(a) = 0$) oziroma analogno je bodisi a levi delitelj niča (če $r_R(a) \neq 0$) bodisi ima desni inverz (če $r_R(a) = 0$). Sedaj se pojavi vprašanje, če obstaja kaka povezava med levimi in desnimi delitelji niča. Delno nam na to odgovori naslednja lema, ki nam pove, da so v matričnem kolobarju levi delitelji niča enaki desnim deliteljem niča.

Lema 4.3. *Naj bo R komutativni enotski kolobar in $A \in M_{n,n}(R)$. Potem velja*

(1) *A je levi delitelj niča v $M_{n,n}(R)$ natanko tedaj, ko je $\det(A) \in Z(R)$,*
(2) *A je desni delitelj niča v $M_{n,n}(R)$ natanko tedaj, ko je $\det(A) \in Z(R)$.*

Opomba 4.4. Dokaz izreka sodi v področje linearne algebre, zato ga bomo izpustili. Zainteresiran bralec ga lahko najde v [4, Izrek 9.1].

V primeru, ko je R polje, nam zgornja lema poda dobro znano dejstvo, da je matrika obrnljiva natanko tedaj, ko je njena determinanta neničelna.

Lema 4.5. *Naj bo R končni kolobar. Če obstaja $a \in R$ tak, da je $r_R(a) = l_R(a) = 0$, potem ima R enoto za množenje.*

Dokaz. Poglejmo si preslikavo $R \to R, x \mapsto xa$. Gre za homomorfizem abelovih grup in ker je $l_R(a) = 0$, je to injektivna preslikava. Ker je R končen, pa je to bijekcija. Obstaja torej $x \in R$, da je $xa = a$. Sklenemo, da za poljuben $t \in R$ velja $ta = txa$, od koder lahko zaključimo, da je $(t - tx)a = 0$ in ker je $l_R(a) = 0$, sklenemo, da za vsak $t \in R$ velja zveza $t = tx$. To pomeni, da je x desna enota za množenje.

Analogno ob upoštevanju dejstva, da je $r_R(a) = 0$ in z opazovanjem preslikave $R \to R, y \mapsto ay$ pridemo do sklepa, da obstaja $y \in R$, da je $ay = a$. Prav tako za vsak $t \in$ velja $ayt = at$ oziroma $yt = t$, kar zaključimo iz dejstva, da je $r_R(a) = 0$. Velja, da je y leva enota za množenje.

Ker veljata za vsak $t \in R$ zvezi $yt = t$ in $tx = t$, dobimo $y = yx = x$, torej je $x = y$ enota kolobarja R. □

Z $\mathrm{GF}(q)$ bomo označevali končno polje moči q.

Lema 4.6. *Naj bo R kolobar moči p. Potem je R bodisi izomorfen $\mathbb{Z}_p = \mathrm{GF}(p)$ bodisi je ničelni kolobar.*

Dokaz. Denimo, da R nima trivialnega množenja. Pokažimo najprej, da R ne more imeti neničelnega enostranskega delitelja niča. V ta namen si najprej pogledamo množico $\tilde{Z}_l(R) = \{x \in R; xy = 0 \text{ za vsak } y \in R\}$. Jasno je to podgrupa, torej je bodisi enaka 0 bodisi R. Vemo, da druga možnost odpade, ker nimamo trivialnega množenja, torej je $\tilde{Z}_l(R) = 0$. Enako vidimo, da je $\tilde{Z}_r(R) = 0$, kjer je $\tilde{Z}_r(R) = \{x \in R; yx = 0 \text{ za vsak } y \in R\}$. Pokažimo še, da ne moremo imeti takega elementa, ki bi pri množenju uničil le del elementov kolobarja. Res, če opazujemo leve ali desne anihilatorje, spet vidimo, da so to podgrupe. V primeru, ko je enostranski anihilator nekega elementa cel R, zaključimo, da je opazovani element iz $\tilde{Z}_l(R)$ ali $\tilde{Z}_r(R)$, torej je enak 0. Po lemi 4.5 ima R enoto. Po lemi 4.2 je R obseg, ker pa je končen, je $R \cong \mathrm{GF}(p)$. □

Lema 4.7. *Naj bo R končni nenilpotentni kolobar. Potem R vsebuje idempotent.*

Dokaz. Ker je R končen in nenilpotenten, obstaja element $0 \neq a \in R$, da je $a^n = a^{n+r}$ za neki naravni števili n, r. Iz zgornje zveze takoj sledi, da je $a^n = a^{n+\alpha r}$, kjer je $\alpha \in \mathbb{N}$ poljubno naravno število. Če obe strani zadnje enakosti pomnožimo še z a^β, $\beta \in \mathbb{N}$, dobimo zvezo

$$a^{n+\beta} = a^{n+\alpha r+\beta}.$$

Poiskati želimo taka $\alpha, \beta \in \mathbb{N}$, da bo veljalo $n+\alpha r+\beta = 2(n+\beta)$ oziroma $n+\beta = \alpha r$. To z lahkoto dosežemo tako, da izberemo $\alpha = \min\{\tilde{\alpha} \in \mathbb{N}; \tilde{\alpha} r \geq n\}$ in $\beta = \alpha r - n$. Iz konstrukcije je jasno, da sta $\alpha, \beta \in \mathbb{N}$ in da je element a res idempotent. □

Lema 4.8. *Naj bo R tak kolobar, da za vsak $x \in R$ velja $x^2 = 0$. Potem je R antikomutativen, kar pomeni, da za poljubna $x, y \in R$ velja $xy = -yx$.*

Dokaz. Naj bosta $x, y \in R$ poljubna neničelna elementa. Velja

$$0 = (x+y)^2 = x^2 + xy + yx + y^2 = xy + yx.$$

□

Lema 4.9. *Naj bo R končni kolobar in naj za vsak $x \in R$ velja $x^2 = 0$. Sledi, da je R nilpotenten.*

Dokaz. Naj bo $r_1, \ldots, r_k$ množica generatorjev kolobarja. Potem se v produktu poljubnih $k+1$ generatorjev zagotovo vsaj eden pojavi dvakrat. Po lemi 4.8 je R antikomutativen, zato lahko dosežemo, da v produktu poljubnih $k+1$ generatorjev nastopi kvadrat nekega elementa, torej je produkt enak 0. To pomeni, da je $R^{k+1} = 0$ in je zato R nilpotenten. □

Opomba 4.10. Če je R kolobar in za vsak $x \in R$ velja $x^2 = 0$, potem je vsak element R-ja kvaziregularen. Res, velja namreč $x + (-x) - x(-x) = x - x + x^2 = 0$.

Lema 4.11. *Naj bo R končni enotski kolobar. Naj bo $u \in U(R)$ obrnljiv element. Potem za vsak $a \in R$ velja*

$$|l_R(ua)| = |l_R(au)| = |l_R(a)| \quad \textit{in} \quad |r_R(ua)| = |r_R(au)| = |r_R(a)|.$$

Dokaz. Dokazali bomo le enakosti za leve anihilatorje, za desne namreč deluje analogen dokaz.

Očitno velja $l_R(a) \subseteq l_R(au)$. Naj bo zdaj $y \in l_R(au)$. Potem je $yau = 0$. Ker je u obrnljiv element, iz te enačbe sledi $ya = 0$, torej $y \in l_R(a)$. Sklenemo, da velja $l_R(au) = l_R(a)$.

Definirajmo preslikavo $\varphi : R \to R$, podano s predpisom $\varphi(x) = u^{-1}xu$. Ker je u obrnljiv element, se z lahkoto preveri, da je ta preslikava homomorfizem in bijekcija, torej avtomorfizem. Pokažimo, da za poljubni avtomorfizem θ velja $\theta(l_R(x)) = l_R(\theta(x))$. Če je $y \in l_R(x)$, potem iz $\theta(y)\theta(x) = \theta(yx) = \theta(0) = 0$ sledi $\theta(y) \in l_R(\theta(x))$. Sledi $\theta(l_R(x)) \subseteq l_R(\theta(x))$. Pokažimo še obratno vsebovanost. Naj bo $y \in l_R(\theta(x))$. Ker je θ avtomorfizem, obstaja z, da je $\theta(z) = y$. Potem velja $0 = y\theta(x) = \theta(z)\theta(x) = \theta(zx)$, torej je $zx = 0$. Sledi $y = \theta(z) \in \theta(l_R(x))$ in posledično $l_R(\theta(x)) \subseteq \theta(l_R(x))$. Dobili smo zvezo $\theta(l_R(x)) = l_R(\theta(x))$, ki implicira enakost $|l_R(x)| = |l_R(\theta(x))|$. To velja tudi za zgoraj definirani avtomorfizem φ. Če vstavimo za $x = ua$, dobimo $\varphi(ua) = au$. Sledi $|l_R(ua)| = |l_R(\varphi(ua))| = |l_R(au)|$. □

Lema 4.12. *Naj bo R končni enotski kolobar. Potem je $x + y \in Z(R)$ natanko tedaj, ko je $(x + J(R)) + (y + J(R)) \in Z(R/J(R))$.*

Dokaz. Naj bo $x+y \in Z(R)$. Potem obstaja $z \in R$, da je $(x+y)z = 0$. Sledi, da je $\big((x+J(R))+(y+J(R))\big)(z+J(R)) = J(R)$. Ker je $R/J(R)$ končen, je $(x+J(R))+(y+J(R))$ bodisi delitelj niča bodisi je obrnljiv. Denimo, da je obrnljiv. Potem obstaja $u \in R$, da je $1+J(R) = \big((x+J(R))+(y+J(R))\big)(u+J(R)) = (x+y)u+J(R)$. To je ekvivalentno s tem, da je $(x+y)u \in 1+J(R)$. Po posledici 2.5 so vsi elementi iz $1+J(R)$ obrnljivi. Potem je tudi $(x+y)u$ obrnljiv element kolobarja R, kar je v nasprotju s tem, da je $x+y \in Z(R)$. Sledi $(x+J(R))+(y+J(R)) \in Z(R/J(R))$.

Dokažimo še obrat. Naj bo $(x+J(R))+(y+J(R)) \in Z(R/J(R))$. Potem obstaja $z \in R \setminus J(R)$, da je $J(R) = \big(x+J(R))+(y+J(R))\big)(z+J(R)) = (x+y)z+J(R)$. Sledi, da je $(x+y)z \in J(R)$. Denimo, da je $x+y$ obrnljiv element kolobarja R. Potem obstaja $u \in R$, da je $(x+y)u = 1$. Ker je $J(R)$ ideal, je $u(x+y)z = z \in J(R)$. Protislovje z izbiro z. □

Lema 4.13. *Naj bo R končni enotski kolobar. Potem karakteristika kolobarja R deli moč kolobarja $|R|$.*

Dokaz. Naj bo karakteristika kolobarja R enaka $\mathrm{char}(R) = n$. Potem je množica $\{0,1,\ldots,n-1\}$ aditivna podgrupa moči n grupe R, torej n deli $|R|$. □

5. Idempotenti in SBI-kolobarji

Naj bo R kolobar in $e \in R$ idempotent. Potem je element $\overline{e} = e+J(R)$ idempotent v kvocientnem kolobarju $\overline{R} = R/J(R)$, saj velja $\overline{e}^2 = (e+J(R))(e+J(R)) = e^2+J(R) = e+J(R) = \overline{e}$. Če ima R enoto in je e kvaziregularen idempotent, potem iz pogoja $e(1-e) = 0$ sledi, da je $e = 0$, saj je kvaziregularnost elementa e ekvivalentna zahtevi, da je $1-e$ obrnljiv element. Ker so elementi $J(R)$ kvaziregularni, je 0 edini idempotent v $J(R)$. To se ujema z že znanim dejstvom, da je $J(R)$ nilpotenten.

Pri opazovanju idempotentov v kolobarju matrik dobimo idejo za naslednjo lemo.

Lema 5.1. *Naj bo R kolobar in $e_1 = e_1^2, e_2 = e_2^2 \in R$ idempotenta. Potem sta leva R-modula Re_1 in Re_2 izomorfna natanko tedaj, ko v R obstajata elementa e_{12}, e_{21}, za katera velja*

$$e_1e_{12}e_2 = e_{12}, \quad e_2e_{21}e_1 = e_{21}, \quad e_{12}e_{21} = e_1, \quad e_{21}e_{12} = e_2.$$

Dokaz. Naj bo najprej $\varphi : Re_1 \to Re_2$ izomorfizem levih R-modulov. Definiramo

$$e_{12} = \varphi(e_1) \quad \text{in} \quad e_{21} = \varphi^{-1}(e_2).$$

Potem velja

$$e_1e_{12} = e_1\varphi(e_1) = \varphi(e_1^2) = \varphi(e_1) = e_{12}$$

in

$$e_2e_{21} = e_2\varphi^{-1}(e_2) = \varphi^{-1}(e_2^2) = \varphi^{-1}(e_2) = e_{21}.$$

Ker je $e_{12} = \varphi(e_1) \in Re_2$, lahko zapišemo $e_{12} = r_{12}e_2$ in zato velja $e_{12}e_2 = r_{12}e_2e_2 = r_{12}e_2^2 = r_{12}e_2 = e_{12}$. Ker pa je $e_{21} = \varphi^{-1}(e_2) \in Re_1$, lahko zapišemo $e_{21} = r_{21}e_1$. Od tu takoj poračunamo $e_{21}e_1 = r_{21}e_1e_1 = r_{21}e_1^2 = r_{21}e_1 = e_{21}$. Dobili smo zveze

$$e_1e_{12} = e_{12}, \quad e_2e_{21} = e_{21}, \quad e_{12}e_2 = e_{12}, \quad e_{21}e_1 = e_{21}.$$

S pomočjo teh zvez z lahkoto dokažemo prvi dve izmed želenih zvez. Velja namreč

$$e_1e_{12}e_2 = (e_1e_{12})e_2 = e_{12}e_2 = e_{12} \quad \text{in} \quad e_2e_{21}e_1 = (e_2e_{21})e_1 = e_{21}e_1 = e_{21}.$$

Dokažimo še preostali dve zvezi. Spet si bomo pomagali z zgornjimi ugotovitvami. Velja

$$e_1 = \varphi^{-1}(\varphi(e_1)) = \varphi^{-1}(e_{12}) = \varphi^{-1}(e_{12}e_2) = e_{12}\varphi^{-1}(e_2) = e_{12}e_{21}$$

in

$$e_2 = \varphi(\varphi^{-1}(e_2)) = \varphi(e_{21}) = \varphi(e_{21}e_1) = e_{21}\varphi(e_1) = e_{21}e_{12}.$$

S tem je trditev v eno smer dokazana. Pokažimo še obrat.

Naj torej neka elementa e_{12}, e_{21} zadoščata zvezam

$$e_1e_{12}e_2 = e_{12}, \quad e_2e_{21}e_1 = e_{21}, \quad e_{12}e_{21} = e_1, \quad e_{21}e_{12} = e_2.$$

Definirajmo preslikavo $\varphi : Re_1 \to Re_2$, podano s predpisom $\varphi(e_1) = e_{12}$. Z lahkoto se preveri, da je φ dobro definiran homomorfizem levih R-modulov. Na podoben način definiramo še preslikavo $\psi : Re_2 \to Re_1$, podano s predpisom $\psi(e_2) = e_{21}$, ki je prav tako dobro definiran homomorfizem levih R-modulov. Preverimo, da velja $\psi(\varphi(e_1)) = e_1$ in $\varphi(\psi(e_2)) = e_2$. Računamo

$$\psi(\varphi(e_1)) = \psi(e_{12}) = \psi(e_1e_{12}e_2) = e_1e_{12}\psi(e_2) = e_1e_{12}e_{21} = e_1e_1 = e_1^2 = e_1$$

in

$$\varphi(\psi(e_2)) = \varphi(e_{21}) = \varphi(e_2e_{21}e_1) = e_2e_{21}\varphi(e_1) = e_2e_{21}e_{12} = e_2e_2 = e_2^2 = e_2.$$

Iz zveze $\psi(\varphi(e_1)) = e_1$ sledi, da je φ injektivna, ψ pa surjektivna. Iz zveze $\varphi(\psi(e_2)) = e_2$ pa sledi, da je ψ injektivna, φ pa surjektivna. Sklenemo, da sta φ, ψ bijekciji, torej izomorfizma. Sledi še $\psi = \varphi^{-1}$. S tem je lema dokazana. $\square$

Opomba 5.2. Analogno lemo lahko dokažemo za desne R-module. V prvem delu dokaza se spremeni le to, da definiramo $e_{21} = \varphi(e_1)$ in $e_{12} = \varphi^{-1}(e_2)$, nato pa dokažemo podobne zveze kot zgoraj in jih uporabimo za dokaz želenih zvez iz formulacije leme. Podobno tudi v drugem delu definiramo homomorfizma $\varphi : e_1R \to e_2R$ s predpisom $\varphi(e_1) = e_{21}$ in $\psi : e_2R \to e_1R$ s predpisom $\psi(e_2) = e_{12}$, nato pa z njuno pomočjo pokažemo, da sta desna R-modula e_1R in e_2R izomorfna.

Lema 5.3. *Naj bo R kolobar in $\overline{R} = R/J(R)$. Naj bosta $e_1 = e_1^2 \neq 0$ in $e_2 = e_2^2 \neq 0$ idempotenta v R. Potem velja, da sta R-podmodula Re_1 in Re_2 modula R izomorfna natanko tedaj, ko sta izomorfna $\overline{R}$ podmodula $\overline{R}\overline{e}_1$ in $\overline{R}\overline{e}_2$ modula $\overline{R}$.*

Dokaz. Denimo, da sta $Re_1 \cong Re_2$. Potem po lemi 5.1 obstajata elementa $e_{12}, e_{21} \in R$, ki zadoščata zvezam

$$e_{12}e_{21} = e_1, \quad e_{21}e_{12} = e_2, \quad e_1e_{12}e_2 = e_{12}, \quad e_2e_{21}e_1 = e_{21}.$$

Poglejmo si preslikavo $\varphi : R \to R/J(R)$, podano s predpisom $x \mapsto \overline{x} = x + J(R)$. Naj bosta $\overline{e}_{12} = \varphi(e_{12}), \overline{e}_{21} = \varphi(e_{21})$. Zanju velja

$$\overline{e}_{12}\overline{e}_{21} = (e_{12} + J(R))(e_{21} + J(R)) = e_{12}e_{21} + J(R) = e_1 + J(R) = \overline{e}_1,$$

$$\overline{e}_{21}\overline{e}_{12} = (e_{21} + J(R))(e_{12} + J(R)) = e_{21}e_{12} + J(R) = e_2 + J(R) = \overline{e}_2,$$

$$\overline{e}_1\overline{e}_{12}\overline{e}_2 = (e_1 + J(R))(e_{12} + J(R))(e_2 + J(R)) = e_1e_{12}e_2 + J(R) = e_{12} + J(R) = \overline{e}_{12},$$

$$\overline{e}_2\overline{e}_{21}\overline{e}_1 = (e_2 + J(R))(e_{21} + J(R))(e_1 + J(R)) = e_2e_{21}e_1 + J(R) = e_{21} + J(R) = \overline{e}_{21}.$$

Ker vse te zveze veljajo, po lemi 5.1 sledi, da je $\overline{R}\overline{e}_1 \cong \overline{R}\overline{e}_2$.

Dokažimo še obrat. Ker je $\overline{R}\overline{e}_1 \cong \overline{R}\overline{e}_2$, obstajata elementa $u_{12}, u_{21} \in R$, za katera velja

$$\overline{e}_1\overline{u}_{12}\overline{e}_2 = \overline{u}_{12}, \quad \overline{e}_2\overline{u}_{21}\overline{e}_1 = \overline{u}_{21}, \quad \overline{u}_{12}\overline{u}_{21} = \overline{e}_1, \quad \overline{u}_{21}\overline{u}_{12} = \overline{e}_2.$$

Predpostavimo lahko, da velja $e_1u_{12}e_2 = u_{12}$ in $e_2u_{21}e_1 = u_{21}$ (sicer zamenjamo u_{12} z $e_1u_{12}e_2$ in u_{21} z $e_2u_{21}e_1$). Ker je

$$e_1 + J(R) = \overline{e}_1 = \overline{u}_{12}\overline{u}_{21} = \overline{e}_1\overline{u}_{12}\overline{e}_2\overline{e}_2\overline{u}_{21}\overline{e}_1 = e_1u_{12}e_2u_{21}e_1 + J(R),$$

je $e_1 - e_1u_{12}e_2u_{21}e_1 \in J(R)$. Ker je e_1 idempotent, je $e_1 - e_1u_{12}e_2u_{21}e_1 \in e_1Re_1$. Izberemo lahko $z_1 \in e_1Re_1 \cap J(R)$, da je $u_{12}u_{21} = e_1 - z_1$. Ker je $z_1 \in J(R)$, je kvaziregularen. Naj bo z_1' njegov kvaziinverz, kar pomeni, da je $z_1 + z_1' - z_1z_1' = 0$. Potem je

$$u_{12}u_{21}(e_1 - z_1') = (e_1 - z_1)(e_1 - z_1') = e_1 - e_1z_1' - z_1e_1 + z_1z_1' =$$
$$e_1 - e_1z_1' - e_1z_1 + e_1z_1z_1' = e_1 - e_1(z_1' + z_1 - z_1z_1') = e_1 - e_1 \cdot 0 = e_1.$$

Definirajmo $e_{12} = u_{12}$ in $e_{21} = u_{21}(e_1 - z_1')$. Velja $\overline{e}_{12} = \overline{u}_{12}$ in $\overline{e}_{21} = \overline{u_{21}(e_1 - z_1')} = \overline{u_{21}e_1} = \overline{u}_{21}\overline{e}_1 = \overline{e}_2\overline{u}_{21}\overline{e}_1\overline{e}_1 = \overline{e}_2\overline{u}_{21}\overline{e}_1 = \overline{u}_{21}$.

Podobno kot zgoraj lahko zapišemo $e_{21}e_{12} = e_2 - z_2$ za neki $z_2 \in e_2Re_2 \cap J(R)$. Velja $e_{21}e_{12}e_{21}e_{12} = e_{21}e_1e_{12} = e_{21}e_1u_{12} = e_{21}u_{12} = e_{21}e_{12}$, zato je $(e_{21}e_{12})^2 = e_{21}e_{12}$. To je ekvivalentno temu, da je $(e_2 - z_2)^2 = e_2 - z_2$. Iz te zveze lahko izrazimo z_2 kot $z_2 = e_2 - (e_2 - z_2)^2$. Naredimo naslednji račun

$$z_2^2 = (e_2 - (e_2 - z_2)^2)^2 = e_2 - e_2(e_2 - z_2)^2 - (e_2 - z_2)^2e_2 + (e_2 - z_2)^4 =$$
$$e_2 - (e_2 - z_2)^2 - (e_2 - z_2)^2 + (e_2 - z_2)^2 = e_2 - (e_2 - z_2)^2 = z_2.$$

To pomeni, da je $z_2 = z_2^2$. Ker je $z_2 \in J(R)$ in idempotenten, je $z_2 = 0$. Ker je $z_2 = 0$, je $e_{21}e_{12} = e_2$. Videli smo že, da je $e_1 = u_{12}u_{21}(e_1 - z_1') = e_{12}e_{21}$. Velja še

$$e_1e_{12}e_2 = e_1u_{12}e_2 = u_{12} = e_{12}$$

in

$$e_2e_{21}e_1 = e_2u_{21}(e_1 - z_1')e_1 = e_2u_{21}e_1(e_1 - z_1') = u_{21}(e_1 - z_1') = e_{21}.$$

Po lemi 5.1 sledi, da je $Re_1 \cong Re_2$. □

Definicija 5.4. Naj bo R kolobar in $J(R)$ njegov Jacobsonov radikal. Kolobar R je *SBI-kolobar* natanko tedaj, ko sta izpolnjena pogoja

(1) za $z \in J(R)$ obstaja tak $z_1 \in J(R)$, da je $z_1^2 - z_1 = z$ (v nadaljevanju bomo temu rekli, da ima enačba $x^2 - x = z$ rešitev $z_1 \in J(R)$), za katerega velja,
(2) da podkolobar elementov kolobarja R, ki komutirajo z z, sovpada s podkolobarjem elementov, ki komutirajo z z_1.

Opomba 5.5. Izraz SBI-kolobar je vpeljal Kaplansky in je okrajšava za *suitable for building idempotent elements*. V nadaljevanju bomo videli, zakaj je tako poimenovanje smiselno.

Lema 5.6. *Naj bo R enotski SBI-kolobar. Potem velja*

(1) *obstaja največ ena rešitev enačbe $x^2 - x = z$, ki zadošča drugemu pogoju iz definicije 5.4,*
(2) *$zu = 0$ (oz. $uz = 0$) implicira $z_1u = 0$ (oz. $uz_1 = 0$),*
(3) *če z pripada desnemu (levemu) idealu I, potem $z_1 \in I$.*

Dokaz. Dokažimo vsako točko posebej. Začnimo s prvo.

(1) Naj bosta z_1, z_2 rešitvi enačbe $x^2 - x = z$, ki zadoščata drugi točki definicije 5.4. Ker je z_2 rešitev enačbe, jasno komutira z z. Po drugi točki definicije potem komutira tudi z z_1, torej $z_1z_2 = z_2z_1$. Po drugi strani pa oba rešita enačbo, torej je $z_1^2 - z_1 = z_2^2 - z_2$. To je ekvivalentno $z_1^2 - z_2^2 - (z_1 - z_2) = 0$

oziroma $(z_1-z_2)(z_1+z_2-1)=0$. Ker sta $z_1, z_2 \in J(R)$, je tudi $z_1+z_2 \in J(R)$, kar pomeni, da je element z_1+z_2-1 obrnljiv. Zaključimo, da je $z_1-z_2=0$.

(2) Iz pogoja $zu=0$ sledi, da je $z_1^2u-z_1u=0$ oziroma $(z_1-1)z_1u=0$. Ker je $z_1 \in J(R)$, je $1-z_1$ obrnljiv, torej je $z_1u=0$.

(3) Ker je $z_1 \in J(R)$, je $z_1 = z(z_1-1)^{-1}$ in ker je $z \in I$, je tudi $z_1 \in I$.

□

Za nadaljnji študij SBI-kolobarjev bomo potrebovali dve tehnični lemi.

Lema 5.7. *Velja naslednja zveza*

$$\frac{1}{2}\Big(1-(1+4z)^{\frac{1}{2}}\Big) = \sum_{n=1}^{\infty} \frac{1}{2n-1}\binom{2n-1}{n}(-z)^n.$$

Dokaz. Ker velja

$$\frac{1}{2}\Big(1-(1+4z)^{\frac{1}{2}}\Big) = \frac{1}{2}\Big(1-\sum_{n=0}^{\infty}\binom{1/2}{n}(4z)^n\Big) = -\frac{1}{2}\sum_{n=1}^{\infty}\binom{1/2}{n}(4z)^n,$$

zadošča dokazati, da za vsak $n \in \mathbb{N}$ velja

$$-\frac{1}{2}\binom{1/2}{n}4^n = \frac{(-1)^n}{2n-1}\binom{2n-1}{n}.$$

Opazimo, da pri $n=1$ enakost velja.

Preoblikujemo izraz na levi strani

$$-2^{2n-1}\binom{1/2}{n} = -2^{2n-1}\frac{\frac{1}{2}(\frac{1}{2}-1)(\frac{1}{2}-2)\cdots(\frac{1}{2}-n+1)}{n(n-1)\cdots 3\cdot 2\cdot 1} =$$

$$-2^{2n-1}\Big(\frac{1}{2}\Big)^n(-1)^{n-1}\frac{(2-1)(4-1)(6-1)\cdots(2(n-1)-1)}{n(n-1)\cdots 2\cdot 1} =$$

$$(-1)^n 2^{n-1}\frac{1\cdot 3\cdot 5\cdot 7\cdots(2n-5)(2n-3)}{n(n-1)\cdots 2\cdot 1}.$$

Ko si pogledamo izraz na desni, opazimo, da zadošča za vsak $n \geq 2$ dokazati zvezo

$$2^{n-1}\Big(1\cdot 3\cdot 5\cdot 7\cdots(2n-5)(2n-3)\Big) = (2n-2)(2n-3)\cdots(n+1)n.$$

Uporabimo indukcijo. Pri $n=2$ na levi dobimo $2(4-3)=2$, na desni pa $2\cdot 2-2=2$, torej se izraza ujemata. Pokažimo, da zveza velja za $n+1$. Po indukcijski predpostavki za n velja

$$2^{n-1}(1\cdot 3\cdot 5\cdots(2n-5)(2n-3)) = n(n+1)\cdots(2n-3)(2n-2).$$

Napišimo levo stran želene enakosti pri $n+1$ in jo preoblikujmo. Dobimo

$$2^n\Big(1\cdot 3\cdot 5\cdots(2n-5)(2n-3)(2n-1)\Big) = 2(2n-1)\Big[2^{n-1}\Big(1\cdot 3\cdot 5\cdots(2n-5)(2n-3)\Big)\Big] =$$

$$2(2n-1)\Big[(2n-2)(2n-3)\cdots(n+1)n\Big] = (2n)(2n-1)(2n-2)(2n-3)\cdots(n+1).$$

Izraz na koncu je ravno desna stran želene enakosti pri $n+1$. S tem je lema dokazana. □

Lema 5.8. *Za vsak $n \in \mathbb{N}$ je*

$$\frac{1}{2n-1}\binom{2n-1}{n} \in \mathbb{N}.$$

Dokaz. Za $n \geq 1$ velja

$$\frac{1}{2n-1}\binom{2n-1}{n} = \frac{1}{2n-1} \cdot \frac{(2n-1)!}{n!(n-1)!} = \frac{(2n-2)!}{n!(n-1)!} = \frac{1}{n}\binom{2(n-1)}{n-1} = C_{n-1},$$

kjer je $C_n = \frac{1}{n+1}\binom{2n}{n}$ n-to Catalanovo število. $\square$

Lema 5.9. *Naj bo R kolobar. Če je $J(R)$ nil ideal, je R SBI-kolobar.*

Dokaz. Rešiti želimo enačbo $x^2 - x - z = 0$. Idejo za iskano rešitev dobimo pri rešitvi običajne kvadratne enačbe. Zapišimo $z_1 = \frac{1-(1+4z)^{\frac{1}{2}}}{2}$. Pokazati moramo, da je to res element kolobarja. Po lemi 5.7 element z_1 razvijemo v vrsto

$$z_1 = \sum_{n=1}^{\infty} \frac{1}{2n-1}\binom{2n-1}{n}(-z)^n.$$

Po lemi 5.8 vemo, da so koeficienti cela števila. Ker je z nilpotenten, gre dejansko za polinom v z-ju z ničelnim prostim členom, torej je $z_1 \in J(R)$ (opazimo še, da za izražanje elementa z_1 ne potrebujemo enote). Jasno je tudi, da poljuben element x komutira z $z = z_1^2 - z_1$ natanko tedaj, ko komutira z z_1. $\square$

Primer 5.10. Vsak artinski kolobar je SBI-kolobar.

