UNIVERZITET U NOVOM SADU
PRIRODNO-MATEMATIČKI FAKULTET
DEPARTMAN ZA MATEMATIKU I INFORMATIKU

Ivan Pavkov

Nesvodljivost polinoma dve promenljive

- master rad -

Mentor: Prof. dr Siniša Crvenković

Novi Sad, 2010.

Zahvaljujem se svom mentoru, prof. dr Siniši Crvenkoviću na pomoći pri izboru teme i velikoj podršci u svim fazama njene izrade.

Takođe se zahvaljujem i van. prof. dr Petru Markoviću i doc. dr Petru Đapiću na korisnim sugestijama.

SADRŽAJ

1. UVOD

Faktorisanje polinoma se smatra fundamentalnim problemom u algebri i teoriji brojeva. Algoritmi koji su pronađeni u poslednjih četrdesetak godina učinili su mogućim da se, uz pomoć računara, efikasno faktoriše polinom sa jednom, dve ili više promenljivih sa koeficijentima iz određenog polja (npr. konačnog polja ili polja racionalnih, realnih ili kompleksnih brojeva).

Za polinome sa 10 promenljivih i 1000 terma, pri čemu je najveći stepen pojedinačne promenljive 10, preko 85% ovakvih polinoma može biti prepoznato kao nesvodljivo u deliću sekunde korišćenjem brzih testova nesvodljivosti. Međutim, ovakvi testovi ne prepoznaju sve nesvodljive polinome, tako da bi trebali biti korišćeni kao pretest pre korišćenja opštijih i sporijih algoritama.

Neka je $\mathbb{F}[x,y]$ prsten polinoma sa dve promenljive nad proizvoljnim poljem $\mathbb{F}$. Polinom maksimalnog stepena d po svakoj promenljivoj u ovom prstenu ima maksimalno $(d+1)^2$ terma i polinom sa $O((d+1)^2)$ nenula terma nazivamo ***gust*** (“***dense***”) polinom.

Intuitivno, ***redak*** (“***sparse***”) polinom je polinom sa mnogo manje nenula terma od ovog maksimuma. Formalno, za polinom iz $\mathbb{F}[x,y]$ sa najvećim stepenom d po svakoj promenljivoj kažemo da je ***redak*** (“***sparse***”) polinom ako je broj nenula terma $O(d)$.

Za polinom nad poljem $\mathbb{F}$ kažemo da je ***apsolutno nesvodljiv*** ako ostaje nesvodljiv nad svakim natpoljem polja $\mathbb{F}$. Na primer, polinom $p(x,y) = x^3 - y^2$ je nesvodljiv nad poljem racionalnih brojeva i ostaje nesvodljiv nad njegovim natpoljem – poljem kompleksnih brojeva, pa je apsolutno nesvodljiv.

Još uvek je otvoreno pitanje da li postoji efektivan algoritam za faktorisanje retkih polinoma sa dve promenljive. Sa druge strane, lako je pokazati vezu između retkih polinoma sa dve promenljive i konveksnih poligona. Pokazaćemo da se svakom nerastavljivom konveksnom poligonu u smislu sume Minkovskog sa celobrojnim temenima može pridružiti klasa apsolutno nesvodljivih polinoma sa dve promenljive.

Poznato je da je većina polinoma apsolutno nesvodljiva, ali su postojeće metode za dokazivanje apsolutne nesvodljivosti veoma spore.

U ovom radu biće prikazan efikasan metod za pokazivanje apsolutne nesvodljivosti za jednu specijalnu klasu polinoma – potklasu klase retkih (“sparse”) polinoma. Ovaj metod ne uključuje bilo kakve pretpostavke o polju $\mathbb{F}$, pa stoga funkcioniše za bilo koje polje.

Takođe, ni vrednosti koeficijenata nisu važne, važno je jedino koji termi imaju nenula koeficijente, pa ovaj metod služi za pokazivanje apsolutne nesvodljivosti čitave familije, a ne samo jednog polinoma. Imajući u vidu opisanu vezu nerastavljivih konveksnih poligona i apsolutno nesvodljivih polinoma, mi ćemo, zapravo, pronalaženjem nerastavljivih konveksnih poligona određivati čitave familije apsolutno nesvodljivih polinoma.

Napomenimo da je jedan od najpoznatijih nerešenih algebarskih problema vezan upravo za polinome sa dve promenljive. Nazvan je Jakobijev problem.

Podsetimo se, Jakobijan $J(u,v)$ u odnosu na x, y definisan je sa:

$$J(u,v) = \begin{pmatrix} \frac{\partial u}{\partial x} & \frac{\partial u}{\partial y} \\ \frac{\partial v}{\partial x} & \frac{\partial v}{\partial y} \end{pmatrix}, \text{ gde je } u = u(x,y),\ v = v(x,y).$$

Formulišimo, sada, Jakobijev problem. Ako su $u = u(x,y)$, $v = v(x,y)$ polinomi sa celobrojnim koeficijentima po x i y takvi da je $J(u,v) = 1$, da li se onda x i y mogu izraziti kao polinomi po u i v, tj. $x = x(u,v)$, $y = y(u,v)$.

2. NJUTNOV POLIGON POLINOMA SA DVE PROMENLJIVE

Obeležimo sa $\mathbb{R}^2$ dvodimenzionalni realni euklidski prostor i neka je $\mathcal{S}$ njegov proizvoljan podskup. ***Konveksni omotač skupa*** $\mathcal{S}$ (u oznaci: $conv(S)$) je najmanji konveksan skup koji sadrži skup S. Kasnije ćemo pokazati da je:

$$conv(S) = \left\{ \sum_{i=1}^{k} \lambda_i x_i : \{x_1, ..., x_k\} \subseteq S, \lambda_i \geq 0, \sum_{i=1}^{k} \lambda_i = 1 \right\}.$$

Konveksni omotač skupa konačnog skupa tačaka u $\mathbb{R}^2$ je poligon. Tačka poligona se naziva teme ako se ne nalazi ni na jednoj duži koja spaja bilo koje druge dve tačke poligona. Poznato je da je poligon uvek konveksni omotač svojih temena. Takođe, zatvoren i ograničen skup nazivaćemo kompaktnim.

Definicija 1: Za bilo koja dva skupa A i B iz $\mathbb{R}^2$ skup $A+B=\{a+b : a\in A,\ b\in B\}$ naziva se ***suma Minkovskog skupova A* i *B***.
Za tačku iz $\mathbb{R}^2$ kažemo da je ***celobrojna*** ako su obe njene koordinate celi brojevi. Za poligon kažemo da je ***celobrojni poligon*** ako su sva njegova temena celobrojna.

Definicija 2: Za celobrojni poligon C kažemo da je ***integralno rastavljiv*** ako postoje celobrojni poligoni A i B takvi da važi $C=A+B$, pri čemu i A i B sadrže bar dve tačke. Poligoni ***A* i *B*** se nazivaju ***poligoni sabirci*** od C. U suprotnom, kažemo da je celobrojni poligon C ***integralno nerastavljiv***, odnosno da ne poseduje netrivijalnu dekompoziciju.

Definicija 3: Neka je $\mathbb{F}$ proizvoljno polje. Posmatrajmo proizvoljan polinom iz $\mathbb{F}[x, y]$ - prstena polinoma sa dve promenljive nad tim poljem:

$$f(x,y) = \sum C_{e_1 e_2} x^{e_1} y^{e_2} \in \mathbb{F}[x, y]$$