Naslednja lema upraviči poimenovanje SBI-kolobarjev.

Lema 5.11. *Naj bo R enotski SBI-kolobar z Jacobsonovim radikalom $J(R)$. Označimo z $\overline{R} = R/J(R)$ in $\overline{x} = x + J(R)$. Če je $\overline{u} \in \overline{R}$ idempotent, potem obstaja $e \in R$, ki zadošča $e^2 = e$ in $\overline{e} = \overline{u}$.*

Dokaz. Zapišemo lahko $u^2 = u + z$, kjer je $z \in J(R)$. Velja, da je element $1 + 4z$ obrnljiv. Ker je R SBI-kolobar, obstaja $z_1 \in J(R)$, ki reši enačbo $x^2 - x = -z(1 + 4z)^{-1}$. Ker u komutira z $z = u^2 - u$, je jasno, da komutira tudi z $-z(1 + 4z)^{-1}$. Posledično tudi rešitev enačbe z_1 komutira z u (sledi iz definicije SBI-kolobarja). Definirajmo $f = 1 - 2z_1$ in $g = z_1$. Iz zgoraj napisanega sledi, da f, g in u paroma komutirajo. Preverimo sedaj, da velja

$$f^2 + 2fg = 1 - 4z_1 + 4z_1^2 + 2z_1 - 4z_1^2 = 1 - 2z_1 = f$$

in

$$\begin{gathered} zf^2 + g^2 = z(1 - 4z_1 + 4z_1^2) + z_1^2 = \\ z - 4zz_1 + z_1^2(1 + 4z) - z_1(1 + 4z) + z_1(1 + 4z) = \\ z - 4zz_1 + (z_1^2 - z_1)(1 + 4z) + z_1 + 4zz_1 = z - z + z_1 = z_1 = g, \end{gathered}$$

torej smo dobili zvezi $f^2 + 2fg = f$ ter $zf^2 + g^2 = g$. Definiramo $e = uf + g$ in s pomočjo gornjih dveh zvez poračunamo, da je e idempotent. Velja namreč

$$\begin{gathered} e^2 = u^2f^2 + g^2 + 2ufg = (u + z)f^2 + g^2 + 2ufg = \\ u(f^2 + 2fg) + (zf^2 + g^2) = uf + g = e. \end{gathered}$$

Iz konstrukcije f in g je jasno, da velja še $\overline{e} = \overline{u}$. $\square$

Opomba 5.12. Zgornja lema velja tudi v poljubnem kolobarju R brez enote, ki zadošča pogoju, da je Jacobsonov radikal $J(R)$ nil ideal, vendar smo se zgoraj omejili na dokaz v primeru enotskih kolobarjev, ker je v tem primeru dokaz bolj pregleden. Enako kot zgoraj lahko zapišemo, da je $u^2 - u = z \in J(R)$. Enako kot zgoraj želimo poiskati $z_1 \in J(R)$, ki reši enačbo $x^2 - x = -z(1 + 4z)^{-1}$. Pri tem je desna stran te enačbe dobro definirana, saj je to polinom v elementu z, ki ima ničelni prosti člen.

Opazimo še, da nam zgornja enačba poda zvezo $-z = z_1^2 + 4z_1^2 z - z_1 - 4zz_1$. Če v njej upoštevamo, da je $z = u^2 - u$, dobimo zvezo $-u^2 + u = z_1^2 + 4z_1^2 u^2 - 4z_1^2 u - 4z_1 u^2 + 4z_1 u - z_1$. Sedaj definiramo $e = u - uz_1 + z_1$. Potem je očitno $\overline{e} = \overline{u}$. Poleg tega je $e^2 = (u - 2uz_1 + z_1)(u - 2uz_1 + z_1) = u^2 - 4u^2 z_1 + 2uz_1 - 4uz_1^2 + z_1^2 + 4u^2 z_1^2 = u + z_1 - 2uz_1 = e$. S tem se trditev posploši na kolobarje brez enote.

Zgornjo lemo lahko posplošimo na več idempotentov.

Lema 5.13. *Naj bo R enotski SBI-kolobar, $\overline{R} = R/J(R)$ in $\overline{x} = x + J(R)$. Če je $\{\overline{u}_i | i = 1, \dots, n\}$ končna množica ortogonalnih idempotentov v $\overline{R}$, potem obstaja ortogonalna množica idempotentov $\{e_i | i = 1, \dots, n\} \subseteq R$, da je $\overline{e}_i = \overline{u}_i, i = 1 \dots, n$. Poleg tega iz $\sum_{i=1}^n \overline{u}_i = \overline{1}$ sledi še $\sum_{i=1}^n e_i = 1$.*

Dokaz. Dokazujemo z indukcijo. Primer $n = 1$ smo obdelali v lemi 5.11. Predpostavimo sedaj, da že imamo idempotente $e_1, \dots, e_m$ za katere velja $e_i e_j = 0$ za $i \neq j$ in $\overline{e}_i = \overline{u}_i$ za $i = 1, \dots, m$. Definirajmo $e = \sum_{i=1}^m e_i$ in $u = u_{m+1} - eu_{m+1} - u_{m+1}e + eu_{m+1}e$. Potem je $\overline{u} = \overline{u}_{m+1}$ in $eu = 0 = ue$ (to se preveri z enostavnim računom). Enako kot v dokazu leme 5.11 najdemo idempotent $e_{m+1} = u(1-2z)+z_1$, kjer je $z_1^2 - z_1 = -z(1+4z)^{-1}$ in $z = u^2 - u$. Ker je $z = u^2 - u \in (1-e)R(1-e) = (1-e)R \cap R(1-e)$ (to velja, ker je $eu = ue = 0$ in je zato $u \in (1-e)R(1-e)$), je po tretji točki leme 5.6 tudi $z_1 \in (1-e)R \cap R(1-e) = (1-e)R(1-e)$. Potem pa velja, da je $e_{m+1} = u(1-2z_1) + z_1 = u - 2uz_1 + z_1 \in (1-e)R(1-e)$, ker je $(1-e)R(1-e)$ podkolobar, ki vsebuje u in z_1. Torej lahko zapišemo $e_{m+1} = (1-e)\tilde{e}_{m+1}(1-e)$. Ker po predpostavki velja $e_i e = e_i = ee_i$, takoj dobimo še zvezi $e_i e_{m+1} = 0 = e_{m+1} e_i$. Dokažimo le prvo, drugo namreč dobimo podobno. Velja

$$e_i e_{m+1} = e_i(1-e)\tilde{e}_{m+1}(1-e) = (e_i - e_i)\tilde{e}_{m+1}(1-e) = 0.$$

Sledi, da je $\{e_1, \dots, e_{m+1}\}$ množica ortogonalnih idempotentov. Iz konstrukcije e_{m+1} sledi še, da je $\overline{e}_{m+1} = \overline{u}_{m+1}$, za ostale pa to velja po indukcijski predpostavki. S tem je prvi del trditve dokazan.

Recimo še, da je $\sum_{i=1}^n \overline{u}_i = \overline{1}$. Definirajmo $e = \sum_{i=1}^n e_i$. Velja $\overline{e} = \overline{1}$. Po definiciji kvocientnega kolobarja to pomeni, da je $e = 1 + x$, $x \in J(R)$. Ker je $1 + x = e = e^2 = 1 + 2x + x^2$, mora veljati $x^2 = -x$. To je ekvivalentno temu, da je $x(1+x) = 0$ in ker je $x \in J(R)$, je $1 + x$ obrnljiv element, torej mora biti $x = 0$. To pomeni, da je $e = 1$ in s tem je lema dokazana. ☐

Opomba 5.14. Prvi del leme o dvigu ortogonalnih idempotentov lahko enako kot prej posplošimo na kolobarje brez enote. Če se namreč poglobimo v dokaz, opazimo, da je enota priročna le zaradi enostavnejšega zapisa in računanja.

Lema 5.15. *Naj bo R enotski SBI-kolobar. Naj vsak neničelni desni ideal kolobarja $\overline{R} = R/J(R)$ vsebuje neničelni idempotent. Potem vsak desni ideal v R, ki ni vsebovan v $J(R)$, vsebuje neničelni idempotent.*

Dokaz. Naj bo I desni ideal kolobarja R, ki ni vsebovan v $J(R)$. Potem je $(I + J(R))/J(R) \neq \overline{0}$. Posledično je za neki $u \in I$ po predpostavki element $\overline{u}$ idempotent v $\overline{I}$. Zapišemo lahko $\overline{u} = u + r, u \in I, r \in J(R)$. Ker je $\overline{u}^2 = \overline{u}$, dobimo, da je $u + r = u^2 + \tilde{r}, \tilde{r}, r \in J(R)$ oziroma $z = u^2 - u \in J(R)$. Po drugi strani je $z \in I$, saj je $u \in I$. Iz prvega pogoja sledi, da je $1 + 4z$ obrnljiv element, iz drugega pogoja pa sledi, da je $-z(1 + 4z)^{-1} \in I$ (ker je desni ideal). Opazujmo enačbo $x^2 - x = -z(1 + 4z)^{-1}$. Ker je R SBI-kolobar, ima rešitev $z_1 \in J(R)$. Ker pa je $-z(1 + 4z)^{-1} \in I$, je po tretji točki leme 5.6 tudi $z_1 \in I$. Uporabimo sedaj formulo za e iz dokaza leme 5.11. Definiramo $e = u(1-2z_1) + z_1 = u - 2uz_1 + z_1 \in I$ (je vsota treh elementov iz ideala I). Ker je $\overline{e} = \overline{u}$, je $e \neq 0$. Na ta način smo v I našli neničelen idempotent. □

Naj bo R enotski kolobar in $\mathbb{M}_n(R)$ kolobar matrik nad R. Množici vseh matrik oblike $\{e_{i,j}, i,j = 1,\dots,n\}$, kjer je $e_{i,j}$ matrika, ki ima na mestu (i,j) element 1, drugje pa ničle, pravimo *množica matričnih enot.* Označevali jih bomo tudi z $u_{i,j}, E_{i,j}$. Zapišimo glavni izrek tega razdelka.

Izrek 5.16. *Naj bo R enotski SBI-kolobar. Denimo, da je $\overline{R} = R/J(R) \cong \mathbb{M}_n(\overline{B})$ za neki kolobar $\overline{B}$. Potem je $R \cong \mathbb{M}_n(D)$, kjer je D tak kolobar, da je $D/J(D) \cong \overline{B}$.*

Dokaz. Ker ima R enoto, jo ima tudi $R/J(R)$. Posledično je $\mathbb{M}_n(\overline{B})$ enotski kolobar. Od tod sledi, da mora imeti tudi $\overline{B}$ enoto. Posledično $\mathbb{M}_n(\overline{B})$ vsebuje množico matričnih enot $\{u_{i,j}, i,j = 1,\dots,n\}$. Enostavno se vidi še, da je $\overline{B} \cong \overline{u}_{11}\overline{R}\overline{u}_{11}$. Po lemi 5.13 lahko najdemo ortogonalne idempotente $e_{ii} \in R$, da je $\overline{e}_{ii} = \overline{u}_{ii}$ in $\sum_{i=1}^{n} e_{ii} = 1$. Po lemi 5.3 vemo, da sta dva podmodula Re_{ii} in Re_{jj} izomorfna natanko tedaj, ko sta izomorfna $\overline{R}\overline{e}_{ii}$ in $\overline{R}\overline{e}_{jj}$. Ker sta v kvocientu poljubna leva modula $\overline{R}\overline{e}_{ii}$ in $\overline{R}\overline{e}_{jj}$ izomorfna, morata biti torej tudi poljubna modula Re_{ii} in Re_{jj} izomorfna. Posebej to pomeni, da je Re_{11} izomorfen poljubnemu modulu Re_{ii}. To je po lemi 5.1 ekvivalentno s tem, da obstajajo elementi $e_{i1}, e_{1i} \in R, i = 1,\dots,n$, da velja $\overline{e}_{1i} = \overline{u}_{1i}, \overline{e}_{i1} = \overline{u}_{i1}, e_{ii}e_{i1}e_{11} = e_{i1}, e_{11}e_{1i}e_{ii} = e_{1i}, e_{1i}e_{i1} = e_{11}, e_{i1}e_{1i} = e_{ii}, i = 1,\dots,n$. Sedaj lahko definiramo še $e_{ij} = e_{i1}e_{1j}, i,j = 1,\dots,n$. Tako smo dobili množico matričnih enot $\{e_{ij} | i,j = 1,\dots,n\} \subseteq R$. Sledi, da je $R \cong M_n(D)$ za neki D in $D \cong e_{11}Re_{11}$. Po lemi 2.21 velja še $J(D) = J(e_{11}Re_{11}) = e_{11}Re_{11} \cap J(R)$. Od tod dobimo (s pomočjo drugega izreka o izomorfizmih)

$$e_{11}Re_{11}/(e_{11}Re_{11} \cap J(R)) \cong (e_{11}Re_{11} + J(R))/J(R) \cong \overline{e}_{11}\overline{R}\overline{e}_{11} = \overline{u}_{11}\overline{R}\overline{u}_{11} = \overline{B}.$$

Če združimo začetek in konec, dobimo še $D/J(D) \cong \overline{B}$. □

6. Osnovni kolobarji z deljenjem

Naj bo R komutativni enotski kolobar. Pravimo, da sta matriki $A, B \in \mathbb{M}_{m\times n}(R)$ *ekvivalentni*, če obstajata obrnljivi matriki $P \in \mathbb{M}_m(R)$ in $Q \in \mathbb{M}_n(R)$, ki zadoščata $PAQ = B$. Če sta A in B ekvivalentni, bomo to označili z $A \approx B$. Ekvivalentnost matrik je ekvivalenčna relacija.

Definicija 6.1. Komutativni enotski kolobar je *osnovni kolobar z deljenjem*, če za vsaka $m, n \geq 1$ in za vsako matriko $A \in \mathbb{M}_{m\times n}(R)$ obstaja diagonalna matrika $D = \operatorname{diag}(d_1,\dots,d_r) \in \mathbb{M}_{m\times n}(R), r = \min\{m,n\}$, ki zadošča

(1) $A \approx D$ in
(2) $d_i | d_{i+1}$ za vsak $1 \leq i \leq r-1$.

Elementom $d_1,\dots,d_r$ pravimo *osnovni delitelji* matrike A.

Spomnimo se, da je komutativni enotski kolobar *glavni kolobar*, če je vsak njegov ideal glavni, kar pomeni, da za vsak ideal I obstaja $x \in R$, da je $I = Rx$.

Zdaj lahko zapišemo najpomembnejši izrek iz tega razdelka.

Izrek 6.2. *Vsak glavni kolobar je osnovni kolobar z deljenjem.*

Dokaz tega izreka bomo izpustili, ker bi preveč razširil obseg tega dela. Zainteresiran bralec si lahko dokaz pogleda v [4, Izrek 15.9].

7. Prerezna vozlišča

Definirajmo graf deliteljev niča. Naj bo R komutativni kolobar in $Z(R)^*$ množica njegovih neničelnih deliteljev niča. *Graf deliteljev niča* je graf, ki ima za vozlišča elemente $Z(R)^*$, dve različni vozlišči $x \neq y$ pa sta povezani natanko tedaj, ko je $xy = 0$. To definicijo enostavno posplošimo na nekomutativne kolobarje. *Neusmerjeni graf deliteljev niča* nekomutativnega kolobarja R je zopet graf, ki ima za vozlišča neničelne delitelje niča, dve različni vozlišči $x \neq y$ pa sta povezani natanko tedaj, ko je $xy = 0$ ali $yx = 0$. V obeh primerih ta graf označimo z $\Gamma(R)$. Na tem mestu omenimo še, da bomo v nadaljevanju spoznali tudi usmerjeni graf deliteljev niča.

Definirajmo še nekaj pojmov. Vozlišče $v \in V(G)$ je *prerezno vozlišče*, če ima graf G', ki ga dobimo iz grafa G z odstranitvijo vozlišča v in vseh pripadajočih povezav, več komponent za povezanost kot graf G. Z $d(x, y)$ označimo razdaljo med x in y, to je dolžino najkrajše poti med x in y. Za poljubno vozlišče $v \in V(G)$ grafa G lahko definiramo *ekscentričnost* vozlišča v kot $e(v) = \sup\{d(v, u); u \in V(G)\}$. Definiramo še *polmer* grafa G kot $\inf\{e(v); v \in V(G)\}$ in *premer* grafa G kot $\sup\{e(v); v \in V(G)\}$. *Center* grafa G je množica vseh vozlišč $v \in V(G)$, za katere je njihova ekscentričnost $e(v)$ enaka polmeru grafa. S K_n bomo označevali poln graf na n vozliščih in podobno bo $K_{m,n}$ označeval poln dvodelen graf.

Dokažimo najprej naslednjo oceno za polmer.

Lema 7.1. *Naj bo R enotski komutativni noetherski kolobar, ki ni cel. Potem je polmer grafa $\Gamma(R)$ največ 2.*

Dokaz. Po [16, Izrek 3.8] vemo, da je graf deliteljev niča povezan.

Polmer bo 0 natanko tedaj, ko bo imel graf eno samo vozlišče. To se zgodi natanko tedaj, ko je R izomorfen bodisi $\mathbb{Z}_4$ bodisi $\mathbb{Z}_2[x]/(x^2)$ (glej [1, Primer 2.1(a)]).

Vprašajmo se, kdaj bo polmer grafa enak 1. To bo res natanko tedaj, ko bo graf vseboval vozlišče, ki bo sosedno z vsemi ostalimi vozlišči. Po [16, Izrek 3.12] vemo, da bo to natanko tedaj, ko bo $R \cong \mathbb{Z}_2 \times A$, kjer je A cel kolobar, ali pa je množica deliteljev niča $Z(R) = \mathrm{ann}_R(x)$ za neki $x \in R$. V drugem primeru je množica deliteljev niča ideal kolobarja R. Velja tudi obrat. Če je $Z(R)$ ideal, je po [11, Izrek 82] $Z(R) = \mathrm{ann}_R(x)$ za neki $x \in Z(R)$. Potem je vozlišče x sosedno z vsemi ostalimi vozlišči iz $\Gamma(R)$ in je polmer grafa enak 1.

Sedaj lahko predpostavimo, da množica $Z(R)$ ni ideal. Po [2, Trditev 4.7] lahko množico vseh deliteljev niča $Z(R)$ zapišemo kot unijo minimalnih praidealov kolobarja R. Ker $Z(R)$ ni ideal, je v zapisu $Z(R) = \cup_{i=1}^{n} P_i$ (P_i minimalni praideali) število $n \geq 2$.

Predpostavimo najprej, da je R reduciran kolobar, kar pomeni, da nima neničelnih nilpotentnih elementov. V tem primeru je $0 = \mathrm{Nil}(R) = \cap_{i=1}^{n} P_i$ (P_i minimalni praideali). Za vsak $i = 1, \ldots, n$ lahko izberemo neničelni element $0 \neq y_i \in P_1 \cap \cdots \cap P_{i-1} \cap P_{i+1} \cap \cdots \cap P_n$. Naj bo še $x \in Z(R)$. Potem je $x \in P_m$ za neki $1 \leq m \leq n$. Sledi, da je $xy_m \in P_m$ in posledično je $xy_m \in \cap_{i=1}^{n} P_i = \mathrm{Nil}(R) = 0$. To pomeni, da je $xy_m = 0$. Jasno je tudi $y_m y_i \in P_m$ za vsak $i \neq m$ in po istem premisleku kot zgoraj sledi, da je $y_m y_i = 0$. V grafu deliteljev niča $\Gamma(R)$ je torej razdalja med x in y_m enaka 1, med x in $y_i, i \neq m$ pa največ 2 (po zgornjem premisleku obstaja pot $x - y_m - y_i$). Ta premislek implicira, da v grafu obstaja vozlišče z ekscentričnostjo, ki ni večja od 2. Res, če vzamemo vozlišče $x \in P_1 \cap \cdots \cap P_{n-1}$, potem je po zgornjem premisleku x od poljubnega vozlišča $y \in P_n$ oddaljeno največ za 1, če pa je $y \in P_i, 1 \leq i \leq n-1$, pa je $d(x,y) \leq 2$ (po zgornjem sta povezana preko y_i). Sledi, da je $e(x) \leq 2$ in posledično je polmer grafa $\Gamma(R)$ največ 2.

Naj bo še $\mathrm{Nil}(R) \neq 0$, torej R ni reduciran. Po [11, Izrek 86] za vsak $1 \leq i \leq n$ obstaja $x_i \in R$, da je $P_i = \mathrm{ann}_R(x_i)$. Ker R ni reduciran, obstaja $0 \neq x \in \mathrm{Nil}(R) = \cap_{i=1}^n P_i = \cap_{i=1}^n \mathrm{ann}_r(x_i)$. Zato je $x \in \mathrm{ann}_R(x_i)$ za $1 \leq i \leq n$ oziroma $xx_i = 0$ za vsak $1 \leq i \leq n$. Naj bo $y \in Z(R)$. Spet obstaja indeks i, da je $y \in P_i = \mathrm{ann}_R(x_i)$. Če je $xy = 0$, je $d(x,y) = 1$, sicer pa je $d(x,y) = 2$, saj obstaja pot $x - x_i - y$. Zato ima vozlišče x ekscentričnost $e(x) \leq 2$ in zato je polmer grafa $\Gamma(R)$ največ 2. ☐

Pravimo, da se graf G *razcepi v podgrafa X in Y preko vozlišča a*, če

(1) $|V(X)|, |V(Y)| \geq 2$,
(2) $X \cup Y = G$,
(3) $V(X) \cap V(Y) = \{a\}$,
(4) vozlišče a je prerezno vozlišče G,
(5) za $x \in V(X) \setminus \{a\}$ in $y \in V(Y) \setminus \{a\}$ v grafu G ni povezave $x - y$.

Sedaj lahko dokažemo nekaj povsem enostavnih lem.

Lema 7.2. *Naj bo R komutativni enotski kolobar in naj se $\Gamma(R)$ razcepi v podgrafa X in Y preko vozlišča $a \neq 0$. Potem je $\{0, a\}$ ideal v R.*

Dokaz. Velja $a \neq a + a \in Z(R)$. Predpostavimo lahko, da je $a + a \in V(X) \setminus \{a\}$. Naj bo $b \in V(Y) \setminus \{a\}$, za katerega velja $ab = 0$. Tak b obstaja, ker je po definiciji $|V(Y)| \geq 2$ in ker je a prerezno vozlišče, torej gre vsaka pot iz $Y - a$ v $X - a$ preko vozlišča a. Potem je $(a + a)b = 0$, zato je $a + a = 0 \in \{0, a\}$ (sicer pridemo v nasprotje z zgornjo definicijo). Podobno dokažemo še $ra \in \{0, a\}$ za vsak $r \in R$. ☐

Iz te leme takoj sledi, da za $r \in R \setminus Z(R)$ velja $ra = a$ (a prerezno vozlišče kot zgoraj). Če $s \notin Z(R)$, potem je jasno tudi, da $-s \notin Z(R)$. Za elementa $s, r \notin Z(R)$ torej velja $a = ra = -sa$, od tu pa sledi, da je $(r + s)a = 0$ in zato $r + s \in Z(R)$.

Lema 7.3. *Naj bo R komutativni enotski kolobar. Naj se graf $\Gamma(R)$ razcepi v podgrafa X in Y preko vozlišča a tako, da je $|V(X)| > 2$. Če je X poln podgraf, potem je $x^2 = 0$ za vsak $x \in V(X)$.*

Dokaz. Naj bo $x \in V(X) \setminus \{a\}$. Denimo najprej, da je $x^2 = x$. Potem je $x(x-1) = 0$ in zato je $x - 1 \in Z(R) \cap V(X)$. Ker je $|V(X)| > 2$, obstaja $y \in V(X) \setminus \{a, x\}$. Če je $y = x - 1$, je $0 = ay = a(x - 1) = ax - a = -a$, kjer prva in zadnja enakost veljata, ker je $V(X)$ poln podgraf. To implicira, da je $a = 0$, kar ni možno. Sledi, da je $y \neq x - 1$. Zaradi polnosti podgrafa je $0 = y(x - 1) = yx - y = 0 - y = -y$, kar implicira, da je $y = 0$, kar ni možno. Zaključimo, da je $x^2 \neq x$. Za y kot zgoraj zaradi polnosti podgrafa sledi, da je $yx^2 = (yx)x = 0$, torej je $x^2 \in V(X) \cup \{0\}$. Zaradi polnosti podgrafa mora veljati še $x(x^2) = 0$. Ker je $y(x^2+x) = yx^2+yx = 0$, mora biti tudi $x^2+x \in V(X) \cup \{0\}$. Potem velja še $0 = x(x^2+x) = x(x^2)+x^2 = x^2$, kar pomeni, da je $x^2 = 0$. Pokažimo še, da $a^2 = 0$. Ker je $y(a + x) = 0$ zaradi polnosti podgrafa, mora biti $a + x \in V(X) \cup \{0\}$. Ker pa je $a + x \neq a$, iz polnosti podgrafa dobimo še zvezo $0 = a(a+x) = a^2+ax = a^2$, ki pove, da je tudi $a^2 = 0$. ☐

Posledica 7.4. *Naj bo R komutativni enotski kolobar in naj se graf $\Gamma(R)$ razcepi v dva podgrafa X in Y preko vozlišča a, pri čemer je $|V(X)| > 2$. Če je X poln podgraf, je množica $V(X) \cup \{0\}$ ideal.*

Dokaz. Naj bo $x \in V(X) \setminus \{a\}$. Po prejšnji lemi in zaradi polnosti je $xy = 0$ za vse $y \in V(X) \cup \{0\}$. Od tod sledi, da je $x(y_1 + y_2) = 0$ za poljubna $y_1, y_2 \in V(X) \cup \{0\}$, zato je $y_1 + y_2 \in V(X) \cup \{0\}$ za vsaka $y_1, y_2 \in V(X) \cup \{0\}$. Podobno je $x(ry_1) = r(xy_1) = 0$, zato je $ry_1 \in V(X) \cup \{0\}$. $\square$

Lema 7.5. *Naj bo R komutativni enotski kolobar. Če je a prerezno vozlišče grafa $\Gamma(R)$, potem $\mathrm{ann}_R(a)$ ni vsebovan v anihilatorju nobenega drugega neničelnega elementa.*

Dokaz. Denimo nasprotno, da obstaja $x \in R^* \setminus \{a\}$, da je $\mathrm{ann}_R(a) \subseteq \mathrm{ann}_R(x)$. Potem iz $ay = 0$ sledi $xy = 0$. Naj bosta $y, z \in V(\Gamma(R)) \setminus \{a, x\}$. Če je $a - z$ povezava v $\Gamma(R)$, je tudi $x - z$ povezava v $\Gamma(R)$. Če torej obstaja pot $y - a - z$, obstaja tudi pot $y - x - z$. To je v nasprotju s tem, da je a prerezno vozlišče. $\square$

Posledica 7.6. *Naj bo R končni komutativni enotski kolobar, ki ni lokalen. Zapišemo ga lahko kot končni direktni produkt lokalnih kolobarjev (glej* [2, Izrek 8.7]*) in zato lahko elemente pišemo tudi kot n-terice. Če je $a \in \Gamma(R)$ prerezno vozlišče, potem ima $a = (a_1, \ldots, a_n)$ natančno eno neničelno komponento.*

Dokaz. Denimo, da ima več kot eno neničelno komponento. Predpostavimo lahko, da je $a = (a_1, \ldots, a_n)$ prerezno vozlišče in $a_1, a_2 \neq 0$. Potem velja $\mathrm{ann}_R(a) \subsetneq \mathrm{ann}_R((a_1, 0, \ldots, 0))$, kar je v nasprotju z lemo 7.5. $\square$

Posledica 7.7. *Naj bo R končni komutativni enotski kolobar, ki ni lokalen in ni izomorfen kolobarju $\mathbb{Z}_2 \times \mathbb{Z}_2$. Vozlišče $a \in \Gamma(R)$ je prerezno vozlišče, ki ima za edino neničelno komponento obrnljiv element natanko tedaj, ko ima eno samo neničelno komponento in je kolobar, ki mu pripada ta neničelna komponenta izomorfen $\mathbb{Z}_2$.*

Dokaz. Naj bo a prerezno vozlišče grafa $\Gamma(R)$. Predpostavimo lahko, da je $a = (u, 0, \ldots, 0)$, kjer je $u \in U(R_1)$. Če obstaja še nek element $x \in R_1 \setminus \{0, u\}$, potem iz tega, da je u obrnljiv, sledi $\mathrm{ann}_R((u, 0, \ldots, 0)) \subseteq \mathrm{ann}_R((x, 0, \ldots, 0))$, kar je v nasprotju z lemo 7.5. Sledi, da je $R_1 \cong \mathbb{Z}_2$. Dokažimo še obrat. Predpostavimo lahko, da je $R \cong \mathbb{Z}_2 \times S$, kjer je $|S| > 2$ po predpostavki. Potem je $\mathrm{ann}_R((0,1)) = \{(0,0), (1,0)\}$, zato je vozlišče $(0,1)$ povezano le z $(1,0)$. Ker ima kolobar S vsaj dva neničelna elementa, je torej vozlišče $(1,0)$ prerezno vozlišče grafa $\Gamma(R)$. $\square$

Lema 7.8. *Naj bo R končni komutativni enotski kolobar, ki ni izomorfen $\mathbb{Z}_2 \times \mathbb{Z}_2$ in naj bo $a \in Z(R)^*$. Če je $|Z(R)^*| \geq 2$ in a ni prerezno vozlišče grafa $\Gamma(R)$, potem vozlišče $(a, 0)$ ni prerezno vozlišče grafa $\Gamma(R \times S)$, kjer je S poljubni končni komutativni enotski kolobar.*

Dokaz. Po predpostavki vozlišče a ni prerezno vozlišče grafa $\Gamma(R)$. Naj bo $b \in V(\Gamma(R))$ tako vozlišče, ki je povezano z a, torej $ab = 0$ (tak b obstaja, ker $|Z(R)^*| \geq 2$). Potem za vsako vozlišče $v \in V(\Gamma(R)) \setminus \{a, b\}$ obstaja pot od v do b (ker je graf povezan). Od tod sledi, da v grafu $\Gamma(R \times S)$ med poljubnim vozliščem oblike (c, y), kjer je $c \in V(\Gamma(R)) \setminus \{a\}$ in vozliščem oblike (b, x) (lahko je $x = 0$) obstaja pot. Konstruiramo jo lahko kar takole: če pot med c in b v $\Gamma(R)$ ni dolžine 1, potem za vozlišča poti v $\Gamma(R \times S)$ vzamemo kar vozlišča (razen krajišč) poti iz $\Gamma(R)$, ki jim na drugo komponento damo 0. Če pa v $\Gamma(R)$ obstaja povezava $c - b$, pa v $\Gamma(R \times S)$ lahko vzamemo pot $(c, y) - (b, 0) - (c, 0) - (b, x)$.

Poiskali smo torej pot med poljubnima vozliščema oblike (b, x) in (c, y), $b, c \neq a$, ki ne gre preko vozlišča $(a, 0)$. Pokažimo še, da po odstranitvi vozlišča $(a, 0)$ vozlišča oblike $(a, y), y \neq 0$ ostanejo povezana z vozlišči oblike $(d, x), d \neq a$. Ker je vsako vozlišče (a, y) s potjo $(a, y) - (b, 0) - (a, 1)$ povezano z vozliščem $(a, 1)$, zadošča poiskati pot med (b, x) in $(a, 1)$, ki ne gre preko $(a, 0)$.

Če je $x = 0$, je vozlišče (b, x) povezano z vozliščem $(a, 1)$. Predpostavimo sedaj, da je $x \neq 0$. Če je $Z(R)^* \neq \{a, b\}$, potem obstaja $c \in Z(R)^* \setminus \{a, b\}$, da je $bc = 0$ (obstaja, ker a ni prerezno). Potem je $(b, x) - (c, 0) - (b, 0) - (a, 1)$ pot med (b, x) in $(a, 1)$, ki ne obišče $(a, 0)$. Naj bo zdaj še $Z(R)^* = \{a, b\}$. Trdimo, da je iskana pot enaka $(b, x) - (b, 0) - (a, 1)$. Da bo to res pot v grafu, zadošča pokazati, da je $b^2 = 0$. Denimo, da temu ni tako. To pomeni, da je $b^2 \neq 0$, poleg tega pa že vemo, da mora biti $ab = 0$. Pokažimo, da mora biti $b^2 = b$. Denimo, da tudi temu ni tako. Potem je $b^2 = a$ in zato je $b^2 b = ab = 0$. Sledi, da mora biti tudi $b^2(b + b^2) = b^2 b + (b^2 b)b = 0$. Sledi, da je $b^2 + b \in Z(R)$. Velja $b^2 + b \neq b$ (če bi veljala enakost, bi bilo $b^2 = 0$, kar je v nasprotju z našo predpostavko), poleg tega pa velja tudi $b + b^2 \neq a$, saj bi iz te enakosti ob upoštevanju zveze $b^2 = a$ sledilo, da je $b = 0$. Protislovje. Sledi, da je $0 = b^2 + b \neq b$. Potem je $b^2 = b^2 + 0 = b^2 + b^3 = b(b + b^2) = b \cdot 0 = 0$, torej $b^2 = 0$. Protislovje. Sledi, da je res $b^2 = b$. Zapišemo lahko $R = Rb \oplus R(1 - b)$, torej je R izomorfen $R \cong R_1 \times R_2$ za neka kolobarja R_1, R_2. Ker ima R enoto, morata imeti tako R_1 kot R_2 enoto. Potem sta $(1, 0), (0, 1)$ delitelja niča. Po predpostavki ima R samo dva neničelna delitelja niča in zato mora veljati $R \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. To je v nasprotju s predpostavko iz leme. Sledi, da je $b^2 = 0$, zato je zgornja pot dobro definirana. Sklenemo, da $(a, 0)$ ni prerezno vozlišče grafa $\Gamma(R \times S)$. □

Lema 7.9. *Naj bosta R_1 in R_2 končna komutativna enotska kolobarja, pri čemer naj za R_1 velja, da se graf $\Gamma(R_1)$ razcepi v dva podgrafa X in Y preko vozlišča a_1. Potem je $(a_1, 0)$ prerezno vozlišče grafa $\Gamma(R_1 \times R_2)$ natanko tedaj, ko eden izmed podgrafov X in Y po odstranitvi vozlišča a_1 in pripadajočih povezav vsebuje vsaj eno izolirano vozlišče.*

Dokaz. Pokažimo najprej lažjo smer. Naj bo $b \in R_1$ tisto izolirano vozlišče, ki ga dobimo po odstranitvi vozlišča a_1 in pripadajočih povezav. Velja $ba_1 = 0$. Ker je $(a_1 + b)b = b^2$, mora biti $b^2 \neq 0$, saj sicer pridemo navzkriž z izoliranostjo vozlišča b. Sledi, da je $\operatorname{ann}_{R_1}(b) = \{0, a_1\}$ in zato je $\operatorname{ann}_{R_1 \times R_2}((b, 1)) = \{(0, 0), (a_1, 0)\}$. Ker se graf $\Gamma(R_1)$ razcepi v dva podgrafa preko a_1, mora obstajati še neko vozlišče $c \neq 0, a_1$, za katero velja $a_1 c = 0$ in $bc \neq 0$. Sledi, da je $(c, 1)$ sosednje z $(a_1, 0)$, ni pa sosednje z $(b, 1)$. Sledi, da je $(a_1, 0)$ res prerezno vozlišče grafa $\Gamma(R_1 \times R_2)$.

Pokažimo še obrat. Denimo, da po odstranitvi vozlišča a_1 in pripadajočih povezav ne X ne Y ne vsebujeta izoliranega vozlišča. Naj bo $(b, x) \in V(\Gamma(R_1 \times R_2))$ vozlišče, za katerega velja $(a_1, 0) - (b, x) \in E(\Gamma(R_1 \times R_2))$. Podoben premislek kot v dokazu prejšnje leme nam pove, da zadošča poiskati pot v grafu $\Gamma(R_1 \times R_2)$ med vozliščema (b, x) in $(a_1, 1)$, ki ne vsebuje vozlišča $(a_1, 0)$. Če je $b \in \{0, a_1\}$, izberimo poljuben $c \in Z(R_1) \setminus \{a_1, 0\}$ za katerega velja $ca_1 = 0$. Potem je $(b, x) - (c, 0) - (a_1, 1)$ iskana pot v $\Gamma(R_1 \times R_2)$. Obravnavajmo sedaj primer, ko $b \notin \{0, a_1\}$. Potem je $a_1 - b \in E(\Gamma(R_1))$. Ker vozlišče b ne postane izolirano ob odstranitvi vozlišča a_1 in pripadajočih povezav, obstaja $c \in Z(R)^* \setminus \{a_1, b\}$, ki zadošča $bc = 0$. Potem je $(b, x) - (c, 0) - (b, 0) - (a_1, 1)$ iskana pot v $\Gamma(R_1 \times R_2)$. Sklenemo, da $(a_1, 0)$ ni prerezno vozlišče v $\Gamma(R_1 \times R_2)$. S tem je lema dokazana. □

Izrek 7.10. *Naj bo komutativni enotski kolobar $R \cong R_1 \times \cdots \times R_n, n \geq 2$ direktni produkt končnih lokalnih kolobarjev R_i. Če $R \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$, potem je vozlišče $a = (a_1, \ldots, a_n)$ prerezno vozlišče grafa $\Gamma(R)$ natanko tedaj, ko velja ena izmed izjav*

(1) *$a_1 = 1$ in $R_1 \cong \mathbb{Z}_2$,*
(2) *$R_1 \cong \mathbb{Z}_4$ ali $R_1 \cong \mathbb{Z}_2[x]/(x^2)$, kjer je v prvem primeru $a_1 = 2$ in v drugem primeru $a_1 = x$,*

(3) *a_1 je prerezno vozlišče grafa $\Gamma(R_1)$, pri čemer ob odstranitvi a_1 in pripadajočih povezav iz grafa $\Gamma(R_1)$ v tem grafu dobimo vsaj eno izolirano vozlišče.*

Dokaz. Za dokaz moramo le pravilno sestaviti prejšnje leme.

Naj bo $a = (a_1, \ldots, a_n)$ prerezno vozlišče grafa $\Gamma(R)$. Vemo že, da ima le eno neničelno komponento. Predpostavimo lahko, da je to a_1. Če je $a_1 \in U(R_1)$, potem je po posledici 7.7 $R_1 \cong \mathbb{Z}_2$ in $a_1 = 1$. Denimo torej, da $a_1 \notin U(R_1)$. Potem je $a_1 \in Z(R_1)^*$. Po lemi 7.8 je bodisi a_1 prerezno vozlišče grafa $\Gamma(R_1)$ bodisi je $|Z(R_1)^*| < 2$. Ker je a prerezno vozlišče, mora biti $a_1 \neq 0$ in zato $Z(R_1) \neq \{0\}$. Če je torej $|Z(R_1)^*| < 2$, je $\Gamma(R_1)$ graf z enim samim vozliščem, zato je po [1, Primer 2.1(a)] bodisi $R_1 \cong \mathbb{Z}_4$ bodisi $R_1 \cong \mathbb{Z}_2[x]/(x^2)$. Preprost premislek pokaže, da mora biti v prvem primeru $a_1 = 2$ in v drugem $a_1 = x$. Če je a_1 prerezno vozlišče grafa $\Gamma(R_1)$ mora biti po lemi 7.9 tako prerezno vozlišče, da ob odstranitvi vozlišča a_1 in pripadajočih povezav dobimo vsaj eno izolirano vozlišče.

Dokažimo še obrat. Če upoštevamo posledico 7.7 in lemo 7.9, moramo pokazati le še, da iz (2) sledi želeno. Naj bo torej bodisi $R_1 \cong \mathbb{Z}_4$ bodisi $R_1 \cong \mathbb{Z}_2[x]/(x^2)$ in naj bo $a_1 = 2$ ali x. Račun pokaže, da je v obeh primerih $\text{ann}_R((a_1, 1 \ldots, 1)) = \{(0, \ldots, 0), (a_1, 0, \ldots, 0)\}$. Sledi, da je $(a_1, 0, \ldots, 0)$ res prerezno vozlišče grafa $\Gamma(R)$. □

Če je $R_1 \cong \mathbb{Z}_2$ in $S \ncong \mathbb{Z}_2$, potem prerezno vozlišče $(1, 0)$ grafa $\Gamma(R_1 \times S)$ izolira vozlišče $(0, 1)$. Podobno v primeru, ko je $R_1 = \mathbb{Z}_4$ (ali $\mathbb{Z}_2[x]/(x^2)$) velja, da vozlišče $(2, 0)$ (ali vozlišče $(x, 0)$) izolira vozlišče $(2, 1)$ (ali $(x, 1)$) v grafu $\Gamma(\mathbb{Z}_4 \times S)$ (ali v grafu $\mathbb{Z}_2[x]/(x^2) \times S$). To pomeni, da prerezna vozlišča grafa deliteljev niča direktnega produkta vsaj dveh končnih komutativnih enotskih lokalnih kolobarjev vedno izolirajo vozlišča. Zapišemo lahko še posledico.

Posledica 7.11. *Naj bo R končni komutativni enotski kolobar. Če graf deliteljev niča $\Gamma(R)$ vsebuje prerezno vozlišče in ob njegovi odstranitvi ne dobimo izoliranih vozlišč, je R lokalni kolobar.*

Dokaz. Sledi iz premisleka pred formulacijo posledice. □

Če je R komutativni enotski lokalni kolobar in m njegov edini maksimalni ideal, potem že vemo, da je m nilpotenten. Označimo torej s k najmanjše naravno število, za katero velja $m^k = 0$ in $m^{k-1} \neq 0$.

Lema 7.12. *Naj bo R končni komutativni lokalni enotski kolobar z maksimalnim idealom m in naj bo x prerezno vozlišče grafa $\Gamma(R)$. Potem je $m^{k-1} = \{x, 0\}$.*

Dokaz. Denimo, da $x \notin m^{k-1}$. Ker je k tako naravno število, da $m^{k-1} \neq 0$, obstaja $0 \neq r \in m^{k-1}$. Potem za vsak $a \in Z(R) = m$ velja $ar = 0$ (sicer je $0 \neq ar \in m^k$, kar je v nasprotju z izbiro števila k). To pa pomeni, da je povezava $ar \in E(\Gamma(R))$ za vsak $a \in Z(R) \setminus \{0, r\}$. Sledi, da je r povezan z vsemi vozlišči $\Gamma(R)$, kar je v nasprotju s tem, da je x prerezno vozlišče $\Gamma(R)$. Sledi torej, da je $x \in m^{k-1}$. Pokazati moramo še, da je to edini neničelni element v m^{k-1}. Denimo nasprotno, da obstaja še $r \in m^{k-1} \setminus \{0, x\}$. Iz enakega razloga kot zgoraj mora spet veljati, da je $ra = 0$ za vsak $a \in Z(R)$ in posledično spet pridemo v protislovje s tem, da je x prerezno vozlišče. Sklenemo, da tak r ne more obstajati in zato je $m^{k-1} = \{0, x\}$. □

Iz zgornje leme pa takoj sledi naslednja posledica.

Posledica 7.13. *Naj bo R končni komutativni lokalni enotski kolobar. Naj ima graf $\Gamma(R)$ prerezno vozlišče. Potem je $|R| = 2^k, k \in \mathbb{N}$.*

Lema 7.14. *Naj bo R komutativni enotski kolobar. Če je x prerezno vozlišče grafa $\Gamma(R)$, potem je x v centru $\Gamma(R)$.*

Dokaz. Vemo že, da je polmer grafa $\Gamma(R)$ največ 2. Če je polmer grafa $\Gamma(R)$ enak 0, ima graf eno samo vozlišče, ki je očitno v centru. Denimo, da ima graf polmer enak 1. Potem ima graf vsaj eno vozlišče y sosedno vsem ostalim vozliščem. Po definiciji so v centru vozlišča, katerih ekscentričnost je enaka 1, to pa pomeni, da so sosednja z vsemi ostalimi vozlišči. Naj bo zdaj x prerezno vozlišče. Potem mora biti x povezan z vsemi vozlišči, saj sta sicer poljubni dve vozlišči v grafu $\Gamma(R) \setminus \{x\}$ povezani preko poti, ki gre skozi center grafa. Ker mora biti x povezan z vsemi vozlišči, je njegova ekscentričnost 1 in je zato v centru grafa.

Naj bo zdaj polmer grafa enak 2. Denimo, da je x prerezno vozlišče grafa $\Gamma(R)$ in da ni v centru. To pomeni, da je njegova ekscentričnost $e(x) > 2$. Po [16, Izrek 3.8] vemo, da je premer grafa $\Gamma(R)$ največ 3. To pomeni, da obstaja vozlišče z, da je $d(x, z) = 3$. Ker je x prerezno vozlišče, je graf $\Gamma(R) \setminus \{x\}$ nepovezan. Denimo, da je sestavljen iz disjunktnih podgrafov X in Y (zagotovo ima vsaj dve neprazni komponenti). Predpostavimo lahko, da je vozlišče z v komponenti X, sicer preimenujemo komponente. Izberimo sedaj še vozlišče y iz komponente Y. Ker je x prerezno vozlišče, mora vsaka pot od y do z iti preko x. To pomeni, da je $d(y, z) = d(x, y) + d(x, z) \geq 1 + 3 = 4$. Protislovje. □

Lema 7.15. *Naj bo R komutativni enotski kolobar. Naj bo $x \in V(\Gamma(R))$ prerezno vozlišče in naj se $\Gamma(R) \setminus \{x\}$ razcepi v dva podgrafa X in Y. Potem je bodisi $d(x, z) = 1$ za vsak $z \in V(X)$ bodisi $d(x, y) = 1$ z vsak $y \in Y$.*

Dokaz. Denimo nasprotno, da obstajata $z \in V(X)$ in $y \in V(Y)$, da velja $d(x, z) \geq 2$ in $d(x, y) \geq 2$. Ker je x prerezno vozlišče, gre vsaka pot med z in y čez vozlišče x. Potem velja $d(z, y) = d(x, z) + d(x, y) \geq 2 + 2 = 4$. To je v nasprotju s tem, da je premer manjši ali enak 3 ([16, Izrek 3.8]). □

Naslednji izrek nam poda karakterizacijo grafov deliteljev niča s prereznimi vozlišči. Izkaže se, da mora imeti tak graf vozlišče stopnje 1, razen v primeru sedmih kolobarjev, ki so izjeme.

Izrek 7.16. *Naj bo R tak končni komutativni enotski kolobar, da ima graf $\Gamma(R)$ vsaj tri vozlišča. Potem ima graf $\Gamma(R)$ prerezno vozlišče natanko tedaj, ko ima vozlišče stopnje 1 ali pa je R izomorfen enemu izmed naslednjih sedmih kolobarjev*

$$\mathbb{Z}_4[x, y]/(x^2, y^2, xy - 2, 2x, 2y), \mathbb{Z}_2[x, y]/(x^2, y^2), \mathbb{Z}_4[x]/(x^2),$$
$$\mathbb{Z}_4[x]/(x^2 + 2x), \mathbb{Z}_8[x]/(2x, x^2 + 4), \mathbb{Z}_2[x, y]/(x^2, y^2 - xy),$$
$$\mathbb{Z}_4[x, y]/(x^2, y^2 - xy, xy - 2, 2x, 2y).$$

Dokaz. Pokažimo najprej lažjo smer. Če ima graf vozlišče x stopnje 1, potem je edino vozlišče sosednje z x prerezno vozlišče. Pogoj, da ima graf vsaj tri vozlišča nam zagotovlja, da je graf brez edinega soseda vozlišča x res razpadel na vsaj dve komponenti. V primeru sedmih naštetih kolobarjev se z lahkoto preveri, da imajo prerezna vozlišča. Vsi imajo po sedem neničelnih deliteljev niča. Zapišimo jih

- $Z(\mathbb{Z}_4[x, y]/(x^2, y^2, xy - 2, 2x, 2y)) = \{2, x, 2 + x, y, 2 + y, x + y, 2 + x + y\}$, prerezno vozlišče 2,
- $Z(\mathbb{Z}_2[x, y]/(x^2, y^2)) = \{xy, x, x + xy, y, y + xy, x + y, x + y + xy\}$, prerezno vozlišče xy,
- $Z(\mathbb{Z}_4[x]/(x^2)) = \{2x, 3x, x, 2x + 2, 2, 2 + x, 3x + 2\}$, prerezno vozlišče $2x$,

- $Z(\mathbb{Z}_4[x]/(x^2+2x)) = \{2x, 2, 2+2x, x, 2+3x, 3x, 2+x\}$, prerezno vozlišče $2x$,
- $Z(\mathbb{Z}_8[x]/(2x, x^2+4)) = \{4, 2+x, 6+x, 2, x, 6, 4+x\}$, prerezno vozlišče 4,
- $Z(\mathbb{Z}_2[x,y]/(x^2, y^2-xy)) = \{xy, x, x+xy, y, x+y, y+xy, x+y+xy\}$, prerezno vozlišče xy,
- $Z(\mathbb{Z}_4[x,y]/(x^2, y^2-xy, xy-2, 2x, 2y)) = \{2, x, 2+x, y, 2+x+y, 2+y, x+y\}$, prerezno vozlišče 2.

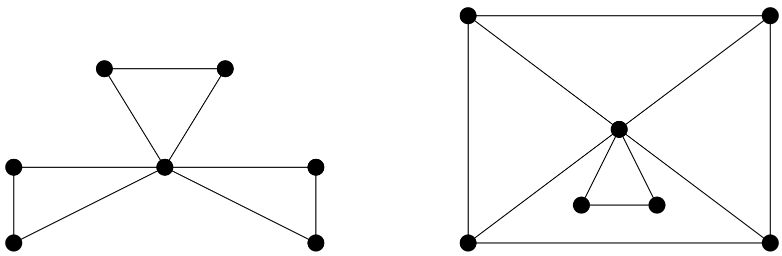
Pri tem imajo prvi trije zgoraj našteti kolobarji

$$\mathbb{Z}_4[x,y]/(x^2, y^2, xy-2, 2x, 2y), \mathbb{Z}_2[x,y]/(x^2, y^2), \mathbb{Z}_4[x]/(x^2)$$

graf tipa 1 (slika 1), zadnji štirje kolobarji

$$\mathbb{Z}_4[x]/(x^2+2x), \mathbb{Z}_8[x]/(2x, x^2+4), \mathbb{Z}_2[x,y]/(x^2, y^2-xy),$$
$$\mathbb{Z}_4[x,y]/(x^2, y^2-xy, xy-2, 2x, 2y)$$

pa graf tipa 2 (slika 1). Delitelji niča so zgoraj navedeni tako, da je pri kolobarjih tipa 1 najprej navedeno sredinsko prerezno vozlišče, potem pa so zaporedoma v parih, ki nastopajo na istih trikotnikih, navedena zunanja vozlišča. Pri grafih tipa 2 je prav tako najprej navedeno sredinsko prerezno vozlišče, potem sta navedeni notranji vozlišči, ki nastopata na malem trikotniku, nazadnje pa so zaporedoma navedena še zunanja vozlišča.



Slika 1. Levo: graf tipa 1, desno: graf tipa 2.

Dokažimo še obrat. Naj ima graf $\Gamma(R)$ prerezno vozlišče a. Denimo najprej, da R ni lokalni kolobar. Potem po [2, Izrek 8.7] R lahko zapišemo kot $R = R_1 \times \cdots \times R_n$, kjer je $n \geq 2$ in so vsi R_i končni lokalni kolobarji. Po posledici 7.6 in izreku 7.10 sledi, da je $a = (a_1, 0, \ldots, 0)$, kjer velja ena od naslednjih možnosti

(1) $a_1 = 1$ in $R_1 \cong \mathbb{Z}_2$,
(2) $R_1 \cong \mathbb{Z}_4$ in $a_1 = 2$ ali $R_1 \cong \mathbb{Z}_2[x]/(x^2)$ in $a_1 = x$,
(3) a_1 je prerezno vozlišče v $\Gamma(R_1)$, ki ob odstranitvi izolira vsaj eno vozlišče.

Opazimo, da v vsakem izmed zgornjih treh primerov lahko v $\Gamma(R)$ najdemo vozlišče stopnje 1 in sicer

(1) $(0, 1, \ldots, 1)$,
(2) $(2, 1, \ldots, 1)$ ali $(x, 1, \ldots, 1)$,
(3) $(b, 1, \ldots, 1)$, kjer je $b \in V(\Gamma(R_1))$ vozlišče stopnje ena,

s čimer dokaz v primeru kolobarja, ki ni lokalen, lahko zaključimo.

Predpostavimo sedaj, da je R lokalni kolobar. Označimo z m njegov edini maksimalni ideal in s k najmanjše tako naravno število, da je $m^k = 0$. Zaradi leme 7.12 vemo, da je $m^{k-1} = \{a, 0\}$. Ker je $m = Z(R)$, je a soseden z vsemi drugimi vozlišči $\Gamma(R)$ in $2a = 0$. Ker je a prerezno vozlišče, po njegovi odstranitvi graf $\Gamma(R)$ razpade na $n \geq 2$ komponent. Označimo jih z $G_1, \ldots, G_n$. Če je v eni izmed komponent eno samo vozlišče, smo našli vozlišče stopnje ena in smo s tem izrek dokazali. Predpostavimo torej, da ima vsaka komponenta G_i vsaj dve vozlišči. Naj bo zdaj $i \neq j$ in $x \in G_i, y \in G_j$. Potem je $xy \neq 0$, ker sta iz različnih komponent in $xy \in Z(R)$. Ker so vse komponente G_k po predpostavki povezane in imajo vsaj dve vozlišči, obstajata $s \in G_i \setminus \{x\}$, za katerega velja $sx = 0$ in $t \in G_j \setminus \{y\}$, za katerega velja $ty = 0$. Potem je $s - xy - t$ pot med s in t v $\Gamma(R)$ (to velja tudi, če je $xy = s$ ali $xy = t$). Sledi $xy = a$, saj sicer pridemo v nasprotje s tem, da je a prerezno vozlišče. Sklenemo, da za poljubna $i \neq j$ in za poljubna $x \in G_i, y \in G_j$ velja $xy = a$.

Naj bo zdaj $y \in G_j$ in naj bo $t \in G_j \setminus \{y\}$ tak, da je $ty = 0$. Potem je za vsak $k \in \mathbb{N}$ tudi $ty^k = 0$. Zato je $y^k \in G_j \cup \{0, a\}$, saj je t povezan le z elementi iz $G_j \cup \{a\}$. Naj bo zdaj $i \neq j$ in $x \in G_i$. Potem je po zgoraj ugotovljenem $xy = a$ in zato $xy^2 = ay = 0$. Če je $y^2 \in G_j$, smo prišli do protislovja s tem, da sta G_i in G_j različni komponenti. Zato je $y^2 \in \{0, a\}$. Denimo, da je $y^2 = a$. Potem je $y^3 = y^2 y = ay = 0$. Sledi, da za vsak $z \in Z(R)$ velja $z^3 = 0$. Velja še $y(y - x) = y^2 - xy = a - a = 0$ in zato je $y - x \in V(G_j)$. Sledi $a = x(y - x) = xy - x^2 = a - x^2$, zato je $x^2 = 0$ za vsak $x \in G_i, i \neq j$. Ugotovili smo, da je $z^2 = 0$ za vsak $z \in Z(R)$ ali pa obstaja natanko ena komponenta G_j (predpostavimo lahko, da je to G_1), da je $y^3 = 0$ za vsak $y \in G_1$ in za vsak $i \neq 1$ je $x^2 = 0$ za vsak $x \in G_i$. Vemo še, da je $2a = 0$. Od tod sledi, da bo karakteristika R sodo število. Ker je R lokalni kolobar, bo karakteristika R oblike $2^k, k \geq 1$. Če je $k > 1$, potem je $2 \in Z(R)$ in mora veljati bodisi $2^2 = 0$ bodisi $2^3 = 0$. Zaključimo, da je karakteristika R enaka 2,4 ali 8. Prav tako iz zgornjega sledi še, da je v primeru, ko je karakteristika enaka 8, element a enak $a = 2^2 = 4$ (za 2 namreč velja, da je $2^2 \neq 0$).

Naj bo $y \in G_1$ in $t \in G_1 \setminus \{y\}$ tak element, da zanj velja $yt = 0$. Naj bo $i \neq 1$ in $x \in G_i$ za $i > 1$. Denimo, da je $|G_i| \geq 3$. Poglejmo si element $x + a$. Velja $x(x+a) = x^2 + xa = 0 + 0 = 0$, torej mora biti $x + a \in G_i$. Vzemimo sedaj poljuben element $z \in G_i$, ki je soseden z $x + a$. Potem je $0 = z(x+a) = zx + za = zx$ in zato je z povezan tudi z x. Ker je komponenta G_i povezana in ima vsaj tri vozlišča, obstaja $v \in G_i \setminus \{x, x + a\}$, ki zadošča $xv = 0$. Potem je $x(x + v) = x^2 + xv = 0 + 0 = 0$ in $y(x + v) = yx + yv = a + a = 2a = 0$. Sledi, da je element $x + v$ bodisi enak 0 bodisi a, saj je sicer povezan z elementom iz G_1 in z elementom iz G_i, kar je v nasprotju z definicijo komponent za povezanost. Denimo najprej, da je $2x = 0$. Če je $x + v = 0$, potem je $v = -x = x$, kar je v nasprotju z izbiro v (zadnja enakost sledi, ker je $x = -x$). Podobno je v primeru, ko je $x + v = a$, $v = a - x = a + x$, kar je spet v nasprotju z izbiro v. Naj bo $2x \neq 0$. Velja $(2x)x = 2x^2 = 0$, torej je $2x \in G_i \cup \{a\}$. Ker pa je $(2x)y = 2(xy) = 0$, mora biti $2x = a$. Če je zdaj $x + v = a = 2x$, je $v = x$, kar je v nasprotju z izbiro v. Sledi, da je $x + v = 0$ oziroma $v = -x$. Če je karakteristika R enaka 4, je $v = -x = 3x = x + 2x = x + a$. Protislovje. Denimo, da je karakteristika R enaka 8. Po predpostavki je $v \neq x + a = x + 2x = 3x$. Od tod sledi, da je $x + v \neq x + 3x = 4x = ax = 0$. Protislovje z zgornjo predpostavko. Sklenemo, da mora za vsak $i \neq 1$ veljati $|G_i| = 2$.

Sedaj ločimo dva primera. Denimo najprej, da obstaja $y \in G_1$, ki zadošča $y^2 \neq 0$. Po zgoraj ugotovljenem mora veljati $y^2 = a$ in $y^3 = 0$. Naj bo zdaj $x \in G_2$. Potem je $y(x + y) = xy + y^2 = a + a = 2a = 0$, torej je $x + y \in G_1$. Denimo, da je $n \geq 3$, torej imamo po odstranitvi elementa a vsaj tri komponente za povezanost. Naj bo $z \in G_3$. Potem je $z(x + y) = zx + zy = a + a = 2a = 0$. Sledi, da mora biti $z \in G_1$, kar je v nasprotju z izbiro elementa z. Zaključimo, da mora biti $n = 2$. To pa pomeni, da je $V(\Gamma(R)) = V(G_1) \cup V(G_2) \cup \{a\}$. Poleg tega smo zgoraj že ugotovili, da je $|G_2| = 2$ in ker je $x(x+a) = x^2 + xa = 0 + 0 = 0$, je $G_2 = \{x, x+a\}$. Podobno se enostavno prepričamo, da je $\{y, x+y, y+a, x+y+a\} \subseteq G_1$.

Recimo, da je $|G_1| \geq 5$. Potem enako kot zgoraj vidimo, da obstaja $s \in G_1 \setminus \{y, x+y, y+a, x+y+a\}$, ki zadošča bodisi $sy = 0$ bodisi $s(x+y) = 0$. Poglejmo si najprej drugi primer, ko je $s(x+y) = 0$. Potem je $0 = s(x+y) = sx + sy = a + sy$. Ker je $2a = 0$, je $a = sy$. Poleg tega $x(s+y) = xs + xy = a + a = 2a = 0$ in $y(y+s) = y^2 + ys = a + a = 2a = 0$. Sledi, da je $y + s$ bodisi 0 bodisi a, saj sicer pridemo v nasprotje z razcepom na komponente. Sedaj naredimo analogen premislek kot zgoraj. Če je $2y = 0$, potem iz $s + y = 0$ dobimo $s = y$ in iz $s + y = a$ dobimo $s = y + a$. Protislovje v obeh primerih. Naj bo $2y \neq 0$. Ker je $(2y)x = 2(xy) = 2a = 0$ in $2y(x+y) = 2(xy + y^2) = 2(a+a) = 0$, mora biti $2y = a$. Če je $y+s = a = 2y$, je $s = y$. Protislovje. Če je $y+s = 0$ in je R karakteristike 4, je $s = -y = 3y = y+2y = y+a$. Protislovje. Če pa je $y+s = 0$ in je karakteristika R enaka 8, iz zveze $s \neq y+a = y+2y = 3y$ dobimo $y+s \neq 4y = ay = 0$. Protislovje. Sklenemo, da ne more veljati $s(x+y) = 0$.

Poglejmo si sedaj primer, ko je $sy = 0$. Potem je $y(x+y+s) = yx + y^2 + ys = a + a + 0 = 2a = 0$ in $x(x+y+s) = x^2 + xy + xs = 0 + a + a = 2a = 0$. Sledi $x + y + s \in \{0, a\}$. Analogno kot v prvem primeru pokažemo, da se to ne more zgoditi. V vseh primerih torej pridemo do protislovja, zato mora biti $|G_1| = 4$. Sledi, da je $G_1 = \{y, x+y, y+a, x+y+a\}$. Pri tem je y povezan z elementi iz množice $\{x+y, x+y+a, a\}$, $x+y$ je povezan z elementi iz $\{y, y+a, a\}$, $y+a$ je povezan z elementi iz $\{x+y, x+y+a, a\}$, $x+y+a$ pa je povezan z elementi iz $\{y, y+a, a\}$. Iz pravkar povedanega in iz zgoraj dokazanega sledi, da je graf $\Gamma(R)$ ravno graf tipa 2 s slike 1 (pri tem je $x + a \in G_2$ povezan z a, ker je $a^2 = 0$, kar sledi iz tega, da je $m^{k-1} = \{0, a\}$ in $m^k = 0$). V [19, Slika 6] so bili natančno določeni kolobarji, ki imajo tak graf deliteljev niča. Izkaže se, da mora biti R izomorfen enemu od kolobarjev $\mathbb{Z}_4[x]/(x^2+2x), \mathbb{Z}_8[x]/(2x, x^2+4), \mathbb{Z}_2[x,y]/(x^2, y^2 - xy), \mathbb{Z}_4[x,y]/(x^2, y^2 - xy, xy - 2, 2x, 2y)$.

Ostane nam torej le še primer, ko za vsak $x \in Z(R)$ velja $x^2 = 0$. Vemo že, da je $V(\Gamma(R)) = V(G_1) \cup V(G_2) \cup \cdots \cup V(G_n) \cup \{a\}$, kjer ima vsaka komponenta G_i dve vozlišči. Označimo $V(G_i) = \{x_i, x_i + a\}$. Denimo najprej, da je $n \geq 4$. Naj bo $y \in G_1$ in $x \in G_2$. Potem velja $x + y \notin G_1 \cup G_2 \cup \{a\}$. Denimo nasprotno, da je $x + y \in G_1$. Če je $x + y = y$, je $x = 0$, kar je v nasprotju z definicijo grafa deliteljev niča. Če pa je $x + y = y + a$, je $x = a$, kar je spet v nasprotju s tem, da je $G_2 = \{x, x+a\}$. Analogno vidimo, da $x + y \notin G_2$. Če pa je $x + y = a$, je $0 = xa = x(x+y) = x^2 + xy = 0 + a = a$. Protislovje. Predpostavimo torej lahko, da je $x + y \in G_3$. Naj bo še $z \in G_4$. Potem je $z(x+y) = zx + zy = a + a = 2a = 0$, torej mora biti še $z \in G_3$. Protislovje. Sledi, da je $n \leq 3$. Vemo, da $n \neq 1$, sicer a ne bi bilo prerezno vozlišče. Če je $n = 2$, potem ima $\Gamma(R)$ 5 vozlišč. V [19, tabela za $n = 5$] so klasificirani vsi grafi deliteljev niča na 5 vozliščih, vendar noben izmed njih nima želene oblike (noben nima prereznega vozlišča za katerega velja, da ob njegovi odstranitvi dobimo dva grafa K_2). Zaključimo, da mora biti $n = 3$ in $V(\Gamma(R)) = V(G_1) \cup V(G_2) \cup V(G_3) \cup \{a\}$. Pri tem imajo vse tri komponente G_i po dve vozlišči. Zaključimo torej, da je graf $\Gamma(R)$ ravno graf tipa 1 s slike 1. V [19, Slika 7] najdemo, da mora biti R izomorfen enemu izmed kolobarjev $\mathbb{Z}_4[x,y]/(x^2, y^2, xy - 2, 2x, 2y), \mathbb{Z}_2[x,y]/(x^2, y^2), \mathbb{Z}_4[x]/(x^2)$. S tem je ta izrek dokazan. $\square$

8. Vozlišča stopnje 1

Lema 8.1. *Naj bo R končni komutativni enotski kolobar, ki ni izomorfen $\mathbb{Z}_4$ ali $\mathbb{Z}_2[x]/(x^2)$. Graf $\Gamma(R)$ ima vozlišče stopnje 1 natanko tedaj, ko je bodisi R izomorfen $\mathbb{Z}_9$ ali $\mathbb{Z}_3[x]/(x^2)$ bodisi v R obstaja element x, za katerega velja $|\operatorname{ann}_R(x)| = 2$.*

Dokaz. Če je R izomorfen $\mathbb{Z}_9$ ali $\mathbb{Z}_3[x]/(x^2)$, potem je graf $\Gamma(R)$ izomorfen K_2. Ta očitno ima vozlišče stopnje 1. Naj bo zdaj R tak, da obstaja element x, za katerega velja, da je $|\operatorname{ann}_R(x)| = 2$. To pomeni, da je poleg 0 v $\operatorname{ann}_R(x)$ še en neničelen element. Če je ta različen od x, potem ima x enega samega soseda in je zato $\deg(x) = 1$. Če pa je $\operatorname{ann}_R(x) = \{0, x\}$, potem mora biti zaradi povezanosti grafa $\Gamma(R)$ ta enak kar grafu K_1, kar pomeni, da imamo eno samo vozlišče in nobene povezave. Po [1, Primer 2.1(a)] je v tem primeru R izomorfen kolobarju $\mathbb{Z}_4$ ali $\mathbb{Z}_2[x]/(x^2)$, kar pa je v nasprotju s predpostavko leme.

Dokažimo še obrat. Denimo, da ima $\Gamma(R)$ vozlišče x, ki zadošča $\deg(x) = 1$. Naj ima najprej $\Gamma(R)$ le dve vozlišči. Potem je $\Gamma(R)$ izomorfen grafu K_2. Po [1, Primer 2.1(a)] je potem R izomorfen enemu izmed kolobarjev $\mathbb{Z}_9, \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_3[x]/(x^2)$. Opazimo, da je $\operatorname{ann}_{\mathbb{Z}_2\times\mathbb{Z}_2}((1,0)) = \{(0,0),(0,1)\}$, torej je $|\operatorname{ann}_{\mathbb{Z}_2\times\mathbb{Z}_2}((1,0))| = 2$. Podobno je $|\operatorname{ann}_{\mathbb{Z}_2\times\mathbb{Z}_2}((0,1))| = 2$. Poglejmo si še primer, ko ima $\Gamma(R)$ vsaj tri vozlišča. Potem je jasno, da je edini sosed vozlišča x prerezno vozlišče. Označimo ga z a. Velja bodisi $\operatorname{ann}_R(x) = \{0, a\}$ bodisi $\operatorname{ann}_R(x) = \{0, a, x\}$. V drugem primeru je potem $x^2 = 0$. Od tod sledi, da je $x(x + a) = x^2 + xa = 0 + 0 = 0$ in zato je $x + a \in \operatorname{ann}_R(x) = \{0, a, x\}$. Če je $x + a = x$, je $a = 0$. Protislovje. Podobno dobimo, da $x + a \neq a$. Sledi torej, da je $x + a = 0$ oziroma $x = -a$. Ker je vsak sosed vozlišča a tudi sosed vozlišča $-a = x$, mora biti $\Gamma(R)$ izomorfen grafu K_2 (ker x soseden le z a). To pa je v nasprotju s tem, da ima graf vsaj tri vozlišča. □

Združimo to lemo z ugotovitvami prejšnjega razdelka.

Posledica 8.2. *Naj bo R tak končni komutativni enotski kolobar, da ima $\Gamma(R)$ vsaj tri vozlišča. Graf $\Gamma(R)$ ima prerezno vozlišče natanko tedaj, ko je izpolnjen eden izmed naslednjih dveh pogojev*

(1) *obstaja $x \in R$, da je $|\operatorname{ann}_R(x)| = 2$ ali*
(2) *R je izomorfen enemu izmed naslednjih sedmih kolobarjev: $\mathbb{Z}_4[x,y]/(x^2, y^2, xy-2, 2x, 2y), \mathbb{Z}_2[x,y]/(x^2,y^2), \mathbb{Z}_4[x]/(x^2), \mathbb{Z}_4[x]/(x^2+2x), \mathbb{Z}_8[x]/(2x, x^2+4), \mathbb{Z}_2[x,y]/(x^2, y^2-xy), \mathbb{Z}_4[x,y]/(x^2, y^2-xy, xy-2, 2x, 2y)$.*

Dokaz. Sledi direktno iz izreka 7.16 in leme 8.1. □

Lema 8.3. *Naj bo R končni komutativni enotski kolobar. Prerezna vozlišča grafa $\Gamma(R)$ tvorijo poln podgraf grafa $\Gamma(R)$.*

Dokaz. Smiselno je gledati le kolobarje, katerih grafi imajo vsaj dve prerezni vozlišči. Pripomnimo, da imajo po lemi 7.12 lokalni kolobarji kvečjemu eno prerezno vozlišče in zato za njih trditev očitno velja.

Naj bo torej R tak kolobar, da ima graf $\Gamma(R)$ vsaj dve prerezni vozlišči. Označimo ju z a in b. Potem graf $\Gamma(R)$ ob odstranitvi vozlišča a razpade na dva disjunktna podgrafa G_1 in G_2. Predpostavimo lahko, da je $b \in G_2$. Naj bo $x_a \in G_1$ sosed vozlišča a v $\Gamma(R)$. Analogno graf $\Gamma(R)$ ob odstranitvi vozlišča b razpade na dva disjunktna podgrafa H_1 in H_2. Spet lahko predpostavimo, da je $a \in H_2$ in izberemo $x_b \in H_1$, ki je soseden z a v $\Gamma(R)$. Poglejmo si zdaj najkrajšo pot med x_a in x_b v $\Gamma(R)$. Če ta pot ne vsebuje vozlišča a, jo lahko podaljšamo s povezavo $x_b - b$ in tako dobimo pot med x_a in b, ki ne obišče vozlišča a. To je v nasprotju s tem, da je a prerezno vozlišče in da sta podgrafa G_1 in G_2 disjunktna. Podobno vidimo še, da mora ta pot vsebovati tudi vozlišče b. Sklenemo torej, da sta tako a kot b na najkrajši poti med vozliščema x_a in x_b. Po [16, Izrek 3.8] je $\text{dist}(x_a, x_b) \leq 3$, zato mora biti najkrajša pot med njima oblike $x_a - a - b - x_b$. To pomeni, da morata biti a in b povezana. Ker sta bili prerezni vozlišči poljubni, sledi, da prerezna vozlišča tvorijo poln podgraf. □

Lema 8.4. *Naj bo R končni komutativni enotski kolobar. Označimo z N število prereznih vozlišč grafa $\Gamma(R)$. Velja $0 \leq N \leq |V(\Gamma(R))|/2$ in obe meji sta lahko doseženi.*

Dokaz. Jasno je, da je $N \geq 0$. Poleg tega obstajajo grafi deliteljev niča, ki nimajo prereznih vozlišč. Vzamemo lahko na primer $R = \mathbb{F}_m \times \mathbb{F}_n$, kjer je $\mathbb{F}_i$ polje z i elementi in sta $m, n \geq 3$. Velja namreč $\Gamma(\mathbb{F}_m \times \mathbb{F}_n) = K_{m-1,n-1}$. Prav tako obstaja kolobar, pri katerem je dosežena zgornja meja iz izreka. Res, vzemimo $R = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Graf $\Gamma(R)$ je tak kot K_3, le da ima iz vsakega vozlišča še eno povezavo. V tem primeru je torej $|V(\Gamma(R))| = 6$, poleg tega pa ima tri prerezna vozlišča. Preveriti je torej potrebno le še, da za vsak graf deliteljev niča res velja zgornja meja iz izreka. Predpostavimo torej, da je R tak, da ima graf $\Gamma(R)$ prerezno vozlišče. Potem je po izreku 7.16 kolobar R bodisi izomorfen enemu izmed sedmih v izreku naštetih kolobarjev bodisi ima $\Gamma(R)$ vozlišče stopnje 1. Vemo že, da ima vsak od sedmih omenjenih kolobarjev bodisi graf tipa 1 bodisi graf tipa 2 s slike 1. Potem ima očitno sedem vozlišč in le eno prerezno vozlišče in zadošča oceni iz leme. Prav tako vemo, da imajo grafi deliteljev niča lokalnih kolobarjev kvečjemu eno prerezno vozlišče in tudi zanje trditev očitno velja. Naj bo torej R kolobar, ki ni izomorfen nobenemu od sedmih kolobarjev iz izreka 7.16 in ni lokalen. Iz izreka 7.10 sledi, da vsako prerezno vozlišče ob odstranitvi izolira vsaj eno vozlišče. To pomeni, da za vsako prerezno vozlišče obstaja vsaj eno vozlišče stopnje 1. Od tod sledi $2N \leq |V(\Gamma(R))|$ oziroma $N \leq |V(\Gamma(R))|/2$. □

9. Uravnoteženi usmerjeni grafi deliteljev niča matričnih kolobarjev

Definirajmo usmerjeni graf deliteljev niča. Naj bo R nekomutativni kolobar in naj bo $Z(R)^*$ množica neničelnih deliteljev niča (tako enostranskih kot dvostranskih) kolobarja R. *Usmerjeni graf deliteljev niča* kolobarja R je usmerjeni graf, ki ima za vozlišča elemente množice $Z(R)^*$. Pri tem obstaja usmerjena povezava $x \to y$ med različnima vozliščema $x \neq y$ natanko tedaj, ko je $xy = 0$. Označimo ga z $\Gamma_d(R)$.

Definirajmo še nekaj pojmov, povezanih z vozlišči usmerjenega grafa. Naj bo $a \in V(\Gamma_d(R))$ poljubno vozlišče. Število povezav oblike $x \to a$ imenujemo *vhodna stopnja* vozlišča a, število povezav oblike $a \to x$ pa *izhodna stopnja* vozlišča a. Če graf ni usmerjen, je jasno, da oba pravkar definirana pojma sovpadata s stopnjo vozlišča. Pravimo, da je graf *uravnotežen*, če za vsako vozlišče grafa njegova vhodna in izhodna stopnja sovpadata.

Če je kolobar R končen, z lahkoto določimo vhodno in izhodno stopnjo poljubnega vozlišča. Naj bo a vozlišče grafa $\Gamma_d(R)$. Potem je vhodna stopnja a enaka $|l_R(a)| - 1$, če $a^2 \neq 0$ in $|l_R(a)| - 2$, če $a^2 = 0$. Podobno je izhodna stopnja a enaka $|r_R(a)| - 1$, če $a^2 \neq 0$ in $|r_R(a)| - 2$, če $a^2 = 0$.

Izrek 9.1. *Naj bo R komutativni končni enotski glavni kolobar in $n \geq 2$. Naj bo $A \in \mathbb{M}_n(R)$ neničelni delitelj niča in naj bodo $d_1, d_2, \ldots, d_n$ osnovni delitelji matrike A. Potem sta tako vhodna kot izhodna stopnja vozlišča A v $\Gamma_d(\mathbb{M}_n(R))$ enaki*

$$\prod_{i=1}^{n} |\operatorname{ann}_R(d_i)|^n - \epsilon,$$

stopnja vozlišča A v $\Gamma(\mathbb{M}_n(R))$ pa je enaka

$$2\prod_{i=1}^{n} |\operatorname{ann}_R(d_i)|^n - \prod_{i,j=1}^{n} |\operatorname{ann}_R(d_i) \cap \operatorname{ann}_R(d_j)| - \epsilon,$$

kjer je $\epsilon = 1$, razen v primeru, ko je $A^2 = 0$. Tedaj je $\epsilon = 2$. Zgornja ugotovitev o vhodni in izhodni stopnji implicira, da je graf $\Gamma_d(\mathbb{M}_n(R))$ uravnotežen.

Dokaz. Po izreku 6.2 vemo, da je vsak komutativni enotski glavni kolobar osnovni kolobar z deljenjem. To pomeni, da je matrika A ekvivalentna matriki $D_A = \operatorname{diag}(d_1, \ldots, d_n)$. Iz leme 4.11 sledi, da je $|l_{\mathbb{M}_n(R)}(A)| = |l_{\mathbb{M}_n(R)}(D_A)|$ in $|r_{\mathbb{M}_n(R)}(A)| = |r_{\mathbb{M}_n(R)}(D_A)|$. Naj bo $X = (x_{ij})_{i,j=1}^n \in \mathbb{M}_n(R)$ poljubna matrika. Potem velja, da je $XD_A = 0$ natanko tedaj, ko je $x_{ij}d_j = 0$ za $i, j = 1, \ldots, n$. Podobno je $D_A X = 0$ natanko tedaj, ko je $d_i x_{ij} = 0$ za $i, j = 1, \ldots, n$. Sledi, da je

$$|l_{\mathbb{M}_n(R)}(D_A)| = \prod_{i=1}^{n} |\operatorname{ann}_R(d_i)|^n = |r_{\mathbb{M}_n(R)}(D_A)|$$

in posledično je po zgoraj ugotovljenem

$$|l_{\mathbb{M}_n(R)}(A)| = |r_{\mathbb{M}_n(R)}(A)| = \prod_{i=1}^{n} |\operatorname{ann}_R(d_i)|^n.$$

Če se spomnimo ugotovitve z začetka razdelka, lahko zaključimo, da sta vhodna in izhodna stopnja res obe enaki $\prod_{i=1}^n |\operatorname{ann}_R(d_i)|^n - \epsilon$, kjer je $\epsilon = 1$ (iz množice deliteljev niča odstranimo ničelno matriko), razen v primeru, ko je $A^2 = 0$ in je $\epsilon = 2$ (matrika ni povezana sama s sabo).

Iz zgornjih zvez sledi, da je matrika $X \in l_{\mathbb{M}_n(R)}(D_A) \cap r_{\mathbb{M}_n(R)}(D_A)$ natanko tedaj, ko je $x_{ij} \in \operatorname{ann}_R(d_i) \cap \operatorname{ann}_R(d_j)$. Posledično je

$$|l_{\mathbb{M}_n(R)}(A) \cap r_{\mathbb{M}_n(R)}(A)| = \prod_{i,j=1}^{n} |\operatorname{ann}_R(d_i) \cap \operatorname{ann}_R(d_j)|.$$

Ugotovitve sedaj združimo v

$$|l_{\mathbb{M}_n(R)}(A) \cup r_{\mathbb{M}_n(R)}(A)| = |l_{\mathbb{M}_n(R)}(A)| + |r_{\mathbb{M}_n(R)}(A)| - |l_{\mathbb{M}_n(R)}(A) \cap r_{\mathbb{M}_n(R)}(A)| =$$

$$2\prod_{i=1}^{n} |\operatorname{ann}_R(d_i)|^n - \prod_{i,j=1}^{n} |\operatorname{ann}_R(d_i) \cap \operatorname{ann}_R(d_j)|.$$

Sklenemo, da je stopnja vozlišča A v grafu $\Gamma(\mathbb{M}_n(R))$ res enaka $2\prod_{i=1}^n |\operatorname{ann}_R(d_i)|^n - \prod_{i,j=1}^n |\operatorname{ann}_R(d_i) \cap \operatorname{ann}_R(d_j)| - \epsilon$, kjer je $\epsilon = 1$, razen v primeru, ko je $A^2 = 0$. Takrat je $\epsilon = 2$. □

Primer 9.2. Denimo, da je kolobar R polje $R = \mathrm{GF}(p^\alpha)$. Vzemimo poljubno matriko $A \in \mathbb{M}_n(\mathrm{GF}(p^\alpha))$ kot zgoraj v izreku. Zgornje formule lahko nekoliko poenostavimo, saj je poljubni osnovni delitelj bodisi obrnljiv bodisi je 0. Velja, da je število neničelnih osnovnih deliteljev matrike A enako njenemu rangu. Velja

$\operatorname{ann}_R(d_i) = 0$, če je d_i obrnljiv element in $\operatorname{ann}_R(d_i) = R = \mathrm{GF}(p^\alpha)$, če je $d_i = 0$. Označimo s k rang matrike A (ker A ni obrnljiva, je $k < n$). Velja

$$|l_{\mathbb{M}_n(R)}(A)| = |r_{\mathbb{M}_n(R)}(A)| = \prod_{i=1}^{n} |\operatorname{ann}_R(d_i)|^n = \prod_{i=1}^{k} |\{0\}|^n \cdot \prod_{i=k+1}^{n} |R|^n = |\mathrm{GF}(p^\alpha)|^{n(n-k)}$$

in

$$|l_{\mathbb{M}_n(R)}(A) \cup r_{\mathbb{M}_n(R)}(A)| = 2|\mathrm{GF}(p^\alpha)|^{n(n-k)} - |\mathrm{GF}(p^\alpha)|^{(n-k)^2}.$$

Sledi, da sta vhodna in izhodna stopnja matrike $A \in \mathbb{M}_n(\mathrm{GF}(p^\alpha))$ v usmerjenem grafu $\Gamma_d(\mathbb{M}_n(\mathrm{GF}(p^\alpha)))$ enaki

$$|\mathrm{GF}(p^\alpha)|^{n(n-k)} - \epsilon,$$

stopnja A v $\Gamma(\mathbb{M}_n(\mathrm{GF}(p^\alpha)))$ pa je enaka

$$2|\mathrm{GF}(p^\alpha)|^{n(n-k)} - |\mathrm{GF}(p^\alpha)|^{(n-k)^2} - \epsilon,$$

kjer je $\epsilon = 1$, če $A^2 \neq 0$ in $\epsilon = 2$, če je $A^2 = 0$.

Zgornji izrek lahko uporabimo pri dokazu naslednjega izreka, a pred tem moramo razviti še malo teorije. Če za zaporedje različnih povezav $e_1, \ldots, e_s$ v usmerjenem grafu velja, da je končno vozlišče povezave e_i enako začetnemu vozlišču povezave e_{i+1} za vsak $1 \leq i \leq s-1$ in če je končno vozlišče e_s enako začetnemu vozlišču povezave e_1, potem pravimo, da je zaporedje vozlišč $e_1, \ldots, e_s$ *cikel* v usmerjenem grafu. Enako kot za neusmerjene grafe definiramo, da je cikel *Eulerjev cikel*, če vsebuje vsako povezavo natančno enkrat (in obišče vsako vozlišče, kar je ekvivalentno zahtevi, da je graf povezan). Graf oziroma usmerjeni graf je Eulerjev, če vsebuje Eulerjev cikel.

Dokažimo naslednjo lemo, ki povezuje Eulerjeve in uravnotežene grafe.

Lema 9.3. *Usmerjeni graf je Eulerjev natanko tedaj, ko je povezan in uravnotežen.*

Dokaz. Naj bo graf Eulerjev. Potem mora biti očitno povezan. Ker Eulerjev cikel vsakič, ko obišče neko vozlišče, vanj vstopi in izstopi po drugi povezavi, mora biti število vstopnih povezav enako številu izstopnih povezav. Povedano drugače, vhodna in izhodna stopnja vsakega vozlišča se morata ujemati, torej mora biti graf uravnotežen.

Naj bo usmerjen graf G povezan in uravnotežen. Z indukcijo na število povezav grafa pokažimo, da mora biti graf Eulerjev. Če je moč množice povezav $|E| = 2$, imamo graf na dveh točkah a, b s povezavama $a \to b$ in $b \to a$. Graf je Eulerjev. Oglejmo si povezan uravnotežen graf G z $|E| > 2$ povezavami. Izberimo poljubno vozlišče u in začnimo graditi pot, ki gre po vsaki povezavi največ enkrat. To storimo tako, da si v vsakem vozlišču preprosto izberemo povezavo, po kateri še nismo potovali in gremo po njej do naslednjega vozlišča. Ko pridemo do vozlišča, iz katerega ne moremo več nadaljevati poti, ker smo vse povezave že obhodili, mora biti to zaradi uravnoteženosti kar začetno vozlišče u. Denimo, da pri tem nismo obhodili vseh povezav grafa G. Oglejmo si graf G', ki ga dobimo tako, da grafu G odstranimo vse povezave na prej skonstruiranem ciklu in vsa izolirana vozlišča. Graf G' ni nujno povezan, še vedno pa je uravnotežen, saj smo iz vsakega vozlišča odstranili enako vhodnih in izhodnih povezav. Po indukcijski predpostavki vsaka povezana komponenta grafa G' vsebuje Eulerjev cikel. Ker je graf G povezan, mora zgoraj konstruirani cikel sekati vsako povezano komponento grafa G' vsaj v eni točki. V vsaki povezani komponenti grafa G' si torej izberemo eno vozlišče, v katerem konstruirani cikel seka to komponento in v njem združimo konstruirani cikel in Eulerjev cikel te komponente. Dobimo Eulerjev cikel za G. □

Lema 9.4. *Usmerjeni graf deliteljev niča $\Gamma_d(R)$ je povezan natanko tedaj, ko je množica levih deliteljev niča $Z_l(R)$ enaka množici desnih deliteljev niča $Z_r(R)$. Velja še: ko je $\Gamma_d(R)$ povezan, med poljubnima vozliščema x in y obstaja usmerjena pot dolžine največ tri.*

Dokaz. Če je graf $\Gamma_d(R)$ povezan, med poljubnima vozliščema x in y obstajata usmerjeni poti od x do y in od y do x. To pomeni, da se vsako vozlišče pojavi kot začetek in konec usmerjene poti, torej je vsako vozlišče tako levi kot desni delitelj niča.

Naj bo zdaj še $Z_l(R) = Z_r(R)$ in naj bosta $x \neq y$ poljubni vozlišči grafa $\Gamma_d(R)$. To pomeni, da sta $x, y \neq 0$. Poiskali bomo le usmerjeno pot od x do y, saj za obratno pot sklepamo analogno. Ločimo nekaj primerov. Če je $xy = 0$, je $x \to y$ iskana pot. Če je $xy \neq 0, x^2 = 0, y^2 = 0$, je $x \to xy \to y$ iskana pot. Če je $xy \neq 0, y^2 \neq 0, x^2 = 0$, potem obstaja $b \in R \setminus \{x, y, 0\}$, ki zadošča $by = 0$. Če je še $xb = 0$, je $x \to b \to y$ iskana pot, če pa je $xb \neq 0$, pa je $x \to xb \to y$ iskana pot. Naj bo zdaj $xy \neq 0, x^2 \neq 0, y^2 = 0$. Potem obstaja $c \in R \setminus \{x, y, 0\}$, da je $xc = 0$. Če je še $cy = 0$, je $x \to c \to y$ iskana pot, sicer pa je $x \to cy \to y$ iskana pot. Ostane nam le še primer, ko je $xy \neq 0, x^2 \neq 0, y^2 \neq 0$. Tedaj obstaja $b \in R \setminus \{x, y, 0\}$, da je $by = 0$. Če je še $xb = 0$, je $x \to b \to y$ iskana pot. Denimo, da je $xb \neq 0$. Po predpostavki obstaja $c \in R \setminus \{x, y, b, 0\}$, da je $xc = 0$. Če je $cy = 0$, je $x \to c \to y$ iskana pot. Denimo še, da je $cy \neq 0$. Če je še $cb \neq 0$, je $x \to cb \to y$ iskana pot, sicer pa je to pot $x \to c \to b \to y$. Opazimo, da smo v vseh primerih našli usmerjeno pot dolžine največ tri. $\square$

Primer 9.5. Naj bo R kolobar matrik nad $\mathbb{Z}_2$ z elementi $R = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, a = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, b = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, a + b = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \right\}$. Enostaven račun nam pokaže, da velja $ab = b, a(a + b) = a + b, ba = 0, b(a + b) = 0, (a + b)a = a, (a + b)b = b$. Ker je $ab = b$ in $ba = 0$, je R nekomutativen kolobar. Ima dve levi enoti a in $a + b$, obenem pa nima nobene desne enote. Velja še $Z_l(R) = \{b\}, Z_r(R) = \{a, a + b\}$. Opazimo, da graf $\Gamma_d(R)$ ni povezan. Res, edini povezavi sta namreč $b \to a$ in $b \to a + b$.

Izrek 9.6. *Naj bo R končni komutativni enotski glavni kolobar in $n \geq 2$. Tedaj je usmerjeni graf deliteljev niča $\Gamma_d(\mathbb{M}_n(R))$ Eulerjev.*

Dokaz. Po lemi 4.3 vemo, da sta v matričnih kolobarjih množici levih in desnih deliteljev niča enaki. Po lemi 9.4 je $\Gamma_d(\mathbb{M}_n(R))$ povezan. Po izreku 9.1 je $\Gamma_d(\mathbb{M}_n(R))$ uravnotežen in zato po lemi 9.3 Eulerjev. $\square$

Poiščimo še komutativni enotski kolobar R z neuravnoteženim grafom $\Gamma_d(\mathbb{M}_n(R))$.

Izrek 9.7. *Naj bo R končni komutativni enotski kolobar in $n \geq 2$. Če usmerjeni graf deliteljev niča $\Gamma_d(\mathbb{M}_n(R))$ ni uravnotežen, potem je $|R| \geq 8$. Ta ocena je optimalna, saj obstaja tak komutativni enotski kolobar R moči $|R| = 8$, da $\Gamma_d(\mathbb{M}_n(R))$ ni uravnotežen.*

Dokaz. Označimo z $\gamma(n)$ število neizomorfnih kolobarjev moči n. Pri tem upoštevamo tudi nekomutativne kolobarje in kolobarje brez enote. Vemo, da lahko vsak kolobar moči $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, kjer so p_i paroma različna praštevila, razcepimo kot $R = R_1 \times \cdots \times R_r$, pri čemer je moč $|R_i| = p_i^{\alpha_i}$ (tak razcep dobimo iz razcepa Abelovih grup). Sledi, da je γ multiplikativna, kar pomeni, da je $\gamma(n) = \gamma(p_1^{\alpha_1} \cdots p_r^{\alpha_r}) = \gamma(p_1^{\alpha_1}) \cdots \gamma_(p_r^{\alpha_r})$.

Opazimo, da je ničelni kolobar edini kolobar z enim elementom. Jasno je, da nima enote. Naj bo R kolobar moči p, kjer je p praštevilo. Po lemi 4.6 je kolobar R bodisi polje moči p bodisi ničelni kolobar moči p. Sledi, da je $\gamma(p) = 2$. Pripomnimo, da ničelni kolobar nima enote, graf $\Gamma_d(\mathbb{M}_n(\mathrm{GF}(p)))$ pa je uravnotežen po izreku 9.1.

Naj bosta $p \neq q$ različni praštevili. Zaradi multiplikativnosti γ velja $\gamma(pq) = \gamma(p)\gamma(q) = 4$. Naj bo R poljuben kolobar moči pq. Potem ima R ideal I_1 moči p in ideal I_2 moči q. Ker sta p in q različna, zapišemo $R \cong I_1 \oplus I_2$. Če naj ima R enoto, jo morata imeti tako I_1 kot I_2. Potem je $I_1 \cong \mathrm{GF}(p)$ in $I_2 \cong \mathrm{GF}(q)$. Ker je $\mathrm{GF}(p) \oplus \mathrm{GF}(q)$ glavni komutativni enotski kolobar, je po izreku 9.1 graf $\Gamma_d(\mathbb{M}_n(R))$ uravnotežen.

Naj bo $|R| = p^2$, kjer je p praštevilo. Znano je, da obstaja natanko 11 neizomorfnih kolobarjev moči p^2 (glej [9, Izrek 2]). Če je R komutativni enotski kolobar moči p^2, potem je glavni. Res, naj bo I poljuben pravi ideal. Potem mora imeti I natanko p elementov. Sledi, da je kot aditivna grupa generiran z neničelnim elementom, torej je I glavni ideal. Po izreku 9.1 je graf $\Gamma_d(\mathbb{M}_n(R))$ uravnotežen.

Če označimo s $k = |R|$, je za $1 < k < 8$ število k bodisi praštevilo bodisi produkt dveh različnih praštevil bodisi kvadrat praštevila. V vseh teh primerih smo zgoraj videli, da graf $\Gamma_d(\mathbb{M}_n(R))$ je uravnotežen. Če za neki kolobar R graf $\Gamma_d(\mathbb{M}_n(R))$ ni uravnotežen, mora biti $|R| \geq 8$. Dokaz bo zaključen, če uspemo skonstruirati kolobar R moči 8, da graf $\Gamma_d(\mathbb{M}_n(R))$ ne bo uravnotežen.

Označimo z R $\mathbb{Z}_2$-algebro z bazo $\{1, a, b\}$ in z množenjem predpisanim takole

$$\begin{array}{c|ccc} \cdot & 1 & a & b \\ \hline 1 & 1 & a & b \\ a & a & 0 & 0 \\ b & b & 0 & 0 \end{array}.$$

Preprost premislek nam pokaže, da je to res komutativni enotski kolobar. Velja $R = \{0, 1, a, b, 1+a, 1+b, a+b, 1+a+b\}$ in $|R| = 8$. Opazimo, da R ni glavni kolobar, saj ideal (a, b), generiran z elementoma a, b, ni glavni. Pokažimo, da $\Gamma_d(\mathbb{M}_2(R))$ ni uravnotežen graf. V ta namen bomo poračunali, da se vhodna in izhodna stopnja vozlišča $A = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ ne ujemata. Naj bo $B = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$ poljubna druga matrika iz $\mathbb{M}_2(R)$. Določimo najprej vhodno stopnjo vozlišča A. Zanima nas, kdaj bo

$$0 = BA = \begin{bmatrix} x & y \\ z & w \end{bmatrix} \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} = \begin{bmatrix} xa + yb & 0 \\ za + wb & 0 \end{bmatrix}.$$

Veljati mora $xa + yb = 0$ in $za + wb = 0$. Določimo pogoje na x, y, za z, w bodo morali veljati isti pogoji. Če je $x \in \{0, a, b, a+b\}$, potem je $xa + yb = yb$ in mora biti $y \in \{0, a, b, a+b\}$. Če je $x \in \{1, 1+a, 1+b, 1+a+b\}$, pa ne obstaja tak y, da bi bilo $xa + yb = 0$. Za matriko B imamo torej $(4 \cdot 4)^2 - 2$ možnosti (kvadriranje se pojavi, ker imamo prav toliko pogojev še na z, w, 2 pa odštejemo, ker iz grafa odstranimo ničelno matriko in ker je $A^2 = 0$). Vhodna stopnja je $16^2 - 2 = 256 - 2 = 254$.

Določimo še izhodno stopnjo. Zanima nas, koliko je matrik B kot zgoraj, za katere je

$$0 = AB = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} ax & ay \\ bx & by \end{bmatrix}.$$

Takoj opazimo, da sta z in w lahko poljubna, element x pa mora biti tak, da je $ax = bx = 0$. To pomeni, da mora biti $x \in \{0, a, b, a+b\}$. Vidimo, da imamo za y iste štiri možnosti. Vseh ustreznih matrik B je $4 \cdot 4 \cdot 8 \cdot 8 - 2$, kjer 2 odštejemo iz istega razloga kot zgoraj. Izhodna stopnja je enaka $4^2 \cdot 8^2 - 2 = 2^{10} - 2 = 1024 - 2 = 1022$. Vhodna in izhodna stopnja se razlikujeta, zato graf $\Gamma_d(\mathbb{M}_2(R))$ ni uravnotežen. $\square$

10. Klasifikacija končnih kolobarjev z Eulerjevim grafom deliteljev niča

V tem razdelku bomo opazovali neusmerjeni graf deliteljev niča. Natančno bomo klasificirali končne kolobarje, ki imajo Eulerjev graf deliteljev niča. Spomnimo se, da je neusmerjeni graf *Eulerjev*, če vsebuje *Eulerjev obhod*, to je sklenjen sprehod, ki vsebuje vsako povezavo grafa natanko enkrat. Znan je izrek, ki pravi, da je graf Eulerjev natanko takrat, ko je povezan in so vse njegove točke sode stopnje [6, Izrek 1.8.1]. Spomnimo se še, da je graf $\Gamma(R)$ vedno povezan (glej [16, Izrek 3.8], pri čemer je potrebno za nekomutativni primer dokaz samo malo popraviti). Obravnavo bomo razdelili na tri podprimere.

10.1. Končni nilpotentni kolobarji z Eulerjevim grafom deliteljev niča.

Trditev 10.1. *Naj bo R končni neničelni nilpotentni kolobar. Graf $\Gamma(R)$ je Eulerjev natanko tedaj, ko je $|R|$ sodo število in je kvadrat vsakega elementa iz R enak 0, to je $x^2 = 0$ za vsak $x \in R$.*

Dokaz. Pokažimo najprej lažjo smer. Naj bo R kolobar moči $|R| = 2^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, kjer so $p_2, \ldots, p_m$ različna liha praštevila, $\alpha_1 \geq 1$ ter $\alpha_i \geq 0$ za $i = 2, \ldots, m$. Naj za vsak $x \in R$ velja še $x^2 = 0$. Iz prve predpostavke sledi, da je $R = R_1 \oplus R_2 \oplus \cdots \oplus R_m$, kjer je $|R_1| = 2^{\alpha_1}$ in $|R_i| = p_i^{\alpha_i}, i = 2, 3, \ldots, m$. Naj bo $a = (a_1, a_2, \ldots, a_m) \in R$ poljuben neničelen element. Iz druge predpostavke po lemi 4.8 sledi, da je R antikomutativen. Zato je $r_{R_i}(a_i) = l_{R_i}(a_i) = \operatorname{ann}_{R_i}(a_i), i = 1, 2, \ldots, m$. S pomočjo pravkar ugotovljenega lahko zapišemo zvezo

$$\deg(a) = |\operatorname{ann}_{R_1}(a_1)| \cdot |\operatorname{ann}_{R_2}(a_2)| \cdots |\operatorname{ann}_{R_m}(a_m)| - |\{0, a\}|.$$

Ker $0, a_1 \in \operatorname{ann}_{R_1}(a_1)$ in ker je $\operatorname{ann}_{R_1}(a_1)$ podgrupa R_1, je $|\operatorname{ann}_{R_1}(a_1)| = 2^t$, kjer je $1 \leq t \leq \alpha_1$. Sledi, da je $\deg(a)$ sodo število in $\Gamma(R)$ Eulerjev graf.

Pokažimo še obrat. Naj bo R končni nilpotentni kolobar z lastnostjo, da je graf $\Gamma(R)$ Eulerjev. Naj bo $n \in \mathbb{N}$ indeks nilpotentnosti R, torej $R^n = 0$ in $R^{n-1} \neq 0$.

Naj bo najprej $|R| = p^m$, kjer je p praštevilo in $m \in \mathbb{N}$. Naj bo $0 \neq a \in R^{n-1}$. Ker je $R^n = 0$, je $aR = Ra = 0$. Posledično velja

$$\deg(a) = |R| - |\{0, a\}| = |R| - 2.$$

Ker je $\Gamma(R)$ Eulerjev graf, je $\deg(a)$ sodo število in zato je $|R| = 2^m$. Naj $x \in R$ zadošča $x^2 \neq 0$. Ker je R nilpotenten, množice $\operatorname{ann}_R(x), r_R(x), l_R(x)$ poleg ničle zagotovo vsebujejo še neko potenco elementa x. Sklenemo, da so števila $|\operatorname{ann}_R(x)|, |r_R(x)|, |l_R(x)|$ vse potence števila 2 in $|\operatorname{ann}_R(x)| \geq 2$. Sledi

$$\deg(x) = |l_R(x)| + |r_R(x)| - |\operatorname{ann}_R(x)| - |\{0\}|.$$

Ker so prvi trije členi na desni soda števila, je $\deg(x)$ liho število, kar je v nasprotju s tem, da je $\Gamma(R)$ Eulerjev graf. Sklenemo, da za vsak $x \in R$ velja $x^2 = 0$.

Naj bo zdaj $|R| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, kjer je $m \geq 2$ in so $p_1, \ldots, p_m$ različna praštevila. Zapišemo lahko $R = R_1 \oplus R_2 \oplus \cdots \oplus R_m$, kjer je $|R_i| = p_i^{\alpha_i}$. Za vsak $i = 1, \ldots, m$ naj bo n_i indeks nilpotentnosti R_i, torej $R_i^{n_i} = 0$ in $R_i^{n_i - 1} \neq 0$ (taka števila n_i obstajajo, ker je R nilpotenten). Podobno kot prej vzemimo $a \in R_1^{n_1-1}$. Velja $a^2 = 0$ in posledično je

$$\deg((a, 0, \ldots, 0)) = |R_1| \cdots |R_m| - 2 = |R| - 2.$$

Ker je graf $\Gamma(R)$ Eulerjev, zaključimo, da je stopnja vozlišča $(a, 0, \ldots, 0)$ soda in zato je $|R|$ sodo število. To pomeni, da je eno izmed praštevil p_i enako 2. Predpostavimo lahko, da je $p_1 = 2$ in $|R_1| = 2^{\alpha_1}$, kjer je $\alpha_1 \geq 1$. Naj bo $0 \neq a \in R_1$. Denimo, da je $a^2 \neq 0$. Izberimo še $0 \neq (r_1, r_2, \ldots, r_m) \in R \setminus (a, 0, \ldots, 0)$ (tak element obstaja, ker je $m \geq 2$). Potem je vozlišče $(a, 0, \ldots, 0)$ sosednje z vozliščem $(r_1, r_2, \ldots, r_m)$ natanko tedaj, ko je $r_1 \in l_{R_1}(a) \cup r_{R_1}(a)$. Spet pogledamo stopnjo vozlišča

$$\deg((a, 0, \ldots, 0)) = (|l_{R_1}(a)| + |r_{R_1}(a)| - |\operatorname{ann}_{R_1}(a)|) \cdot |R_2| \cdots |R_m| - 1.$$

Ker je člen v oklepaju sod, je ta stopnja liho število, kar je v nasprotju z našo predpostavko, da je graf Eulerjev. Sledi, da je $a^2 = 0$ za vsak $a \in R_1$.

Naj bo zdaj $b \in R_2$. Denimo, da je $b^2 \neq 0$. Potem je

$$\deg((0, b, 0, \ldots, 0)) = |R_1| \cdot |l_{R_1}(b) \cup r_{R_1}(b)| \cdot |R_3| \cdots |R_m| - 1,$$

kar je liho število (ker je $|R_1|$ sodo število). Protislovje. Sklenemo, da je $b^2 = 0$ za vsak $b \in R_2$. Na enak način kot za $b \in R_2$ lahko vidimo, da za poljuben $b \in R_i, i = 2, \ldots, m$ velja $b^2 = 0$. Sledi, da za vsak $x \in R$ velja $x^2 = 0$. Trditev je dokazana. $\square$

Primer 10.2. (1) Naj bo $R = \left\{ \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}; a \in \mathbb{Z}_4 \right\}$. Jasno je, da je $|R| = 4$ sodo število in $R^2 = 0$, torej kolobar R ustreza predpostavkam trditve. Velja tudi, da je $\Gamma(R)$ Eulerjev graf, saj velja $\Gamma(R) \cong K_3$.

(2) Naj bo $R = \left\{ \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}; a \in \mathbb{Z}_5 \right\}$. Kolobar ima pet elementov in zato ne ustreza prvi zahtevi trditve. Velja še $\Gamma(R) \cong K_4$, torej je stopnja vsakega vozlišča enaka 3 in graf zato ni Eulerjev.

(3) Naj bo $R = \left\{ \begin{bmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{bmatrix}; a, b, c \in \mathbb{Z}_2 \right\}$. Velja $|R| = 8$, torej R zadošča prvi predpostavki izreka. Naj E_{ij} označuje matriko, ki ima na mestu (i, j) 1, drugje pa same ničle. Označimo z $m_0 = 0, m_1 = E_{23}, m_2 = E_{13}, m_3 = E_{13} + E_{23}, m_4 = E_{12}, m_5 = E_{12}+E_{23}, m_6 = E_{12}+E_{13}, m_7 = E_{12}+E_{13}+E_{23}$ elemente kolobarja R. Potem je $m_5^2 = m_2 \neq 0$, torej R ne ustreza drugi predpostavki izreka. Nekaj računanja nam pokaže, da so edini neničelni produkti različnih elementov naslednji $m_4m_1 = m_2, m_4m_3 = m_2, m_4m_5 = m_2, m_4m_7 = m_2, m_5m_1 = m_2, m_5m_3 = m_2, m_5m_7 = m_2, m_6m_1 = m_2, m_6m_3 = m_2,$ $m_6m_5 = m_2, m_6m_7 = m_2, m_7m_1 = m_2, m_7m_3 = m_2, m_7m_5 = m_2$. Ker smo definirali, da sta vozlišči, ki pripadata elementoma x in y sosednji natanko tedaj, ko je vsaj eden izmed produktov xy, yx enak 0, lahko pozoren bralec ugotovi, da vozlišči, ki pripadata elementoma m_5 in m_7 nista sosednji, po drugi strani pa je m_5 soseden z vsemi ostalimi. To pomeni, da je $\deg(m_5) = 5$, kar ni sodo število. Sklenemo, da $\Gamma(R)$ ni Eulerjev graf.

V drugi in tretji točki zgornjega primera smo videli, da sta pogoja v izreku res potrebna.

10.2. **Končni nenilpotentni enotski kolobarji z Eulerjevim grafom deliteljev niča.**

Trditev 10.3. *Naj bo R končni enotski kolobar, ki ni polje. Potem je graf $\Gamma(R)$ Eulerjev natanko tedaj, ko R zadošča enemu izmed naslednjih dveh pogojev:*

(1) *$R \cong \oplus_{i=1}^{k} \mathrm{GF}(p_i^{\alpha_i})$, kjer so p_i liha praštevila in je $k \geq 2$,*
(2) *R je lokalni kolobar moči $|R| = 2^{\alpha}, \alpha \geq 2$ in za vsak $x \in J(R)$ velja $x^2 = 0$.*

Dokaz. Naj bo R končni enotski kolobar z Eulerjevim grafom deliteljev niča. Denimo, da je $|R| = n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}, s \geq 1$, p_i paroma različna praštevila. Zapišemo lahko $R = R_1 \oplus \cdots \oplus R_s$, kjer je $|R_i| = p_i^{\alpha_i}, 1 \leq i \leq s$. Sedaj ločimo več primerov.

Naj bo najprej $s \geq 2$. Potem za $1 \leq i \leq s$ označimo z e_i enoto kolobarja R_i. Potem je $(e_1, \ldots, e_s)$ enota R. Poglejmo element $x_i = (0, \ldots, 0, e_i, 0, \ldots, 0)$. Velja

$$\mathrm{ann}_R(x_i) = R_1 \oplus \cdots \oplus R_{i-1} \oplus \{0\} \oplus R_{i+1} \oplus \cdots \oplus R_s.$$

Od tod takoj sledi, da je

$$\deg(x_i) = |\operatorname{ann}_R(x_i)| - 1 = p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_s^{\alpha_s} - 1.$$

Ker je graf $\Gamma(R)$ Eulerjev, je stopnja vsakega vozlišča sodo število, zato nobeno izmed praštevil p_i ni enako 2. Sledi, da je n liho število in je karakteristika R liha. Če torej za neki $x \in R$ velja $2x = 0$, potem je $x = 0$. To pomeni, da za vsak $x \in R^*$ velja $x \neq -x$, saj bi sicer prišli v nasprotje s pravkar ugotovljenim. Denimo, da obstaja neničelni element $x \in R$, da je $x^2 = 0$. Torej velja $0, x \in \mathrm{ann}_R(x)$. Denimo, da je vozlišče x povezano še z nekim vozliščem y. To pomeni, da je bodisi $xy = 0$ bodisi $yx = 0$. Oglejmo si le prvo možnost, za drugo namreč lahko naredimo podoben premislek. Če je $xy = 0$, je tudi $0 = -xy = x(-y)$, torej je vozlišče x sosednje tudi z $-y$. To pomeni, da vsi sosedi $y \neq -x$ vozlišča x nastopajo v parih $(y, -y)$. Takih je torej sodo, poleg tega pa je x soseden še z $-x$, torej je stopnja x liho število. Protislovje. Sklenemo, da kolobar R ne vsebuje neničelnih nilpotentnih elementov. Torej je $J(R) = 0$. Za artinske in v posebnem tudi končne kolobarje je to po [13, Izrek 4.14] ekvivalentno temu, da je kolobar R polenostaven. Po Wedderburn-Artinovem izreku je $R \cong \mathbb{M}_{n_1}(D_1) \times \cdots \times \mathbb{M}_{n_k}(D_k)$, kjer so D_i končni obsegi, torej polja. Ker smo ravnokar dokazali, da R nima neničelnih nilpotentov, je $n_i = 1$ za vsak $1 \leq i \leq k$. Zaključimo, da je $R \cong \oplus_{i=1}^{k} \mathrm{GF}(q_i)$, kjer je $q_i = \tilde{p}_i^{\beta_i}$, $\tilde{p}_i$ pa so liha praštevila. Velja še $k \geq s \geq 2$.

Naj bo $s = 1$. Potem je $|R| = p^n$, kjer je p praštevilo in $n \geq 1$ naravno število. Naj bo najprej p liho praštevilo. Če je $n = 1$, je po lemi 4.6 R polje (ker ima enoto). Protislovje. Naj bo torej $n \geq 2$. Če je $J(R) \neq 0$, potem v R obstaja neničelni element $x \in J(R)$, da je $x^2 = 0$ (ker $J(R)$ nilpotenten). Tako kot v prvem primeru vidimo, da $x \neq -x$ in da je $\deg(x)$ liho število. Protislovje. Sledi, da R nima neničelnih nilpotentov in zato je enako kot zgoraj R izomorfen direktni vsoti končnih polj $R = \oplus_{i=1}^{k} \mathrm{GF}(p^{\beta_i})$,kjer sta $k \geq 2$ (ker R po predpostavki ni polje), $\beta_i \geq 1, \beta_1 + \cdots + \beta_k = n$.

Poglejmo še zadnji primer, ko je $|R| = 2^{\alpha}$, kjer $\alpha \geq 1$. Če je $\alpha = 1$, je po lemi 4.6 R spet polje. Protislovje. Torej je $\alpha \geq 2$. Denimo, da obstaja neki delitelj niča (enostranski ali dvostranski) x, da je $x^2 \neq 0$ in $\mathrm{ann}_R(x) \neq 0$. Ker so $l_R(x), r_R(x), \mathrm{ann}_R(x)$ podgrupe in ker po zgornji predpostavki niso trivialne, sledi, da so njihove moči soda števila. Potem je stopnja

$$\deg(x) = |(l_R(x) \cup r_R(x)) \setminus \{0\}| = |l_R(x)| + |r_R(x)| - |\operatorname{ann}_R(x)| - 1$$

liho število. Protislovje. Sklenemo, da je za poljuben enostranski ali dvostranski delitelj niča x bodisi $x^2 = 0$ bodisi je $\operatorname{ann}_R(x) = 0$.

Naj bo najprej $J(R) = 0$, torej je R polenostavni kolobar. Potem je $R \cong \oplus_{i=1}^{k}\mathbb{M}_{n_i}(\mathrm{GF}(2^{\beta_i}))$. Pokažimo, da je $n_i = 1$ za $1 \leq i \leq k$. Denimo nasprotno, da za neki i velja $n_i \geq 2$. Označimo z $\{E_{l,j}\}_{l,j=1}^{n}$ množico matričnih enot kolobarja $\mathbb{M}_{n_i}(\mathrm{GF}(2^{\beta_i}))$. Velja $E_{1,1}^2 = E_{1,1}$ in $\operatorname{ann}_R(E_{1,1}) \neq 0$, saj zagotovo vsebuje $E_{2,2}$. Protislovje z zgornjo ugotovitvijo. Zapišemo lahko $R \cong \oplus_{i=1}^{k}\mathrm{GF}(2^{\beta_i})$. Denimo, da je $k \geq 2$. Izberemo $x \in \mathrm{GF}(2^{\beta_1})^*$ in $y \in \mathrm{GF}(2^{\beta_2})^*$. Oglejmo si elementa $\tilde{x} = (x, 0, \ldots, 0)$ in $\tilde{y} = (0, y, 0, \ldots, 0)$. Velja $\tilde{x}^2 \neq 0$ in $\tilde{y} \in \operatorname{ann}_R(\tilde{x}) \neq 0$. Protislovje. Sledi, da je $k = 1$ in $R \cong \mathrm{GF}(2^{\beta_1})$, kar je v nasprotju s predpostavko izreka.

Naj bo $J(R) \neq 0$. Potem je $R/J(R) \cong \oplus_{i=1}^{k}\mathbb{M}_{n_i}(\mathrm{GF}(2^{\beta_i}))$. Ker je $J(R)$ nilpotenten, obstaja $N \in \mathbb{N}$, da je $J(R)^N \neq 0$ in $J(R)^{N+1} = 0$. Vzemimo $0 \neq x \in J(R)$. Potem je $0 \neq J(R)^N \subseteq \operatorname{ann}_R(x)$, torej je $\operatorname{ann}_R(x) \neq 0$. Ker je $\operatorname{ann}_R(x) \neq 0$, mora biti po zgoraj ugotovljenem $x^2 = 0$ (videli smo, da je za vsak delitelj niča x bodisi $x^2 = 0$ bodisi je $\operatorname{ann}_R(x) = 0$). Sklenemo, da je $x^2 = 0$ za vsak $x \in J(R)$. Ker je R končen, je artinski in zato je $J(R)$ nil ideal. Sledi, da je $J(R)$ SBI-kolobar. Ker je $R/J(R) \cong \oplus_{i=1}^{k}\mathbb{M}_{n_i}(\mathrm{GF}(2^{\beta_i}))$, lahko najdemo elemente $\overline{u}_i \in R/J(R), i = 1, \ldots, k$, da je $\overline{u}_i$ enota $\mathbb{M}_{n_i}(\mathrm{GF}(2^{\beta_i}))$. Ker je R enotski SBI-kolobar, lahko po lemi 5.13 najdemo idempotente $e_i, i = 1, \ldots, k$, da je $\overline{e}_i = \overline{u}_i, i = 1, \ldots, k$. Ker so $\{\overline{u}_i\}_{i=1}^{k}$ ortogonalni idempotenti, so po lemi 5.13 tudi $\{e_i\}_{i=1}^{k}$ ortogonalni idempotenti. Denimo, da je $k > 2$. Potem je $e_ie_j = e_je_i = 0$ za $i \neq j$. Potem je $\operatorname{ann}_R(e_i) \neq 0$ za vsak $i \in \{1, \ldots, k\}$. Velja torej $e_1^2 = e_1 \neq 0$ in $\operatorname{ann}_R(e_1) \neq 0$, kar je v nasprotju z našo ugotovitvijo, da je za vsak delitelj niča x bodisi $x^2 = 0$ bodisi je $\operatorname{ann}_R(x) = 0$.

Sledi, da je $k = 1$ in zato je $R/J(R) \cong \mathbb{M}_{n_1}(\mathrm{GF}(2^{\beta_1}))$. Denimo, da je $n_1 > 1$. Ker je R SBI-kolobar po izreku 5.16 sledi, da ima R matrične enote. To nas spet pripelje v protislovje, saj za matrično enoto e_{11} velja $e_{11}^2 = e_{11} \neq 0$ in $e_{22} \in \operatorname{ann}_R(e_{11}) \neq 0$. Sledi, da je $n_1 = 1$, torej je $R/J(R) \cong \mathrm{GF}(2^{\beta_i})$. To pomeni, da je R lokalni kolobar.

Dokažimo še obrat. Naj bo najprej $R = \oplus_{i=1}^{s}\mathrm{GF}(p_i^{\alpha_i})$, kjer so p_i liha praštevila. Delitelji niča so s-terice, ki vsaj na enem mestu vsebujejo 0. Naj bo torej $x = (x_1, x_2, \ldots, x_s)$ poljubni neničelni delitelj niča. Naj bo $\mathcal{I}(x) = \{i; x_i = 0\}$ množica indeksov, kjer ima element x ničelne komponente. Vzemimo poljuben element $y \in R$. Vozlišči x in y sta povezani natanko tedaj, ko sta množici $\mathcal{I}(x)^C$ in $\mathcal{I}(y)^C$ disjunktni. Sledi, da je $\deg(x) = \prod_{l\in\mathcal{I}(x)} p_l^{\alpha_l} - 1$ sodo število in posledično je graf $\Gamma(R)$ Eulerjev.

Naj bo zdaj R lokalni kolobar z $2^{\alpha}, \alpha \geq 2$, elementi in naj za vsak $x \in J(R)$ velja $x^2 = 0$. Ker je R lokalen, je $R \setminus J(R) = U(R)$ množica obrnljivih elementov. Vemo, da je $J(R)$ nilpotentni ideal, torej je $J(R)$ množica vseh deliteljev niča. Iz predpostavke $x^2 = 0$ za vsak $x \in J(R)$ po lemi 4.8 sledi, da je $J(R)$ antikomutativen. To pomeni, da iz $xy = 0$ sledi $yx = 0$ in zato je $l_R(x) = r_R(x) = \operatorname{ann}_R(x)$ za vsak delitelj niča. Vzemimo poljuben delitelj niča $x \neq 0$. Iz predpostavke $x^2 = 0$ sledi, da $\operatorname{ann}_R(x) \neq 0$ in zato je

$$\deg(x) = |l_R(x)| + |r_R(x)| - |\operatorname{ann}_R(x)| - |\{0, x\}| = |l_R(x)| - 2$$

sodo število. Sklenemo, da je graf Eulerjev. □

10.3. **Končni nenilpotentni kolobarji brez enote in z Eulerjevim grafom deliteljev niča.**

Trditev 10.4. *Naj bo R končni nenilpotentni kolobar brez enote. Potem je graf $\Gamma(R)$ Eulerjev natanko tedaj, ko je izpolnjen eden izmed naslednjih dveh pogojev:*

(1) $R \cong S \oplus N$, *kjer je* S *lokalni enotski kolobar moči* $|S| = 2^\alpha, \alpha \geq 1$ *in za vsak* $s \in J(S)$ *velja* $s^2 = 0$, N *pa je neničelni nilpotentni kolobar lihe moči in za vsak* $x \in N$ *velja* $x^2 = 0$,

(2) $R \cong S \oplus N$, *kjer je* S *nerazcepni kolobar brez enostranske enote moči* $|S| = 2^\alpha, \alpha \geq 2$, *za vsak* $s \in J(S)$ *velja* $s^2 = 0$ *in je kvocientni kolobar* $S/J(S)$ *polje,* N *pa je nilpotentni kolobar lihe moči v katerem za vsak* x *velja* $x^2 = 0$ *(lahko je* $N = 0$*).*

Dokaz. Naj bo R končni nenilpotentni kolobar brez enote z Eulerjevim grafom deliteljev niča. Velja $R = R_1 \oplus R_2 \oplus \cdots \oplus R_m, m \geq 1$ in $|R_i| = p_i^{\alpha_i}, i = 1, \ldots, m$ (p_i paroma različna praštevila). Ker je R brez enote, po lemi 4.1 obstaja tak indeks j, da R_j vsebuje nilpotentni element x. Predpostavimo, da je $x^2 = 0$ (sicer zamenjamo x z x^{n-1}, kjer je n najmanjše število, ki zadošča $x^n = 0$). Stopnja x je sodo število, saj je graf Eulerjev. Zapišemo lahko (x enačimo z $(0, \ldots, 0, x, 0, \ldots, 0)$)

$$\deg(x) = |l_{R_j}(x) \cup r_{R_j}(x)| \cdot |R_1| \cdots |R_{j-1}| \cdot |R_{j+1}| \cdots |R_m| - |\{0, x\}| =$$
$$\Big(|l_{R_j}(x)| + |r_{R_j}(x)| - |\operatorname{ann}_{R_j}(x)|\Big) \cdot |R_1| \cdots |R_{j-1}| \cdot |R_{j+1}| \cdots |R_m| - 2.$$

Ker je $x \in \operatorname{ann}_{R_j}(x)$, je $\operatorname{ann}_{R_j}(x) \neq 0$ in zato je prava podgrupa moči p_j. Ker je stopnja sodo število, trdimo, da je eno izmed praštevil p_i enako 2. Izraz v oklepaju namreč lahko zapišemo kot $p_j^{\beta_1} + p_j^{\beta_2} - p_j^{\beta_3}$, pri čemer velja $1 \leq \beta_3 \leq \beta_1, \beta_2$. Preoblikujemo to v $p_j^{\beta_3}(p_j^{\beta_1 - \beta_3} + p_j^{\beta_2 - \beta_3} - 1)$. Če je p_j liho praštevilo, je tudi izraz v zadnjem oklepaju liho število. Ker je stopnja sodo število, mora biti v tem primeru neko drugo praštevilo sodo. Predpostavimo, da je $p_1 = 2$.

Denimo, da za neki element $y \in R_2$ velja $y^2 \neq 0$ Zapišemo lahko

$$\deg((0, y, 0, \ldots, 0)) = |R_1| \cdot |l_{R_2}(y) \cup r_{R_2}(y)| \cdot |R_3| \cdots |R_m| - 1,$$

torej je stopnja $(0, y, 0, \ldots, 0)$ liho število, kar je v nasprotju s predpostavko, da je graf Eulerjev. To pomeni, da za vsak element $y \in R_2$ velja $y^2 = 0$. Na analogen način pokažemo, da za poljuben $y \in R_i, i \geq 2$ velja $y^2 = 0$.

Če definiramo $N = R_2 \oplus R_3 \oplus \cdots \oplus R_m$, nam zgornji premislek pokaže, da za vsak $y \in N$ velja $y^2 = 0$. Po lemi 4.9 je N nilpotentni kolobar.

Naj bo zdaj $r \in R_1$ nilpotentni element za katerega velja $r^2 \neq 0$. Ker je r nilpotenten, obstaja $n \geq 3$, da je $r^{n-1} \neq 0$ in $r^n = 0$. Potem je $r^{n-1} \in \operatorname{ann}_{R_1}(r)$ in zato $\operatorname{ann}_{R_1}(r) \neq 0$. Posledično je

$$\deg((r, 0, \ldots, 0)) = \Big(|l_{R_1}(r)| + |r_{R_1}(r)| - |\operatorname{ann}_{R_1}(r)|\Big) \cdot |R_2| \cdots |R_m| - 1$$

liho število. To pa je v nasprotju s predpostavko. Sklenemo, da za vsak nilpotentni element $r \in R_1$ velja $r^2 = 0$.

Po predpostavki je kolobar R nenilpotenten, torej vsebuje vsaj en nenilpotentni element. Ta mora ležati v R_1, saj je N nilpotenten. Denimo, da je ta element x . Zanj velja, da je $\operatorname{ann}_{R_1}(x) = 0$. Recimo nasprotno, da je $|\operatorname{ann}_{R_1}(x)| \geq 2$. Iz enačbe

$$\deg((x, 0, \ldots, 0)) = \Big(|l_{R_1}(x)| + |r_{R_1}(x)| - |\operatorname{ann}_{R_1}(x)|\Big) \cdot |R_2| \cdots |R_m| - 1$$

sledi, da je $\deg((x, 0, \ldots, 0))$ liho število, saj je člen v oklepaju oblike $2^{\beta_1}k, 1 \leq \beta_1 \leq \alpha_1, k \in \mathbb{N}$. To je protislovje. Zaključimo, da je $\operatorname{ann}_{R_1}(x) = 0$ za vsak nenilpotentni element $x \in R_1$.

Denimo, da obstaja nenilpotentni element $x \in R_1$ za katerega velja $r_{R_1}(x) = 0$. Če je $l_{R_1}(x) \neq 0$, potem je

$$\deg((x, 0, \ldots, 0)) = |l_{R_1}(x)| \cdot |R_2| \cdots |R_m| - 1$$

liho število, saj je $|l_{R_1}(x)|$ sode moči (ker je prava podgrupa R_1). Protislovje. Sklenemo lahko, da za vsak nenilpotentni element $x \in R_1$ iz $r_{R_1}(x) = 0$ sledi $l_{R_1}(x) = 0$. Na enak način pokažemo, da za vsak nenilpotentni element $x \in R_1$ iz $l_{R_1}(x) = 0$ sledi $r_{R_1}(x) = 0$. Zaključimo, da je za vsak nenilpotentni element $x \in R_1$ bodisi $l_{R_1}(x) = r_{R_1}(x) = 0$ bodisi $l_{R_1}(x) \neq 0 \neq r_{R_1}(x)$.

Recimo, da je kolobar R_1 razcepen. To pomeni, da ga lahko zapišemo kot $R_1 = S_1 \oplus S_2$, kjer sta S_1 in S_2 dva dvostranska ideala kolobarja R_1. Ker je $|R_1| = 2^{\alpha_1}$, sta tudi kolobarja S_1 in S_2 moči $2^{\alpha_{11}}$ in $2^{\alpha_{12}}$, kjer je $\alpha_{11}+\alpha_{12} = \alpha_1$. Ker R_1 ni nilpotenten, zagotovo vsaj eden izmed S_1 in S_2 ni nilpotenten, saj bi bil v nasprotnem primeru R_1 nilpotenten. Predpostavimo, da S_1 ni nilpotenten. Pokažimo, da mora biti S_2 nilpotenten. Recimo nasprotno. Potem obstaja $s \in S_2$, da je $s^2 \neq 0$. Velja, da je

$$\deg((0, s, 0, \dots, 0)) = |S_1| \cdot |l_{S_2}(s) \cup r_{S_2}(s)| \cdot |R_2| \cdots |R_m| - 1$$

liho število, saj je $2 \leq |S_1|$ potenca števila 2. Protislovje. Torej je res S_2 nilpotenten. Torej je $R = S_1 \oplus N_1$, kjer je $N_1 = S_2 \oplus N$ nilpotentni kolobar, S_1 pa nerazcepen.

Poenostavimo oznake. Zgornji premislek pokaže, da lahko R zapišemo kot $R = S \oplus N$, kjer je S nerazcepni nenilpotentni kolobar moči $|S| = 2^\alpha$, N pa je nilpotentni kolobar. Dodatno velja še za vsak nilpotentni element $x \in R$, da je $x^2 = 0$.

Pokažimo še, da je S bodisi lokalni enotski kolobar in je $\alpha \geq 1$ bodisi nerazcepni kolobar brez enostranske enote in je $\alpha \geq 2$ ter $S/J(S)$ polje. Dodatno moramo videti še, da je $s^2 = 0$ za vsak $s \in J(S)$ in da je $|N|$ liho število, ki je v prvem primeru strogo večje od 1.

Predpostavimo, da v S obstaja element x, za katerega velja $r_S(x) = l_S(x) = 0$. Po lemi 4.5 ima S enoto za množenje. To implicira, da je $N \neq 0$, saj bi sicer R imel enoto, kar je v nasprotju z našo predpostavko. Zgoraj smo videli, da je $\operatorname{ann}_S(x) = 0$ za vsak nenilpotentni element $x \in S$ (uporabljali smo oznako R_1). Od tod sledi, da S ne vsebuje ortogonalnih idempotentov. Recimo nasprotno, da obstajata $e^2 = e \in S^*$ in $f^2 = f \in S^*$, za katera velja $ef = fe = 0$. Iz zadnjih dveh enakosti dobimo, da je $e \in l_S(f) \cap r_S(f) = \operatorname{ann}_S(f) = 0$, torej je $e = 0$. Protislovje. Sledi, da S res nima ortogonalnih idempotentov. Ker je S končen, po lemi 3.4 sledi, da je S lokalni kolobar. Odtod po lemi 3.2 sledi, da je $S/J(S)$ obseg, ker pa je končen, je res polje. Denimo, da je $|N|$ sodo število. Potem je

$$\deg((1, 0, \dots, 0)) = |l_S(1) \cup r_S(1)| \cdot |N| - 1 = |N| - 1$$

liho število. Protislovje. Število $|N|$ je torej liho. Jasno je $\alpha \geq 1$, saj smo videli, da S vsebuje enoto. Prav tako smo videli, da je $J(S)$ maksimalni ideal. Po drugi strani vemo, da je Jacobsonov radikal maksimalni nilpotentni ideal in da vsebuje vse nil ideale. Sklenemo, da so vsi njegovi elementi nilpotentni. Zgoraj smo že dokazali, da je kvadrat vsakega nilpotentnega elementa enak 0, zato je $s^2 = 0$ za vsak $s \in J(S)$.

Predpostavimo zdaj, da za vsak nenilpotentni element $x \in S$ velja $l_S(x) \neq 0, r_S(x) \neq 0$. Potem S zagotovo ne vsebuje enostranske enote (če bi jo, je to v nasprotju s predpostavko na leve in desne anihilatorje). Dokazali smo že, da za vsak nenilpotentni element $x \in S$ velja $\operatorname{ann}_S(x) = 0$. To implicira, da S ne vsebuje ortogonalnih idempotentov. Če bi namreč v S obstajala ortogonalna idempotenta $e \neq 0 \neq f$, bi iz zveze $ef = fe = 0$ sledilo, da je $f \in \operatorname{ann}_S(e)$, kar je v nasprotju z zgoraj napisanim. Po Wedderburnovem izreku 2.9 sledi, da je $S/J(S) \cong \oplus_{i=1}^r \mathbb{M}_{n_i}(\mathrm{GF}(p_i^{l_i}))$. Če bi bil $r > 1$ ali pa bi bilo katero izmed števil $n_i > 1$, bi kolobar $S/J(S)$ vseboval ortogonalne idempotente, ki bi jih potem lahko dvignili v S (glej del o SBI-kolobarjih). To ne gre, saj smo zgoraj ugotovili, da

S nima ortogonalnih idempotentov. Sledi, da je $S/J(S) \cong \mathrm{GF}(2^k)$. Veljati mora $k \geq 1$, saj bi v primeru $k = 0$ veljalo $S \cong J(S)$, torej bi bil S nilpotentni kolobar. Protislovje. Sledi, da $|S| \geq 2$. Če bi veljalo $|S| = 2$, bi bil $S = \{0, x\}$, kjer je x^2 bodisi 0 bodisi x. Jasno je, da $x^2 \neq 0$, saj bi bil sicer S nilpotentni kolobar, kar je v nasprotju z našo predpostavko. Sledi, da je $x^2 = x$. Potem je $l_S(x) = 0, r_S(x) = 0$. Protislovje. Sklenemo, da mora veljati $|S| \geq 4$, to je $\alpha \geq 2$. Enako kot zgoraj sledi tudi, da za vsak $s \in J(S)$ velja $s^2 = 0$. Pokažimo še, da je $|N|$ liho število. Recimo nasprotno, da je sodo. Po lemi 4.7 sledi, da S vsebuje idempotent e . Potem je

$$\deg((e, 0, \ldots, 0)) = \Big(|l_S(e)| + |r_S(e)| - |\operatorname{ann}_S(e)|\Big) \cdot |N| - 1 =$$

$$\Big(|l_S(e)| + |r_S(e)| - 1\Big) \cdot |N| - 1$$

liho število (ker je e idempotent, ni nilpotent, za take elemente pa smo zgoraj pokazali, da je $\operatorname{ann}_S(\cdot) = 0$). Protislovje. Torej ima N liho število elementov. S tem je izrek dokazan v eno smer.

Pokažimo še obrat. Naj bo $R \cong S \oplus N$, kjer je S lokalni enotski kolobar moči $|S| = 2^\alpha, \alpha \geq 1$ in $s^2 = 0$ za vsak $s \in J(S)$, kolobar N pa je neničelni nilpotentni kolobar lihe moči. Poleg tega naj za vsak $x \in N$ velja $x^2 = 0$. Po lemi 4.8 sta $J(S)$ in N antikomutativna . Naj bo zdaj $x = (s, n) \in R, s \in S, n \in N$. Recimo, da je $s \in J(S)$. Po predpostavki velja $s^2 = 0$. Ker je poleg tega še $n^2 = 0$, je

$$\deg(x) = |\operatorname{ann}_S(s)| \cdot |\operatorname{ann}_N(n)| - |\{0, x\}| = |\operatorname{ann}_S(s)| \cdot |\operatorname{ann}_N(n)| - 2.$$

Ker $0, s \in \operatorname{ann}_S(s)$, je zagotovo $|\operatorname{ann}_S(s)| \geq 2$, torej je $\deg(x)$ sodo število.

Naj bo zdaj še $s \notin J(S)$. Vemo, da je s obrnljiv element v S. Zato je

$$\deg(x) = |\operatorname{ann}_N(n)| - 1.$$

Ker je po predpostavki moč N liho število, je stopnja x sodo število. To pokaže, da je graf $\Gamma(R)$ v tem primeru Eulerjev.

Naj bo zdaj $R \cong S \oplus N$, kjer je S nerazcepni kolobar brez enostranske enote moči $|S| = 2^\alpha, \alpha \geq 2$, poleg tega je $S/J(S)$ polje in $s^2 = 0$ za vsak $s \in J(S)$. Za N velja, da je nilpotentni kolobar lihe moči in za vsak $x \in N$ je $x^2 = 0$. Naj bo $x = (s, n) \in R, s \in S, n \in N$. Naj bo $s \in J(S)$. Potem je $s^2 = 0$ in zato je $0, s \in \operatorname{ann}_S(s)$. Sledi, da je

$$\deg(x) = |l_S(s) \cup r_S(s)| \cdot |\operatorname{ann}_N(n)| - 2$$

sodo število.

Naj bo $s \notin J(S)$. Potem s ni nilpotenten. Na enak način kot v dokazu leme 4.7 skonstruiramo $k \in \mathbb{N}$, da je $s^k = f = f^2 \neq 0$ neničelni idempotent. Ker po predpostavki velja, da S ne vsebuje enostranske enote, je množica

$$(1 - f)S = \{r - fr; r \in S\} \neq 0.$$

Bralca naj ne zmoti zapis $(1 - f)S$ v kolobarju brez enote, saj je to le oznaka za množico. Podobno je

$$S(1 - f) = \{r - rf; r \in S\} \neq 0.$$

Takoj vidimo, da velja $l_S(f) \neq 0$ in $r_S(f) \neq 0$. Recimo, da je $l_S(f) = 0$. Potem za vsak $a \in S^*$ drži zveza $af \neq 0$. To pomeni, da je preslikava $x \mapsto xf$ bijekcija. Obstajati mora element y, da je $f = yf$. Potem za poljuben $t \in S$ velja $tf = tyf$ oziroma $(t - ty)f = 0$, od koder zaključimo $t = ty$. To pomeni, da je t leva enota. Protislovje. Sklenemo, da je res $l_S(f) \neq 0$ in $r_S(f) \neq 0$. Enako pokažemo, da je

$l_S(s) \neq 0$ in $r_S(s) \neq 0$. Predpostavimo, da je $\operatorname{ann}_S(f) \neq 0$ in naj bo $r \in \operatorname{ann}_S(f)^*$. Velja

$$r = r + 0 = r - rf - fr + frf,$$

kar pomeni, da element r pripada množici $(1-f)S(1-f) = \{x - xf - fx + fxf; x \in S\}$, torej $\operatorname{ann}_S(f) \subseteq (1-f)S(1-f)$. Naj bo $y \in (1-f)S(1-f)$. Zapišemo lahko

$$y = y_0 - y_0 f - f y_0 + f y_0 f.$$

Poglejmo produkta yf in fy. Velja

$$fy = fy_0 - fy_0 f - f^2 y_0 + f^2 y_0 f = 0$$

in

$$yf = y_0 f - y_0 f^2 - f y_0 f + f y_0 f^2 = 0,$$

kjer sta oba produkta enaka 0, ker je f idempotent. To pomeni, da $y \in \operatorname{ann}_S(f)$, torej $(1-f)S(1-f) \subseteq \operatorname{ann}_S(f)$. Če združimo obe inkluziji, dobimo zvezo $\operatorname{ann}_S(f) = (1-f)S(1-f)$.

Zapišimo S kot direktno vsoto grup

$$S = fSf + fS(1-f) + (1-f)Sf + (1-f)S(1-f).$$

Pokažimo, da so množice $fS(1-f), (1-f)Sf, (1-f)S(1-f) \subseteq J(S)$. V ta namen si poglejmo preslikavo $\pi : S \to S/J(S)$, podano s predpisom $x \mapsto x + J(S)$. Če vzamemo poljuben element iz množice $fS(1-f)$ in ga z desne pomnožimo z elementom f, dobimo 0. Podobno dobimo 0, če poljuben element iz množice $(1-f)Sf$ ali $(1-f)S(1-f)$ z leve pomnožimo z f. Ugotovili smo, da so elementi v teh množicah vsaj enostranski delitelji niča. Poglejmo, kaj se z njimi zgodi, ko jih preslikamo s π. Ker je po predpostavki $S/J(S)$ polje, je brez deliteljev niča, torej se morajo elementi iz množic $fS(1-f), (1-f)Sf, (1-f)S(1-f)$ slikati v $0 + J(S)$. Zato velja $fS(1-f), (1-f)Sf, (1-f)S(1-f) \subseteq J(S)$. Ker je $\operatorname{ann}_S(f) \subseteq J(S)$, ki je nilpotenten, je tudi $\operatorname{ann}_S(f)$ nilpotenten. Pokažimo še, da je dvostranski ideal. Naj bo $x \in \operatorname{ann}_S(f)$. Če vzamemo $r \in J(S)$, potem je $rx = -xr$ in zato $rx, xr \in \operatorname{ann}_S(f)$. Ker so $fS(1-f), (1-f)Sf, (1-f)S(1-f) \subseteq J(S)$, moramo videti le še, da za $r \in fSf$ velja $rx, xr \in \operatorname{ann}_S(f)$. To velja, ker je $\operatorname{ann}_S(f) = (1-f)S(1-f)$.

Definirajmo sedaj $S_1 = fSf + fS(1-f) + (1-f)Sf$. Trdimo, da je $\operatorname{ann}_S(f) \subseteq \operatorname{ann}_S(S_1)$. Jasno je, da poljuben element iz $\operatorname{ann}_S(f)$ uniči vsak element iz fSf, prav tako pa za vsak $x \in \operatorname{ann}_S(f)$ velja $x \cdot fS(1-f) = 0$. Pokažimo, da je tudi $fS(1-f) \cdot x = 0$. Ker sta $fS(1-f), \operatorname{ann}_S(f) \subseteq J(S)$ zaradi antikomutativnosti $J(S)$ velja $fS(1-f) \cdot x = -x \cdot fS(1-f) = 0$. Podobno velja za množico $(1-f)Sf$, torej je res $\operatorname{ann}_S(f) \subseteq \operatorname{ann}_S(S_1)$.

Poglejmo sedaj $x \in S_1 \cap \operatorname{ann}_S(f)$. Recimo, da je $x \neq 0$. Potem je $x = fx_1 f + (fx_2 - fx_2 f) + (x_3 f - fx_3 f)$ in je vsaj eden izmed elementov $x_i \neq 0$. Potem je $fx = fx_1 f + (fx_2 - fx_2 f)$ in $xf = fx_1 f + (x_3 f - fx_3 f)$ in je vsaj eden izmed teh dveh elementov neničelen. To je v nasprotju s tem, da je $x \in \operatorname{ann}_S(f)$. Sledi, da je $S_1 \cap \operatorname{ann}_S(f) = 0$. Posledično lahko zapišemo $S = S_1 \oplus \operatorname{ann}_S(f)$ (vemo že, da je $\operatorname{ann}_S(f)$ dvostranski ideal, ker pa sta množici $fS(1-f), (1-f)Sf \subseteq J(S)$ in je slednji antikomutativen, je tudi S_1 dvostranski ideal). Ker je $0 \neq f \in S_1$, je $S_1 \neq 0$ in je zgornja dekompozicija v nasprotju z nerazcepnostjo kolobarja S. Sklenemo, da je $\operatorname{ann}_S(f) = 0$. Ker je $\operatorname{ann}_S(s) \subseteq \operatorname{ann}_S(f)$ (velja, ker je za $x \in \operatorname{ann}_S(s)$ tudi $fx = s^k x = s^{k-1}(sx) = 0$), je $\operatorname{ann}_S(s) = 0$. Spet pogledamo stopnjo

$$\deg(x) = |l_S(s) \cup r_S(s)| \cdot |\operatorname{ann}_N(n)| - 1 = (|l_S(s)| + |r_S(s)| - 1) \cdot |\operatorname{ann}_N(n)| - 1.$$

Prvi faktor je liho število, torej je x sode stopnje. Sklenemo, da graf je Eulerjev. $\square$

10.4. **Končni kolobarji z Eulerjevim grafom deliteljev niča.** Če združimo zadnje tri trditve, dobimo naslednji izrek, ki karakterizira vse končne kolobarje z Eulerjevim grafom deliteljev niča.

Izrek 10.5. *Naj bo R končni kolobar, ki ni polje. Potem je graf $\Gamma(R)$ Eulerjev natanko tedaj, ko R zadošča enemu izmed naslednjih pogojev*

(1) $R \cong \oplus_{i=1}^{k} \mathrm{GF}(p_i^{\alpha_i})$*, kjer so p_i liha praštevila in je $k \geq 2$,*
(2) *R je nilpotentni kolobar sode moči in za vsak $x \in R$ velja $x^2 = 0$,*
(3) *$R \cong S \oplus N$, kjer je S lokalni enotski kolobar moči $|S| = 2^\alpha, \alpha \geq 1$ in za vsak $s \in J(S)$ velja $s^2 = 0$, N pa je nilpotentni kolobar lihe moči in za vsak $x \in N$ velja $x^2 = 0$. Lahko je tudi $N = 0$,*
(4) *$R \cong S \oplus N$, kjer je S nerazcepni kolobar moči $|S| = 2^\alpha, \alpha \geq 2$, za vsak $s \in J(S)$ velja $s^2 = 0$, vsaka enostranska enota S je dvostranska enota za S in $S/J(S)$ je polje, N pa je nilpotentni kolobar lihe moči in za vsak $x \in N$ velja $x^2 = 0$. Lahko je tudi $N = 0$.*

Dokaz. Pri dokazu tega izreka je potrebno pravilno zložiti skupaj prejšnje trditve.

Če je R kot v (1), potem po prvi točki trditve 10.3 sledi, da je graf $\Gamma(R)$ Eulerjev, če pa je R kot v (2) točki, je po trditvi 10.1 graf $\Gamma(R)$ Eulerjev. Naj bo zdaj R kot v točki (3). Denimo najprej, da je $N = 0$. Ker R ni polje, mora biti $\alpha \geq 2$. Potem je po drugi točki trditve 10.3 graf $\Gamma(R)$ Eulerjev. Naj bo zdaj še $N \neq 0$. Potem je po prvi točki trditve 10.4 graf $\Gamma(R)$ Eulerjev. Ostane še primer, ko je R kot v (4). Denimo najprej, da S nima enostranske enote. Potem je po drugi točki trditve 10.4 graf $\Gamma(R)$ Eulerjev. Če pa S ima enostransko enoto, ima po predpostavki tudi dvostransko enoto. Ker je $S/J(S)$ polje, je $J(S)$ edini maksimalni levi ideal in zato je S lokalni kolobar. Če je še $N = 0$, je $R = S$ enotski lokalni kolobar in zato je po drugi točki trditve 10.3 graf $\Gamma(R)$ Eulerjev. Če pa je $N \neq 0$, je $\Gamma(R)$ po prvi točki trditve 10.4 Eulerjev graf.

Pokažimo še obrat. Če je R nilpotentni kolobar z Eulerjevim grafom deliteljev niča, je R tak kot v (2) po trditvi 10.1. Če je R enotski kolobar z Eulerjevim grafom deliteljev niča, je po trditvi 10.3 R tak kot v (1) ali (3), pri čemer je $N = 0$ in $\alpha \geq 2$. Če pa je R nenilpotentni kolobar brez enote z Eulerjevim grafom deliteljev niča, je R po trditvi 10.4 bodisi tak kot v (3), pri čemer je $N \neq 0$ (če R zadošča prvi točki omenjene trditve) bodisi kot v (4), pri čemer S nima enostranske enote (če R zadošča drugi točki omenjene trditve). $\square$

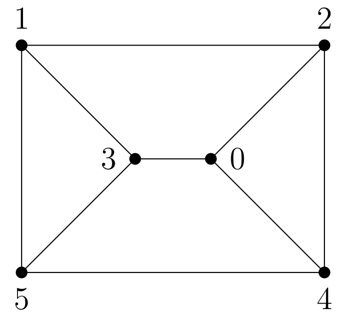
Opomba 10.6. Če je kolobar S tak, da ima dvostransko enoto, potem iz pogoja, da je $S/J(S)$ polje, sledi, da je $J(S)$ enolično določeni maksimalni levi ideal, torej je S lokalni kolobar. Točka (4) zgornjega izreka 10.5 je tedaj poseben primer točke (3).

11. Totalni grafi

Naj bo R komutativni kolobar. S $T(R)$ označimo njegov *totalni graf.* Ta ima za vozlišča vse elemente kolobarja R, dve različni vozlišči $x, y \in R$ pa sta povezani natanko tedaj, ko je $x + y \in Z(R)$. Ta graf je zanimiv, ker poveže obe operaciji v kolobarju (graf deliteljev niča je vezan le na množenje) in tako iz njega lahko dobimo več informacij o samem kolobarju.

Primer 11.1. Naj bo R cel kolobar. Potem je graf $T(R)$ disjunktna unija podgrafov K_1 in K_2. To velja, ker je vsak $x \in R$ povezan le z elementom $-x$. Tako v primeru, ko je $x \neq -x$, dobimo K_2, sicer pa K_1 .

Primer 11.2. Poglejmo si še totalni graf kolobarja $\mathbb{Z}_6 = \mathbb{Z}_2 \times \mathbb{Z}_3$. Vemo, da je $Z(\mathbb{Z}_6) = \{0, 2, 3, 4\}$. Opazimo še, da R ni lokalni kolobar. Graf je na sliki 2.



Slika 2. Graf $T(\mathbb{Z}_6)$.

Totalni graf je v primeru, ko R ni lokalni kolobar, povezan. To nam pove naslednja lema.

Lema 11.3. *Naj bo R artinski komutativni enotski kolobar, ki ni lokalen. Potem je $T(R)$ povezan graf in njegov premer je* $\operatorname{diam}(T(R)) = 2$.

Dokaz. Po [2, Izrek 8.7] lahko kolobar R zapišemo kot $R = R_1 \times \cdots \times R_n$, kjer so R_i artinski lokalni kolobarji in je $n \geq 2$, ker R ni lokalen. Naj bosta $x = (x_1, \ldots, x_n)$ in $y = (y_1, \ldots, y_n)$ poljubni vozlišči grafa $T(R)$. Poiskati moramo pot dolžine največ dve med njima. Označimo z $z = (-x_1, -y_2, 0, \ldots, 0)$. Potem je $x + z = (0, x_2 - y_2, x_3, \ldots, x_n) \in Z(R)$ in $z + y = (y_1 - x_1, 0, y_3, \ldots, y_n) \in Z(R)$. Iskana pot je torej $x - z - y$. Jasno je, da med $(0, \ldots, 0)$ in $(1, \ldots, 1)$ ni krajše poti. $\square$

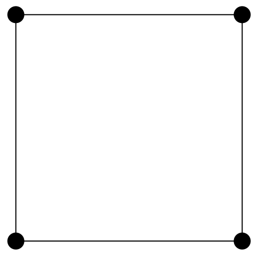
Poglejmo si sedaj, kdaj v totalnem grafu lahko najdemo cikel lihe dolžine.

Lema 11.4. *Naj bo R artinski komutativni enotski kolobar, ki ni lokalen. Če $R \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$, potem graf $T(R)$ vsebuje tricikel.*

Dokaz. Ker je R artinski komutativni enotski kolobar, ga lahko po [2, Izrek 8.7] zapišemo kot $R = R_1 \times \cdots \times R_n$, kjer so R_i artinski lokalni kolobarji. Pri tem je še $n \geq 2$, ker R ni lokalen. Denimo najprej, da je $n \geq 3$. Ker je R enotski, so tudi vsi R_i enotski kolobarji. Označimo z $x_0 = (0, \ldots, 0), x_1 = (1, 0, \ldots, 0), x_2 = (0, 1, 0, \ldots, 0)$. Očitno je $x_0x_1, x_1x_2, x_2x_0 \in E(T(R))$, torej graf $T(R)$ vsebuje tricikel. Naj bo sedaj $n = 2$. Velja torej $R = R_1 \times R_2$. Ker je $R \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$, ima vsaj eden izmed kolobarjev R_1, R_2 vsaj tri elemente. Predpostavimo lahko, da je $|R_1| \geq 3$. Potem v $R_1 \setminus \{0\}$ obstajata dva različna elementa $a \neq b$. Označimo spet z $x_0 = (0, 0), x_1 = (a, 0), x_2 = (b, 0)$. Spet velja $x_0x_1, x_1x_2, x_2x_0 \in E(T(R))$, saj so $x_0 + x_1, x_1 + x_2, x_2 + x_0 \in Z(R)$. Našli smo tricikel v $T(R)$, s čimer smo dokazali lemo. $\square$

Opomba 11.5. Graf $T(\mathbb{Z}_2 \times \mathbb{Z}_2)$ ne vsebuje tricikla. Glej sliko 3.

Lema 11.6. *Graf je dvodelen natanko tedaj, ko ne vsebuje ciklov lihe dolžine.*



SLIKA 3. Graf $T(\mathbb{Z}_2 \times \mathbb{Z}_2)$.

Dokaz. Glej [6, Trditev 1.6.1]. $\square$

Posledica 11.7. *Kolobar $R = \mathbb{Z}_2 \times \mathbb{Z}_2$ je edini artinski enotski komutativni kolobar, ki ni lokalen in ima dvodelen totalni graf $T(R)$.*

Prav tako znamo natančno določiti ožino (velikost najmanjšega cikla v grafu) artinskega komutativnega enotskega kolobarja, ki ni lokalen.

Posledica 11.8. *Naj bo R artinski komutativni enotski kolobar, ki ni lokalen. Potem je njegova ožina enaka 4, če je $R \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, in 3 sicer.*

Lema 11.9. *Naj bo R končni komutativni enotski kolobar. Potem je $2 \in Z(R)$ natanko tedaj, ko 2 deli $|R|$.*

Dokaz. Naj bo najprej R lokalni kolobar. Če 2 deli $|R|$, je po [16, Posledica 2.4] $|R| = 2^n$. Po lemi 4.13 je $\mathrm{char}(R) = 2^k, k > 1$, torej je $2 \cdot 2^{k-1} = 0$ in posledično je $2 \in Z(R)$. Dokažimo še obrat. Naj bo $2 \in Z(R)$. Obstaja $x \in R \setminus 0$, da je $2x = 0$. Če je $n = \mathrm{char}(R)$, potem mora 2 deliti n, sicer $nx \neq 0$. Po lemi 4.13 pa n deli $|R|$ in ker je relacija deljivosti tranzitivna, 2 deli $|R|$.

Če R ni lokalen, ga po [2, Izrek 8.7] lahko zapišemo kot $R = R_1 \times \cdots \times R_n$, kjer so R_i lokalni kolobarji. Če 2 deli $|R|$, mora biti vsaj eden izmed kolobarjev R_i sode moči in ker je lokalen, mora biti moči 2^k. Predpostavimo lahko, da je to R_1. Po prvem delu sledi, da je $2 \in Z(R_1)$ in posledično je $2 \in Z(R)$. Če pa je $2 \in Z(R)$, obstaja indeks i, da je $2 \in Z(R_i)$. Po prvem delu sledi, da 2 deli $|R_i|$. Ker je $|R| = \prod_{i=1}^{n} |R_i|$, sledi, da 2 deli $|R|$. $\square$

Poglejmo si zdaj še totalne grafe lokalnih kolobarjev. Za razliko od prej ti niso povezani.

Izrek 11.10. *Naj bo R končni lokalni enotski kolobar. Graf $T(R)$ ni povezan. Če je karakteristika R enaka $\mathrm{char}(R) = 2^k$, je $T(R)$ izomorfen disjunktni uniji $|R/Z(R)|$ kopij grafa $K_{|Z(R)|}$, sicer pa je $T(R)$ izomorfen disjunktni uniji grafa $K_{|Z(R)|}$ in $\frac{1}{2}(|R/Z(R)| - 1)$ kopij grafa $K_{|Z(R)|,|Z(R)|}$.*

Dokaz. Po lemi 4.12 je $x + y \in Z(R)$ natanko tedaj, ko je $(x + J(R)) + (y + J(R)) \in Z(R/J(R))$. Ker je R lokalni kolobar, je $J(R) = Z(R)$ edini maksimalni ideal. Posledično je $F = R/Z(R) = R/J(R)$ polje. Ker ta nima pravih deliteljev niča, sta dve vozlišči x in y povezani v $T(F)$ natanko tedaj, ko je $x = -y$. Če je $\mathrm{char}(R) = 2^k$, potem je $\mathrm{char}(F) = 2$. To pomeni, da je za vsak element $x = -x$, torej je $T(F)$ sestavljen iz $|F| = |R/Z(R)|$ kopij K_1. Sledi, da $T(R)$ ni povezan.

Če $\mathrm{char}(R) \neq 2^k$, potem $2 \nmid \mathrm{char}(F)$, saj je zaradi lokalnosti kolobarja $\mathrm{char}(R) = p^k$, kjer je p liho praštevilo. Zato je $x \neq -x$ za vsak $x \neq 0$. Sledi, da ima $T(F)$ eno komponenento K_1 za vozlišče 0 in $\frac{1}{2}(|F| - 1)$ komponent K_2 za ostale pare vozlišč x in $-x$. Spet sledi, da $T(R)$ ni povezan.

Pokažimo še, da $T(R)$ res vsebuje prave komponente. Ko je $\mathrm{char}(R) = 2^k$, moramo videti, da so vsi elementi iz odseka povezani med sabo. Vzemimo poljuben odsek $x + Z(R)$. Naj bosta $x + y_1$ in $x + y_2$ poljubna elementa iz tega odseka. Ker je $x = -x$, je $2x = 0$ in ker je R lokalni kolobar, je $Z(R) = J(R)$ ideal in zato zaprt za seštevanje. Sledi $(x + y_1) + (x + y_2) = 2x + y_1 + y_2 = y_1 + y_2 \in J(R) = Z(R)$. To implicira, da vsaki kopiji K_1 v $T(F)$ pripada kopija $K_{|Z(R)|}$ v $T(R)$. Sledi, da je $T(R)$ v tem primeru res disjunktna unija $|R/Z(R)|$ kopij $K_{|Z(R)|}$.

Naj bo še $\mathrm{char}(R) \neq 2^k$. Enako kot zgoraj vidimo, da kopiji K_1, ki pripada vozlišču 0 v $T(F)$ v grafu $T(R)$ pripada graf $K_{|Z(R)|}$. Pokažimo še, da kopiji grafa K_2, ki pripada paru vozlišč x in $-x$ iz grafa $T(F)$, v grafu $T(R)$ pripada graf $K_{|Z(R)|,|Z(R)|}$. Naj bo $x + y_1 \in x + Z(R)$ in $-x + y_2 \in -x + Z(R)$, kjer je $x \neq 0$. Potem je $(x + y_1) + (-x + y_2) = y_1 + y_2 \in Z(R)$, ker je $Z(R) = J(R)$ zaprt za seštevanje. Če pa $x \notin Z(R)$ in sta $x + y_i \in x + Z(R), i = 1, 2$, potem je $(x + y_1) + (x + y_2) = 2x + (y_1 + y_2) \in 2x + Z(R) \not\subseteq Z(R)$, saj $x \notin Z(R)$ in karakteristika R ni sodo število. Na podoben način vidimo, da tudi elementi, ki pripadajo odseku $-x + Z(R)$ v $T(R)$ niso povezani med sabo. Sledi, da vsaki kopiji K_2 iz grafa $T(F)$ v grafu $T(R)$ pripada kopija $K_{|Z(R)|,|Z(R)|}$. □

S pomočjo zgornjega izreka lahko karakteriziramo ožino totalnega grafa lokalnega kolobarja.

Posledica 11.11. *Naj bo R končni lokalni enotski kolobar. Če je $|Z(R)| \geq 3$, je ožina $gr(T(R)) = 3$, sicer je ožina $gr(T(R)) = \infty$.*

Dokaz. To sledi iz izreka 11.10. Če je $\mathrm{char}(R) = 2^k$, potem graf $T(R)$ vsebuje kopijo grafa $K_{|Z(R)|}$, ki v primeru, ko je $|Z(R)| \geq 3$, vsebuje tricikel. Če pa je $|Z(R)| \in \{1, 2\}$, potem je $T(R)$ sestavljen iz samih disjunktnih kopij grafov K_1 ali grafov K_2, ki sploh ne vsebujejo cikla. V tem primeru je $\mathrm{gr}(T(R)) = \infty$. Podobno je v primeru, ko $\mathrm{char}(R) \neq 2^k$ in $|Z(R)| \geq 3$, spet $\mathrm{gr}(T(R)) = 3$, saj $T(R)$ vsebuje kopijo $K_{Z(R)}$. Denimo torej, da $\mathrm{char}(R) \neq 2^k$ in je $|Z(R)| \leq 2$. Poglejmo najprej primer, ko je $|Z(R)| = 1$. Tedaj je $T(R)$ disjunktna unija podgrafa K_1 in $\frac{1}{2}(|R| - 1)$ kopij grafa $K_{1,1} = K_2$. Nobeden izmed teh grafov ne vsebuje cikla, torej je $\mathrm{gr}(T(R)) = \infty$. Naj bo zdaj še $|Z(R)| = 2$. Ker smo v lokalnem primeru, je $Z(R) = J(R)$ in ker je to podgrupa, deli moč kolobarja R. Po [16, Posledica 2.4] je moč lokalnega kolobarja praštevilo. Sledi, da je $|R| = 2^n$. Ker po lemi 4.13 karakteristika deli moč kolobarja, mora biti $\mathrm{char}(R) = 2^k$. Protislovje. Sledi, da tak kolobar sploh ne obstaja. □

Poglejmo si regularnost totalnega grafa. V pomoč nam bosta naslednji lemi.

Lema 11.12. *Naj bo R končni komutativni kolobar. Naj bo x poljubno vozlišče grafa $T(R)$. Če velja $x + x = 2x \notin Z(R)$, je stopnja x enaka $\deg(x) = |Z(R)|$, sicer pa je $\deg(x) = |Z(R)| - 1$. Velja še, da je $2 \in Z(R)$ natanko tedaj, ko je $T(R)$ $(|Z(R)| - 1)$-regularen graf.*

Dokaz. Naj bo x poljubno vozlišče grafa $T(R)$. Za vsak $z \in Z(R)$ lahko definiramo element $a = z - x \in R$. Potem velja $a + x = z \in Z(R)$. To pomeni, da je x povezan z a, razen če je $x = a$. Če je torej x tak, da je $x + x = 2x \in Z(R)$, je $\deg(x) = |Z(R)| - 1$, ker x ni povezan sam s sabo. Če pa $x + x = 2x \notin Z(R)$, je za vsak $z \in Z(R)$ element $z - x \neq x$. Sledi $\deg(x) = |Z(R)|$.

Dokažimo še drugi del leme. Denimo najprej, da $2 \notin Z(R)$. Vemo, da je vozlišče 0 povezano le z neničelnimi elementi iz $Z(R)$, torej $\deg(0) = |Z(R)| - 1$. Potem je $\deg(1) = |Z(R)| \neq |Z(R)| - 1 = \deg(0)$ in posledično graf $T(R)$ ni regularen.

Dokažimo še obrat. Denimo, da $2 \in Z(R)$. Potem je zaradi komutativnosti za vsak $x \in R$ tudi $2x \in Z(R)$. Po prvem delu leme sledi, da je za vsak $x \in R$ stopnja $\deg(x) = |Z(R)| - 1$, kar ravno pomeni, da je $T(R)$ res $(|Z(R)| - 1)$-regularen graf. $\square$

Lema 11.13. *Naj bo R končni komutativni enotski kolobar. Če je $|R|$ liho število, je $|U(R)|$ sodo število.*

Dokaz. Naj bo najprej R lokalni kolobar. Po [16, Posledica 2.4] je $|R| = p^n$, kjer je p praštevilo. Če je $|R|$ liho število, je $p \neq 2$. Ker je R končen, je vsak njegov element bodisi obrnljiv bodisi delitelj niča. Vsi delitelji niča so torej ravno v edinem maksimalnem idealu $J(R)$, ki je moči $p^k, k < n$. Ker je $U(R) = R \setminus Z(R) = R \setminus J(R)$, je $|U(R)| = |R| - |J(R)| = p^n - p^k = p^k(p^{n-k} - 1)$. Ker je $n > k$, je p^{n-k} liho število in posledično je $|U(R)|$ sodo število. Če pa R ni lokalen, ga lahko zapišemo kot $R = R_1 \times \cdots \times R_n$, kjer so R_i končni lokalni kolobarji. Ker je $|R|$ liho število, je za vsak i tudi $|R_i|$ liho število. Po prvem delu je tako $|U(R_i)|$ sodo število. Ker pa je $U(R) = U(R_1) \times \cdots \times U(R_n)$, je $|U(R)| = \prod_{i=1}^{n} |U(R_i)|$ produkt sodih števil in zato sodo število. $\square$

S pomočjo teh ugotovitev dobimo naslednji izrek.

Izrek 11.14. *Naj bo R končni komutativni enotski kolobar. Tedaj velja:*

(1) *če je $|R|$ sodo število, je $T(R)$ $(|Z(R)| - 1)$-regularen graf,*
(2) *če je $|R|$ liho število, je za $x \in Z(R)$ stopnja $\deg(x) = |Z(R)| - 1$ in za $x \in U(R)$ je stopnja $\deg(x) = |Z(R)|$.*

Dokaz. Po lemi 11.12 je $T(R)$ $(|Z(R)| - 1)$ regularen graf natanko tedaj, ko je $2 \in Z(R)$, kar je po lemi 11.9 res natanko tedaj, ko je $|R|$ sodo število. Če je $|R|$ liho število, potem po lemi 11.9 sledi, da $2 \notin Z(R)$. Če je $x \in U(R)$, potem tudi $2x \notin Z(R)$. Po lemi 11.12 je $\deg(x) = |Z(R)|$. Naj bo $x \in Z(R)$. Obstaja $y \in R \setminus \{0\}$, da je $xy = 0$. Če je $2x \neq 0$, je $(2x)y = 2(xy) = 0$ in je $2x \in Z(R)$, zato je po lemi 11.12 $\deg(x) = |Z(R)| - 1$. Če pa je $2x = 0$, zaključimo, da je $x = 0$, saj po predpostavki velja $2 \notin Z(R)$. Element $x = 0$ je povezan z vsemi delitelji niča razen z 0, torej je tudi v tem primeru $\deg(x) = \deg(0) = |Z(R)| - 1$. $\square$

12. Ravninskost totalnega grafa

Poglejmo najprej primer, ko je R cel kolobar. Potem je vozlišče x povezano edino z vozliščem $-x$ in še to le v primeru, ko je $x \neq -x$. Sledi, da je graf $T(R)$ disjunktna unija podgrafov K_1 in K_2. Očitno je torej ravninski. V posebnem to seveda velja za vsa polja. Omejimo se na končne komutativne enotske kolobarje. Najprej bomo pogledali primer, ko imamo lokalni kolobar, nato pa še primer, ko je R splošni končni komutativni enotski kolobar. Pri tem si bomo pomagali z naslednjim izrekom.

Izrek 12.1. *(Wagner) Graf je ravninski natanko tedaj, ko nima minorja izomorfnega K_5 ali $K_{3,3}$.*

Dokaz tega izreka se nahaja v [6, Izrek 4.2.9]. Pri tem pripomnimo, da v primeru, ko graf vsebuje podgraf izomorfen K_l, kjer je $l \geq 5$, vsebuje tudi minor K_5.

12.1. **Lokalni kolobarji.** Naj bo R končni komutativni lokalni enotski kolobar. Po [16, Posledica 2.4] je $|R| = p^n$, kjer je p praštevilo in $n \geq 1$. Po lemi 4.13 in izreku 11.10 je v primeru, ko je $p = 2$, graf $T(R)$ izomorfen disjunktni uniji $|R/Z(R)|$ kopij $K_{|Z(R)|}$, sicer pa je $T(R)$ izomorfen disjunktni uniji grafa $K_{|Z(R)|}$ in $\frac{1}{2}(|R/Z(R)| - 1)$ kopij grafa $K_{|Z(R)|,|Z(R)|}$. Predpostavimo lahko, da R ni polje, saj smo zgoraj videli, da je totalni graf poljubnega polja ravninski. Označimo z m še edini maksimalni ideal kolobarja R. Ker je R lokalen, je $m = J(R) = Z(R)$. Ker pa R ni polje in je $|R| = p^n, n \geq 2$, je $|m| = p^k, 1 \leq k < n$. Ločimo nekaj primerov glede na to, kakšen je p. Če je R kolobar moči p^n, kjer je praštevilo $p \geq 5$, potem je $|Z(R)| = |m| \geq 5$. Sledi, da $T(R)$ vsebuje minor K_5 in zato ni ravninski. Ostaneta nam torej možnosti $p = 3$ ali $p = 2$. Najprej si poglejmo primer, ko je $p = 3$. Tedaj je $|R| = 3^n, n \geq 2$ in $|m| = 3^k$, kjer je $1 \leq k \leq n-1$, ker R ni polje in ima enoto. Sledi, da je $|R/Z(R)| \geq 3$ in zato $T(R)$ vsebuje vsaj eno kopijo $K_{|Z(R)|,|Z(R)|}$. Ker je $Z(R) = m$ in je $|m| \geq 3$, graf $T(R)$ vsebuje podgraf $K_{3,3}$, ki ni ravninski. Sledi, da tudi $T(R)$ v tem primeru ni ravninski. Obravnavajmo še primer, ko je $p = 2$. Tedaj je $|R| = 2^n, n \geq 2$ in $|m| = 2^k, 1 \leq k \leq n-1$. Če je $k \geq 3$, potem graf $T(R)$ vsebuje minor K_5 in ni ravniski. Če pa je $k = 2$, je graf $T(R)$ izomorfen disjunktni uniji 2^{n-2} kopij $K_{2^2} = K_4$ (seveda mora biti $n \geq 3$). V tem primeru je $T(R)$ ravninski. Če pa je $k = 1$, je $T(R)$ izomorfen disjunktni uniji 2^{n-1} kopij grafa K_2. Tudi v tem primeru je $T(R)$ ravninski.

Zgornje ugotovitve lahko strnemo v naslednjo trditev.

Trditev 12.2. *Naj bo R končni komutativni lokalni enotski kolobar. Potem je $T(R)$ ravninski graf natanko tedaj, ko je bodisi R polje bodisi je R lokalni kolobar moči $|R| = 2^n, n \geq 2$ z edinim maksimalnim idealom m moči $|m| = 2$ ali $|m| = 4$.*

12.2. **Nelokalni kolobarji.** Vemo že, da vsak končni komutativni enotski kolobar R lahko zapišemo kot $R = R_1 \times \cdots \times R_n$, kjer so R_i lokalni kolobarji (glej [2, Izrek 8.7]). Določimo sedaj minimalne praideale v kolobarju R. Če je R tak kot zgoraj, vpeljimo še oznako $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, kjer je enica na i-tem mestu. Element e_i ima torej na vseh komponentah ničle, le na i-ti ima enico. Od tod jasno sledi, da za množico $\{e_i\}_{i=1}^n$ velja $e_i \cdot e_j = \delta_{ij}$. Začnimo s prvo lemo.

Lema 12.3. *Naj bo $R = R_1 \times \cdots \times R_n, n \geq 2$, končni komutativni enotski kolobar in naj bodo R_i končna polja. Potem je množica $\{P_i\}_{i=1}^n$, kjer je $P_i = R_1 \times \cdots \times R_{i-1} \times \{0\} \times R_{i+1} \times \cdots \times R_n$, ravno množica vseh minimalnih praidealov kolobarja R.*

Dokaz. Za vsak praideal P obstaja tak indeks i, da $e_i \notin P$, sicer je $P = R$ in P sploh ni pravi ideal. Označimo s Q_i minimalni praideal, ki ne vsebuje elementa e_i. Množica Q_i zagotovo vsebuje 0. Ker je za vsak $j \neq i$ produkt $e_j e_i = 0 \in Q_i$ in ker je Q_i praideal, za katerega velja $e_i \notin Q_i$, mora Q_i vsebovati vse $e_j, j \neq i$. Ker je Q_i ideal, mora biti zaprt za seštevanje in množenje z R in zato je $R_1 \times \cdots \times R_{i-1} \times \{0\} \times R_{i+1} \times \cdots \times R_n \subseteq Q_i$. Ta množica je očitno ideal. Je tudi praideal, ker je R_i polje. Po konstrukciji je minimalni praideal, ki ne vsebuje e_i. Dobili smo ravno P_i.

Pokažimo še, da mora vsak praideal vsebovati vse razen enega izmed elementov e_i. Denimo nasprotno, da je P neki praideal, ki ne vsebuje elementov $e_i, e_j, i \neq j$. Velja $e_i e_j = 0 \in P$, vendar $e_i, e_j \notin P$. Sledi, da P ni praideal. Protislovje. Od tod sledi, da nam zgornja konstrukcija res da vse minimalne praideale, torej je množica vseh minimalnih praidealov res enaka $\{P_i\}_{i=1}^n$. □

Poglejmo si, kaj se zgodi, če kateri izmed faktorjev R_i ni polje.

Lema 12.4. *Naj bo R končni komutativni enotski kolobar, ki ni lokalen. Zapišemo ga lahko kot $R = R_1 \times \cdots \times R_n, n \geq 2$, kjer so R_i lokalni kolobarji. Označimo z m_i edini maksimalni ideal kolobarja R_i. Potem je množica $\{P_i\}_{i=1}^n$, kjer je $P_i = R_1 \times \cdots \times R_{i-1} \times m_i \times R_{i+1} \times \cdots \times R_n$, ravno množica vseh minimalnih praidealov kolobarja R.*

Dokaz. Če so vsi faktorji R_i polja, potem trditev sledi po prejšnji lemi 12.3. Denimo torej, da so $R_1, \ldots, R_k, k \leq n$, lokalni kolobarji, ki niso polja. Lema 12.3 nam pove, da so minimalni praideali, ki ne vsebujejo elementov $e_{k+1}, \ldots, e_n$, prave oblike. Naj bo $1 \leq i \leq k$. Naj bo Q_i minimalni praideal, ki ne vsebuje e_i. Enako kot v lemi 12.3 vidimo, da mora biti $R_1 \times \cdots \times R_{i-1} \times \{0\} \times R_{i+1} \times \cdots \times R_n \subseteq Q_i$. Ta množica ne more biti praideal, saj obstajata $x_i, y_i \in m_i \setminus \{0\}$, da je $x_i y_i = 0$. Množica Q_i bo praideal natanko tedaj, ko bo na mestu i nastopal neki praideal. Za vsak praideal S_i v R_i, je kolobar R_i/S_i cel. Ker je R_i/S_i končen, je polje. To pomeni, da je vsak praideal kolobarja R_i maksimalen. Ker je R_i lokalen, ima enolično določen maksimalni ideal m_i in to je edini praideal kolobarja R_i. Potem je $Q_i = R_1 \times \cdots \times R_{i-1} \times m_i \times R_{i+1} \cdots \times R_n = P_i$. Enako kot zgoraj premislimo še, da so to res vsi minimalni praideali. □

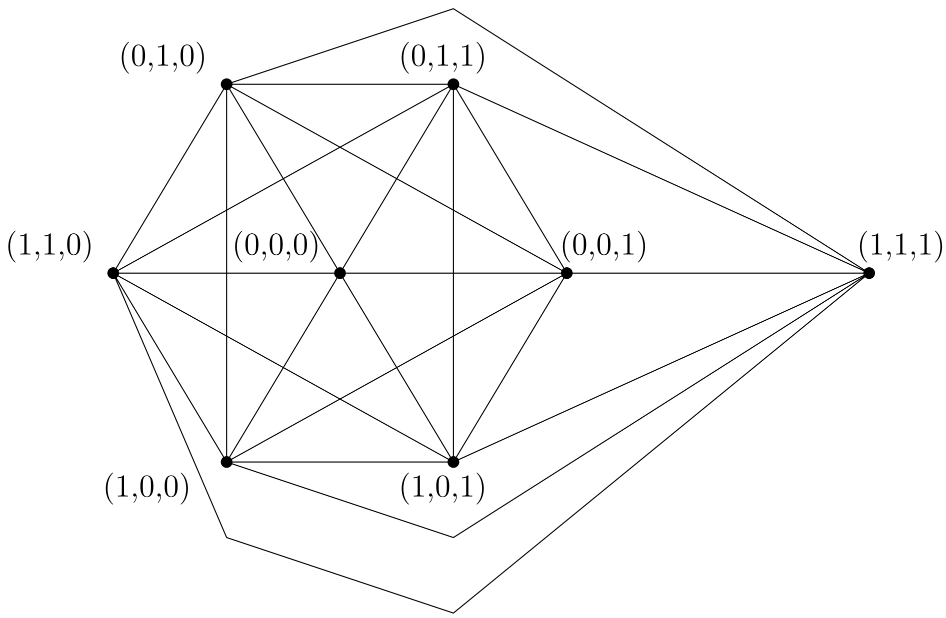
Sedaj bomo zgoraj ugotovljeno s pridom uporabili. Po [2, Trditev 4.7] lahko množico vseh deliteljev niča zapišemo kot unijo minimalnih praidealov kolobarja R.

Posledica 12.5. *Naj bo R končni komutativni enotski kolobar, ki ni lokalen. Zapišemo ga lahko kot $R = R_1 \times \cdots \times R_n, n \geq 2$, kjer so R_i lokalni kolobarji (*[2, Izrek 8.7]*). Označimo z m_i edini maksimalni ideal kolobarja R_i. Potem je $Z(R) = \cup_{i=1}^n P_i$, kjer je $P_i = R_1 \times \cdots \times R_{i-1} \times m_i \times R_{i+1} \times \cdots \times R_n$.*

Naj bo zdaj P_i minimalni praideal kolobarja R. Potem je $P_i \subseteq Z(R)$. Ker je $P_i + P_i \subseteq P_i \subseteq Z(R)$, vsakemu minimalnemu praidealu v totalnem grafu $T(R)$ pripada poln podgraf $K_{|P_i|}$. Pri tem velja, da je $|P_i| = |R_1| \cdots |R_{i-1}| \cdot |m_i| \cdot |R_{i+1}| \cdots |R_n|$. S pomočjo tega kriterija bomo obravnavali ravninskost totalnega grafa. Ločimo nekaj primerov.

(1) Naj bo $n \geq 4$. Ker je $|R_i| \geq 2$, za minimalni praideal P_1 zagotovo velja $|P_1| = |m_1| \cdot \prod_{i=2}^n |R_i| \geq \prod_{i=2}^n 2 = 2^{n-1} \geq 2^3 = 8$, zato $T(R)$ v tem primeru vsebuje minor K_5 in posledično ni ravninski.

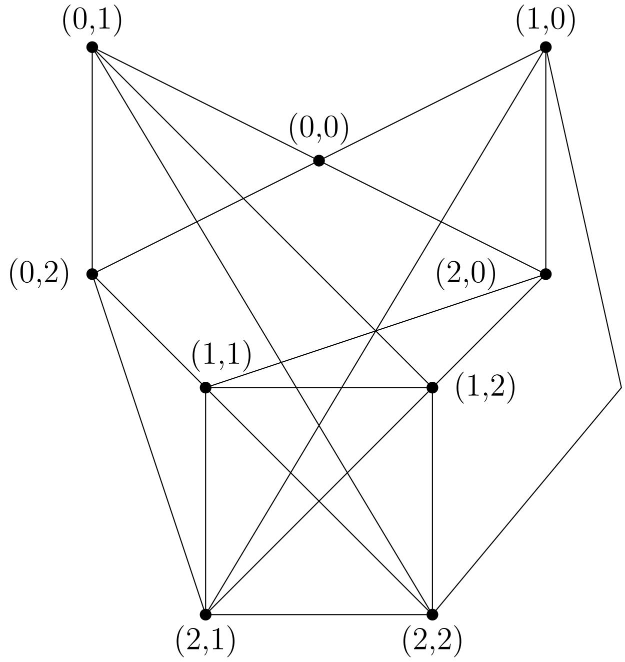
(2) Naj bo $n = 3$. V tem primeru je R oblike $R = R_1 \times R_2 \times R_3$, kjer je R_i lokalni kolobar moči $p_i^{k_i}$. Predpostavimo lahko, da je $2 \leq p_1 \leq p_2 \leq p_3$. Poglejmo najprej primer, ko sta $p_2, p_3 > 2$. Moč minimalnega praideala $P_1 = m_1 \times R_2 \times R_3$ lahko ocenimo kot $|P_1| = |m_1||R_2||R_3| > 4$, torej $T(R)$ v tem primeru zagotovo vsebuje minor K_5 in zato ni ravninski. Oglejmo si še možnost, ko je $p_2 = 2$. Ker je $p_1 \leq p_2$, je tudi $p_1 = 2$. Če je pri tem $p_3 \geq 3$, lahko ocenimo moč minimalnega praideala P_1 kot $|P_1| = |m_1||R_2||R_3| \geq 2 \cdot 3 = 6$, zato vsebuje minor K_5 in posledično ni ravninski. Ostane še primer, ko je $p_1 = p_2 = p_3 = 2$. Spet lahko predpostavimo, da je $1 \leq k_1 \leq k_2 \leq k_3$. Če je $k_3 \geq 2$, je možno moč minimalnega praideala oceniti kot $|P_1| = |m_1||R_2||R_3| \geq 2 \cdot 2^2 = 8$ in zato $T(R)$ spet vsebuje minor K_5. Posledično tudi v tem primeru ni ravninski. Če pa je $k_3 = 1$, zaradi predpostavke $1 \leq k_1 \leq k_2 \leq k_3$ sledi $k_1 = k_2 = k_3 = 1$. Kolobar R je v tem primeru enak $R = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Njegov graf je na sliki 4. Če v njem skrčimo povezave $(1,1,0) - (0,0,0), (1,0,0) - (0,0,0), (1,0,1) - (0,0,0)$, dobimo minor K_5 in zato $T(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)$ ravno tako ni ravninski graf.



Slika 4. Graf $T(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)$.

(3) Naj bo $n = 2$. V tem primeru kolobar R lahko zapišemo kot $R = R_1 \times R_2$, kjer sta R_1 in R_2 lokalna kolobarja. Njuni moči sta enaki $|R_1| = p_1^{k_1}$ in $|R_2| = p_2^{k_2}$, kjer sta p_1 in p_2 praštevili in $k_1, k_2 \geq 1$. Predpostavimo, da je $2 \leq p_1 \leq p_2$. Če je $p_2 \geq 5$, lahko moč minimalnega praideala P_1 navzdol ocenimo s $|P_1| = |m_1||R_2| \geq 5$, kar pomeni, da $T(R)$ vsebuje minor K_5 in zato ni ravninski. Poglejmo primer, ko je $p_2 < 5$. Potem je bodisi $p_2 = 2$ bodisi je $p_2 = 3$. Začnimo s primerom $p_2 = 3$. Po predpostavki je $2 \leq p_1 \leq 3 = p_2$. Če je $p_1 = 3$, predpostavimo, da je $1 \leq k_1 \leq k_2$. Če je $k_2 \geq 2$, ocenimo moč minimalnega praideala P_1 kot $|P_1| = |m_1||R_2| \geq 3^2 = 9$. Graf $T(R)$ torej vsebuje minor K_5 in zato ni ravninski. Če pa je $k_2 = 1$, je tudi $k_1 = 1$ in imamo kolobar $R = \mathbb{Z}_3 \times \mathbb{Z}_3$. Njegov graf je na sliki 5. Če v njem skrčimo povezave $(0,2)-(0,0), (0,1)-(0,0), (1,0)-(0,0), (2,0)-(0,0)$, odstranimo zanke in večkratne povezave, dobimo ravno graf K_5. Sledi, da $T(R)$ v tem primeru ni ravninski.

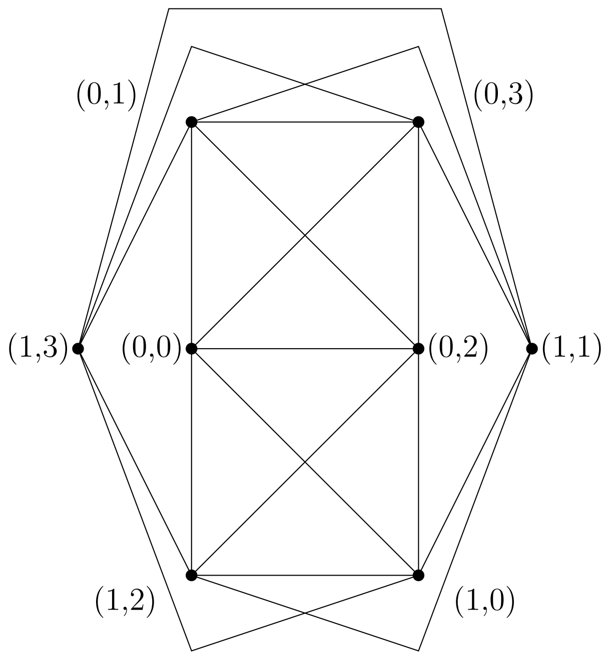
Naj bo zdaj $p_2 = 3$ in $p_1 = 2$. Če je $k_2 \geq 2$, ocenimo moč minimalnega praideala P_1 kot $|P_1| = |m_1||R_2| \geq 3^2 = 9$. Graf v tem primeru vsebuje minor K_5 in zato ni ravninski. Predpostavimo, da je $k_2 = 1$. Če je $k_1 \geq 3$, potem je $|P_2| = |R_1||m_2| \geq 2^3 = 8$ in graf $T(R)$ spet ni ravninski, ker v njem lahko najdemo minor K_5. Ostal je še primer, ko je $k_1 = 1$ ali $k_1 = 2$. Če je $k_1 = 1$, je $R = \mathbb{Z}_2 \times \mathbb{Z}_3$. Graf $T(\mathbb{Z}_2 \times \mathbb{Z}_3)$ je ravninski, glej sliko 2. Če pa je $k_1 = 2$, je $R = R_1 \times \mathbb{Z}_3$, kjer je R_1 lokalni komutativni enotski kolobar moči 4. Po [8] obstajajo štirje komutativni enotski kolobarji moči 4. Ti so $\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2[x]/(x^2+1) = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \right\}, \mathbb{Z}_2[x]/(x^2 + x + 1) = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \right\}$. Pri tem kolobar $\mathbb{Z}_2 \times \mathbb{Z}_2$ ne pride v poštev, saj je razcepen in zato ni lokalen. Omeniti velja, da je zadnji kolobar polje. Preverimo, da je kolobar $\mathbb{Z}_2[x]/(x^2+1)$ lokalen. Njegovi elementi so $0, 1, x, 1+x$. Pri tem sta 1 in x obrnljiva, $1+x$ pa je delitelj



SLIKA 5. Graf $T(\mathbb{Z}_3 \times \mathbb{Z}_3)$.

niča. Množica $\{0, 1+x\}$ je torej res edini ideal tega kolobarja, ki je zato lokalen. Poglejmo najprej primer kolobarja $R = \mathbb{Z}_4 \times \mathbb{Z}_3$. Enostavno je videti, da ima množica $Z(R)$ osem elementov, zato je graf $T(R)$ 7-regularen graf. Ker ima precej povezav, ne bomo risali njegovega grafa. Opazimo, da je $P_1 = m_1 \times R_2 = \{0, 2\} \times \mathbb{Z}_3$, zato $|P_1| = 6$. Sledi, da ima $T(R)$ minor K_6 in zato tudi K_5, kar pomeni, da $T(R)$ v tem primeru ni ravninski. Podobno velja za $R = \mathbb{Z}_2[x]/(x^2+1) \times \mathbb{Z}_3$. Tudi tu je minimalni praideal $P_1 = m_1 \times R_2 = \{0, 1+x\} \times \mathbb{Z}_3$, zato je $|P_1| = 6$. Sledi, da tudi v tem primeru graf $T(R)$ ni ravninski, saj vsebuje minor K_6. Ostane nam še tretji primer, ko je $R = \mathbb{Z}_2[x]/(x^2+x+1) \times \mathbb{Z}_3$. Pri tem je kolobar $\mathbb{Z}_2[x]/(x^2+x+1)$ polje. Množica obrnljivih elementov $U(R) = \{(1,1), (1,2), (x,1), (x,2), (1+x,1), (1+x,2)\}$. Pri tem sta dva različna elementa iz $U(R)$ v $T(R)$ povezana natanko takrat, ko imata različni drugi komponenti ali pa enako prvo komponento. Sledi, da vozlišča $U(R)$ tvorijo podgraf $K_{3,3}$ grafa $T(R)$. Posledično ta ni ravninski.

Obravnavajmo še primer, ko je $p_2 = 2$. Ker je $2 \leq p_1 \leq p_2 = 2$, je tudi $p_1 = 2$. Predpostavimo, da je $1 \leq k_1 \leq k_2$. Če je $k_2 \geq 3$, je moč $|P_1| = |m_1||R_2| \geq 2^3 = 8$. Posledično v tem primeru graf $T(R)$ ni ravninski, saj vsebuje minor K_5. Obravnavati moramo še možnosti, ko je $k_2 = 2$ ali $k_2 = 1$. Začnimo z drugo, ker je enostavnejša. Če je $k_2 = 1$, mora biti zaradi naše predpostavke tudi $k_1 = 1$. Tedaj je $R = \mathbb{Z}_2 \times \mathbb{Z}_2$. Njegov totalni graf je ravninski in je na sliki 3. Naj bo zdaj $k_2 = 2$. Tedaj je bodisi $k_1 = 1$ bodisi je $k_1 = 2$. Začnimo s prvim primerom. Kolobar R je oblike $R = \mathbb{Z}_2 \times R_2$, kjer je R_2 komutativni lokalni enotski kolobar moči 4. Zgoraj smo ugotovili, da obstajajo natanko trije taki kolobarji. Naj bo najprej $R = \mathbb{Z}_2 \times \mathbb{Z}_4$. Njegov graf je na sliki 6. Če skrčimo povezave $(1,2)-(0,0), (1,0)-(0,2), (1,1)-(0,3)$, odstranimo zanke in večkratne povezave, dobimo ravno graf K_5. Sledi, da $T(\mathbb{Z}_2 \times \mathbb{Z}_4)$ ni ravninski, ker vsebuje minor K_5.



SLIKA 6. Graf $T(\mathbb{Z}_2 \times \mathbb{Z}_4)$.

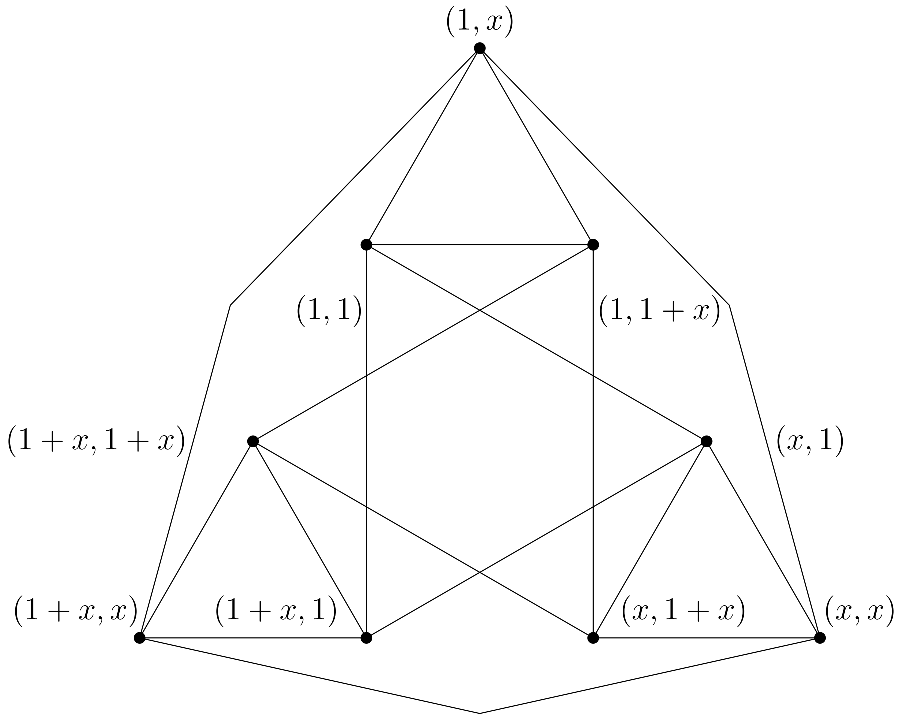
Naslednji je kolobar $R = \mathbb{Z}_2 \times \mathbb{Z}_2[x]/(x^2+1)$. Izkaže se, da je njegov totalni graf kar izomorfen totalnemu grafu kolobarja $\mathbb{Z}_2 \times \mathbb{Z}_4$. Preslikava $\varphi : T(\mathbb{Z}_2 \times \mathbb{Z}_2[x]/(x^2+1)) \to T(\mathbb{Z}_2 \times \mathbb{Z}_4)$, ki slika vozlišča $\varphi((0,0)) = (0,0), \varphi((0,1+x)) = (0,2), \varphi((0,1)) = (0,1), \varphi((0,x)) = (0,3), \varphi((1,1+x)) = (1,2), \varphi((1,0)) = (1,0), \varphi((1,x)) = (1,3), \varphi((1,1)) = (1,1)$, je izomorfizem med tema dvema grafoma. Sledi, da $T(\mathbb{Z}_2 \times \mathbb{Z}_2[x]/(x^2+1))$ ni ravninski. Poglejmo še primer kolobarja $R = \mathbb{Z}_2 \times \mathbb{Z}_2[x]/(x^2+x+1)$. Minimalna praideala sta $P_1 = \{0\} \times \mathbb{Z}_2[x]/(x^2+x+1)$ in $P_2 = \mathbb{Z}_2 \times \{0\}$. Obrnljivi elementi so $U(R) = \{(1,1),(1,x),(1,1+x)\}$. Graf $T(Z(R))$ je ravno K_4, ki ima še eno povezavo iz vozlišča $(0,0)$. Graf $T(R)$ vsebuje ta graf kot podgraf, poleg tega pa kot podgraf vsebuje še tricikel, ki ga sestavljajo vozlišča iz $U(R)$. Poleg tega je v $T(R)$ vozlišče $(1,0)$ povezano z vsemi vozlišči iz $U(R)$, vsako vozlišče iz $P_1 \setminus \{0,0\}$ pa je povezano s tistim vozliščem iz $U(R)$, ki ima enako drugo komponento. S skrčitvijo povezav med vozliščem $(1,0)$ in vozlišči iz $U(R)$ dobimo minor K_5. Graf $T(R)$ tudi tokrat ni ravninski.

Ostal nam je še zadnji primer, ko je $p_1 = p_2 = 2$ in $k_1 = k_2 = 2$. Kolobar R lahko zapišemo kot $R = R_1 \times R_2$, kjer sta oba kolobarja R_1 in R_2 komutativna lokalna enotska kolobarja moči 4, torej izomorfna enemu izmed treh zgoraj omenjenih kolobarjev. Obravnavati moramo primere, ko je R izomorfen enemu izmed kolobarjev

- $\mathbb{Z}_4 \times \mathbb{Z}_4$,
- $\mathbb{Z}_4 \times \mathbb{Z}_2[x]/(x^2+1)$,
- $\mathbb{Z}_4 \times \mathbb{Z}_2[x]/(x^2+x+1)$,
- $\mathbb{Z}_2[x]/(x^2+1) \times \mathbb{Z}_2[x]/(x^2+1)$,
- $\mathbb{Z}_2[x]/(x^2+1) \times \mathbb{Z}_2[x]/(x^2+x+1)$,
- $\mathbb{Z}_2[x]/(x^2+x+1) \times \mathbb{Z}_2[x]/(x^2+x+1)$.

V prvih petih primerih pogledamo minimalni praideal P_1. Zaporedoma dobimo $\{0,2\} \times \mathbb{Z}_4$, $\{0,2\} \times \mathbb{Z}_2[x]/(x^2+1)$, $\{0,2\} \times \mathbb{Z}_2[x]/(x^2+x+1)$, $\{0,1+$

$x\} \times \mathbb{Z}_2[x]/(x^2+1), \{0, 1+x\} \times \mathbb{Z}_2[x]/(x^2+x+1)$. Opazimo, da je v vseh petih primerih $|P_1| = 2 \cdot 4 = 8$. To implicira, da je K_8 podgraf $T(R)$ in zato ta ni ravninski. Opazujmo še zadnji primer, ko je $R = \mathbb{Z}_2[x]/(x^2+x+1) \times \mathbb{Z}_2[x]/(x^2+x+1)$. Trdimo, da $T(R)$ ni ravninski. V ta namen zadošča pokazati, da podgraf $T(U(R))$ ni ravninski. Ta je na sliki 7. Če skrčimo povezave $(1+x, 1+x) - (1+x, x), (1+x, 1) - (1+x, x), (x, 1+x) - (x, x), (x, 1) - (x, x)$, odstranimo zanke in večkratne povezave, dobimo minor K_5. Sledi, da $T(U(R))$ ni ravninski in posledično tudi $T(R)$ ni ravninski.



Slika 7. Graf $T\Big(U\Big(\mathbb{Z}_2[x]/(x^2+x+1) \times \mathbb{Z}_2[x]/(x^2+x+1)\Big)\Big)$.

Zgornje ugotovitve lahko združimo v naslednjo trditev.

Trditev 12.6. *Edina končna komutativna enotska kolobarja, ki nista lokalna in imata ravninski totalni graf, sta* $\mathbb{Z}_2 \times \mathbb{Z}_2$ *in* $\mathbb{Z}_2 \times \mathbb{Z}_3$.

13. O barvanju povezav totalnega grafa

Poglejmo, kaj lahko povemo o barvanju povezav totalnega grafa. S $\chi'(G)$ bomo označevali *kromatični indeks* grafa G, pri čemer je to moč najmanjše množice barv, s katerimi lahko povezave grafa pravilno pobarvamo. Jasno je, da kromatični indeks ne more biti strogo manjši kot je maksimalna stopnja grafa. Velja pa še več.

Izrek 13.1. *(Vizing) Naj bo G enostaven graf in naj Δ označuje maksimalno stopnjo grafa G. Tedaj je bodisi $\chi'(G) = \Delta$ bodisi $\chi'(G) = \Delta + 1$.*

Dokaz tega izreka najdemo v [6, Izrek 5.3.2].

Za posebne družine grafov je znano, kakšen je njihov kromatični indeks. Takšni so na primer polni grafi in dvodelni grafi. Iz [16, Izrek 7.10, Izrek 7.13] se spomnimo, da veljata naslednji lemi.

Lema 13.2. *Za $n \geq 2$ je $\chi'(K_n) = n$, če je n lih in $\chi'(K_n) = n-1$, če je n sod.*

Lema 13.3. *Za dvodelni graf G je $\chi'(G) = \Delta(G)$.*

Obravnavo bomo razdelili na lokalne in nelokalne kolobarje.

13.1. **Lokalni kolobarji.** Poglejmo najprej primer, ko imamo končni komutativni lokalni enotski kolobar. Vemo že, kakšen je v tem primeru totalni graf. Vemo, da je $|R| = p^n$, kjer je p praštevilo in $n \geq 1$. Po izreku 11.10 vemo, da bo v primeru, ko bo $p = 2$, graf $T(R)$ disjunktna unija $|R/Z(R)|$ kopij grafa grafa $K_{|Z(R)|}$, sicer pa bo $T(R)$ disjunktna unija grafa $K_{|Z(R)|}$ in $\frac{1}{2}(|R/Z(R)|-1)$ kopij grafa $K_{|Z(R)|,|Z(R)|}$. Ker je v komutativnem lokalnem enotskem kolobarju $Z(R) = m$, kjer je m edini maksimalni ideal, je $|Z(R)| = p^k$, kjer je $0 \leq k < n$. V primeru, ko je $p = 2$, je po lemi 13.2 kromatični indeks vsake kopije $K_{|Z(R)|} = K_{2^k}$ enak $2^k - 1$. Ker so kopije tega grafa disjunktne med sabo, je tudi $\chi'(T(R)) = 2^k - 1$. Če je $p \geq 3$, je $|Z(R)|$ liho število. Po lemi 13.2 je kromatični indeks podgrafa $K_{|Z(R)|} = K_{p^k} = p^k$. Ker je tudi maksimalna stopnja podgrafa $K_{|Z(R)|,|Z(R)|} = K_{p^k,p^k}$ enaka p^k, je po lemi 13.3 kromatični indeks podgrafa $K_{|Z(R)|,|Z(R)|} = K_{p^k,p^k}$ enak p^k. Ker je v tem primeru graf $T(R)$ sestavljen iz disjunktnih kopij takih grafov, je njegov kromatični indeks $\chi'(T(R)) = p^k$. Te ugotovitve lahko združimo v naslednjo trditev.

Trditev 13.4. *Naj bo R končni komutativni lokalni enotski kolobar. Potem je $|R| = p^n$ in $|Z(R)| = p^k$, kjer je p praštevilo in $n \geq 1, 0 \leq k < n$ naravni števili. Kromatični indeks totalnega grafa $\chi'(T(R))$ je enak $2^k - 1$, če je $p = 2$, sicer pa p^k.*

13.2. **Nelokalni kolobarji.** Problem postane težji, če izpustimo predpostavko o lokalnosti, saj v tem primeru totalnega grafa ni moč opisati na tako lep način kot v primeru lokalnega kolobarja. Če združimo izreka 13.1 in 11.14, dobimo naslednjo trditev.

Trditev 13.5. *Naj bo R končni komutativni enotski kolobar. Če je $|R|$ sodo število, je $\chi'(T(R)) \in \{|Z(R)|-1, |Z(R)|\}$, sicer pa je $\chi'(T(R)) \in \{|Z(R)|, |Z(R)|+1\}$.*

Dokaz. Po izreku 11.14 je v primeru, ko je $|R|$ sodo število, graf $T(R)$ $(|Z(R)|-1)$-regularen graf. To pomeni, da je maksimalna stopnja $\Delta(T(R)) = |Z(R)| - 1$ in po Vizingovem izreku 13.1 trditev v tem primeru sledi. Če $|R|$ ni sodo število, pa je za $x \in U(R)$ stopnja $\deg(x) = |Z(R)|$ in za $y \in Z(R)$ stopnja $\deg(y) = |Z(R)| - 1$. V tem primeru je maksimalna stopnja enaka $|Z(R)|$ in z uporabo Vizingovega izreka 13.1 dobimo trditev. □

Ta trditev seveda velja tudi v primeru, ko je R lokalni kolobar. Za lokalni kolobar R sode moči velja $\chi'(T(R)) = |Z(R)| - 1$, če pa je R lokalni kolobar lihe moči, pa velja $\chi'(T(R)) = |Z(R)|$.

Poglejmo družino kolobarjev oblike $R(p,k) = \mathbb{Z}_2 \times \mathrm{GF}(p^k)$, kjer je p praštevilo in $k \geq 1$ naravno število. Totalni graf takega kolobarja znamo natančneje opisati, kar nam bo v pomoč pri določitvi njegovega kromatičnega indeksa. Najprej ugotovimo, da sta minimalna praideala enaka $P_1 = \{0\} \times \mathrm{GF}(p^k)$ in $P_2 = \mathbb{Z}_2 \times \{0\} = \{(0,0),(1,0)\}$. Ker je $Z(R) = P_1 \cup P_2$, je $|Z(R)| = p^k + 1$. Množica obrnljivih elementov je enaka $U(R(p,k)) = \{1\} \times \mathrm{GF}(p^k)^*$ in zato moči $|U(R(p,k))| = |\mathrm{GF}(p^k)^*| = p^k - 1$. Ker je $1 + 1 = 0$ v $\mathbb{Z}_2$, sta poljubni vozlišči iz množice $U(R(p,k))$ povezani med sabo v $T(R(p,k))$, saj ima njuna vsota na prvi komponenti 0. Vozlišča iz $U(R(p,k))$ napenjajo poln podgraf K_{p^k-1}. Vemo že, da elementi vsakega minimalnega praideala napenjajo poln podgraf. Praideal P_1 napenja podgraf K_{p^k} in praideal P_2 napenja podgraf K_2, pri čemer imata ta dva podgrafa skupno vozlišče $(0,0)$. V grafu $T(R(p,k))$ imamo še povezavo med vozliščem $(1,0) \in P_2$ in poljubnim vozliščem iz $U(R(p,k))$, za vsak neničelni $x \in \mathrm{GF}(p^k)$ pa še povezavo med vozliščem $(0,x) \in P_1$ in vozliščem $(1,-x) \in U(R(p,k))$. Zapišimo to formalno. Ker je $|R(p,k))| = 2p^k$, ima graf $T(R(p,k))$ natanko $2p^k$ vozlišč. Označimo jih kot $V(T(R(p,k))) = \{v_i\}_{i=1}^{p^k} \cup \{u_i\}_{i=1}^{p^k}$. Vozlišče u_1 enačimo z vozliščem $(0,0)$, vozlišče v_1 pa z vozliščem $(1,0)$. Množica povezav je enaka $E(T(R(p,k))) = \{u_iu_j\}_{1\leq i<j\leq p^k} \cup \{v_iv_j\}_{1\leq i<j\leq p^k} \cup \{u_iv_i\}_{i=1}^{p^k}$. To natančno določa graf $T(R(p,k))$.

Poglejmo si, kaj lahko povemo o kromatičnem indeksu $\chi'(T(R(p,k)))$. Pri tem bomo ločili dva primera v odvisnosti od parnosti praštevila p.

Naj bo najprej $p = 2$. Potrebovali bomo naslednjo lemo.

Lema 13.6. *Naj bo n liho število. Naj bo G graf z množico vozlišč $V(G) = \{v_i\}_{i=1}^n \cup \{u\}$ in množico povezav $E(G) = \{v_iv_j\}_{1\leq i<j\leq n} \cup \{v_iu\}_{i=1}^n$. Tedaj je $\chi'(G) = n$.*

Dokaz. Opazimo, da je graf G sestavljen iz podgrafa K_n na vozliščih $\{v_i\}_{i=1}^n$, iz vsakega vozlišča pa ima še eno povezavo do vozlišča u. Iz leme 13.2 vemo, da je $\chi'(K_n) = n$, ker je n liho število. Stopnja vsakega vozlišča v_i je enaka $n-1$, torej v vsakem vozlišču manjka natanko ena barva in v nobenih dveh vozliščih ne manjka ista barva (glej [16, Izrek 7.10]). Povezavo v_iu pobarvamo z barvo, ki manjka v vozlišču v_i, potem ko smo pravilno pobarvali podgraf K_n. Na ta način dobimo pravilno barvanje z n barvami. Sledi, da je $\chi'(G) = n$. □

Posledica 13.7. $\chi'(T(\mathbb{Z}_2 \times \mathrm{GF}(2^k))) = \chi'(T(R(2,k))) = 2^k$.

Dokaz. Spomnimo se opisa grafa $T(R(2,k))$. Vemo, da je vozlišče $(0,0)$ sosedno z vsemi neničelnimi vozlišči iz $Z(R)$. Sledi, da je $\chi'(T(R(2,k))) \geq 2^k$. Pokažimo, da obstaja pravilno barvanje z 2^k barvami. Spomnimo se, da graf $T(R(2,k))$ vsebuje podgraf K_{2^k}, ki pripada minimalnemu praidealu $P_1 = \{0\} \times \mathrm{GF}(2^k)$. Za pravilno barvanje tega podgrafa po lemi 13.2 potrebujemo $2^k - 1$ barv. Pobarvajmo ta podgraf z $2^k - 1$ barvami $\{b_i\}_{i=1}^{2^k-1}$. Ker gre iz vsakega vozlišča tega podgrafa še po ena povezava, moramo vse te povezave pobarvati z barvo b_{2^k}. To pomeni, da v vozlišče $(1,0)$ in v vsa vozlišča iz $U(R(2,k))$ pride po ena povezava barve b_{2^k}. Če uspemo povezave iz vozlišča $(1,0)$ in med vozlišči iz $U(R(2,k))$ pobarvati z barvami $b_1,\ldots,b_{2^k-1}$, smo našli pravilno 2^k-barvanje. To naredimo po lemi 13.6, saj za vozlišča $\{v_i\}_{i=1}^n$, kjer je $n = 2^k-1$ liho število, lahko vzamemo kar elemente množice $U(R(p,k))$, za vozlišče u pa vzamemo $(1,0)$. Sledi, da je $\chi'(T(R(2,k)) = 2^k$. □

Poglejmo sedaj še primer, ko je $p > 2$.

Lema 13.8. *Naj bo $p \geq 3$ praštevilo. Tedaj je $\chi'(T(\mathbb{Z}_2 \times \mathrm{GF}(p^k))) = \chi'(T(R(p,k))) = p^k$.*

Dokaz. Enako kot prej je $\deg((0,0)) = p^k$, zato je $\chi'(T(R(p,k))) \geq p^k$. Opazimo, da vozlišča iz minimalnega praideala $P_1 = \{0\} \times \mathrm{GF}(p^k)$ tvorijo poln podgraf K_{p^k}. Tudi vozlišča iz množice $U(R(p,k)) \cup \{(1,0)\}$ tvorijo poln podgraf K_{p^k}. V grafu $T(R(p,k))$ imamo še povezave med $(1,x)$ in $(0,-x)$, kjer je $x \in \mathrm{GF}(p^k)$ poljuben element. Po lemi 13.2 za barvanje ene kopije grafa K_{p^k} potrebujemo p^k barv. Pri tem v vsakem vozlišču manjka ena barva. Denimo, da smo najprej s p^k barvami pobarvali kopijo grafa K_{p^k}, ki pripada vozliščem iz P_1. Nato pravilno pobarvamo povezave med obema kopijama grafa K_{p^k}. To se res da, saj v prvi kopiji grafa K_{p^k} v vsakem vozlišču manjka natanko ena barva in v nobenem paru vozlišč ne manjkata isti barvi. Nato moramo samo še prenesti barvanje s prve kopije grafa K_{p^k} na drugo kopijo tega grafa. Če so v prvi kopiji grafa K_{p^k} vozlišča označena kot $\{v_i\}_{i=1}^{p^k}$ in v drugi kot $\{u_i\}_{i=1}^{p^k}$, kjer je vozlišče v_i povezano še z vozliščem u_i, povezavo u_iu_j pobarvamo z isto barvo kot povezavo v_iv_j. Ker je prva kopija pravilno pobarvana, bo pravilno pobarvana tudi druga kopija podgrafa K_{p^k}. Sledi, da je $\chi'(T(R(p,k))) = p^k$. □

Ko združimo zgornje ugotovitve, pridemo do naslednje trditve.

Trditev 13.9. *Naj bo p poljubno praštevilo. Tedaj je*

$$\chi'(T(\mathbb{Z}_2 \times \mathrm{GF}(p^k))) = \chi'(T(R(p,k))) = p^k = |Z(R)| - 1 = \Delta(T(R(p,k))).$$

14. Eulerjevost totalnega grafa

Spomnimo se, da je graf Eulerjev natanko takrat, ko je povezan in so vse njegove točke sode stopnje [6, Izrek 1.8.1]. S pomočjo tega je lahko ugotoviti, ali je graf Eulerjev, poznati moramo le stopnje vseh vozlišč.

Primer 14.1. Definirajmo kolobarje $R_{p,k} = \left\{ \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}; a \in \mathbb{Z}_{p^k} \right\}$. Takoj poračunamo, da je produkt poljubnih dveh elementov iz $R_{p,k}$ enak 0, kar pomeni, da je $R_{p,k} = Z(R_{p,k})$. Očitno je $R_{p,k}$ tudi brez enote. Ker so vsi elementi delitelji niča, je $T(R_{p,k}) = K_{|Z(R_{p,k})|} = K_{|R_{p,k}|} = K_{p^k}$. Stopnja vsakega vozlišča v K_{p^k} je enaka $p^k - 1$. Če je torej p liho praštevilo, je graf $T(R_{p,k})$ Eulerjev graf.

Obravnavo bomo spet ločili na lokalne in nelokalne kolobarje. Začnimo z lokalnimi kolobarji. Naj bo R končni lokalni enotski kolobar. Po izreku 11.10 graf $T(R)$ ni povezan in zato ni Eulerjev.

Naj bo zdaj R končni komutativni enotski kolobar, ki ni lokalen. Po izreku 11.14 vemo, da je v primeru, ko $|R|$ ni sodo število, stopnja vozlišča $x \in Z(R)$ enaka $\deg(x) = |Z(R)| - 1$ in stopnja vozlišča $y \in U(R)$ enaka $\deg(y) = |Z(R)|$. Ti dve števili ne moreta biti obe hkrati sodi, zato graf v tem primeru ni Eulerjev. Obravnavati moramo le še končne komutativne enotske kolobarje sode moči, ki niso lokalni. Dokažimo naslednjo lemo.

Lema 14.2. *Naj bo $n \in \mathbb{N}$. Označimo z R kolobar $R = \prod_{i=1}^n \mathrm{GF}(p_i^{k_i})$, kjer so p_i praštevila in $k_i \geq 1$ naravna števila. Moč množice $|Z(R)|$ je liho število natanko tedaj, ko so vsa praštevila p_i iste parnosti. To lahko povemo še drugače. Moč množice $|Z(R)|$ je liho število natanko tedaj, ko je bodisi $p_i = 2, i = 1, \ldots, n$ bodisi $p_i > 2, i = 1, \ldots, n$.*

Dokaz. Označimo z $R_i = \mathrm{GF}(p_i^{k_i})$. Velja $|Z(R)| = |R \setminus U(R)| = |R| - \prod_{i=1}^n |R_i^*|$. Če $p_i = 2$ za vsak i, potem je $|R_i^*|$ liho število za vsak i. Potem je $|R|$ sodo, $|U(R)|$ pa liho število, zato je $|Z(R)|$ liho. Če velja $p_i > 2$ za vsak i, pa je $|R|$ liho, $|U(R)|$ pa sodo število, zato je $|Z(R)|$ liho. Če za neka i in j velja $p_i = 2$ in $p_j > 2$, sta $|R|$ in $|U(R)|$ sodi števili, saj p_i deli $|R|$ in $2|(p_j^{k_j} - 1) = |R_j^*|$. Zato je $|Z(R)|$ sodo. □

Če to lemo združimo z ugotovitvijo, da je za končni komutativni razcepni enotski kolobar R sode moči graf $T(R)$ po izreku 11.14 $(|Z(R)| - 1)$-regularen, imamo na dlani naslednjo posledico.

Posledica 14.3. *Naj bo $R = \prod_{i=1}^n \mathrm{GF}(p_i^{k_i})$, kjer so $p_i, i = 1, \ldots, n$ praštevila in $n, k_1, \ldots, k_n \geq 1$ naravna števila, kolobar sode moči. Graf $T(R)$ je Eulerjev natanko tedaj, ko je $p_i = 2, 1 \leq i \leq n$.*

Literatura

[1] D. F. Anderson, A. Frazier, A. Lauve in P. S. Livingston, *The zero-divisor graph of a commutative ring, II*, Lecture Notes in Pure and Appl. Math. **220**, Marcel Dekker, New York, 2001.

[2] M. F. Atiyah in I. G. MacDonald, *Introduction to Commutative Algebra*, Adison-Wesley Publishing Company, Reading, Massachusetts, 1969.

[3] M. Axtell, N. Baeth in J. Stickles, *Cut Vertices in Zero-Divisor Graphs of Finite Commutative Rings*, Communications in Algebra **39** (2011) 2179-2188.

[4] W. C. Brown, *Matrices Over Commutative Rings*, Monographs and textbooks in pure and applied mathematics **169**, Marcel Dekker, New York, 1993.

[5] G. Chartrand in L. Lesniak, *Graphs & Digraphs, third edition*, Chapman & Hall/CRC, 1996.

[6] R. Diestel, *Graph Theory*, Graduate Texts in Mathematics **173**, Springer-Verlag, 2006.

[7] D. Dolžan in P. Oblak, *The total graphs of finite rings*, [ogled 10. 6. 2014], dostopno na `http://arxiv.org/pdf/1401.1941v1.pdf`.

[8] G. Dresden, *Small Rings*, [ogled 1. 3. 2014], dostopno na `http://home.wlu.edu/ dresdeng/smallrings/`.

[9] B. Fine, *Classification of Finite Rings of Order* p^2, Mathematics Magazine **66** (1993) 248-252.

[10] A. Gibbons, *Algorithmic graph theory*, Cambridge University Press, 1985.

[11] I. Kaplansky, *Commutative Rings*, Allyn and Bacon, 1970.

[12] A. S. Kuzmina, *Finite rings with Eulerian zero-divisor graphs*, Journal of Algebra and Its Applications **11** (2012).

[13] T. Y. Lam, *A First Course in Noncommutative Rings, Second Edition*, Graduate Texts in Mathematics **131**, Springer-Verlag, New York, 2001.

[14] C. Miguel, *Balanced Zero-Divisor Graphs of Matrix Rings*, Lobachevskii Journal of Mathematics **34** (2013) 137-141.

[15] A. Nechaev, *Finite rings*, [ogled 8. 4. 2014], dostopno na `http://www.cimpa-icpam.org/anciensite/NotesCours/PDF/2008/Nechaev.pdf`.

[16] K. Pavlič, *Grafi deliteljev niča nad komutativnimi kolobarji*, diplomsko delo, Fakulteta za matematiko in fiziko, Univerza v Ljubljani, 2012.

[17] S. P. Redmond, *Central Sets and Radii of the Zero-Divisor Graphs of Commutative Rings*, Communications in Algebra **34** (2006) 2389-2401.

[18] S. P. Redmond, *Cut Vertices and Degree One Vertices of Zero-Divisor Graphs*, Communications in Algebra **40** (2012) 2749-2756.

[19] S. P. Redmond, *On zero-divisor graphs of small finite commutative rings*, Discrete Math. **307** (2007) 1155-1166.

[20] M. H. Shekarriz, M. H. Shirdareh Haghighi in H. Sharif, *On the Total Graph of a Finite Commutative Ring*, Communications in Algebra **40** (2012) 2798-2807.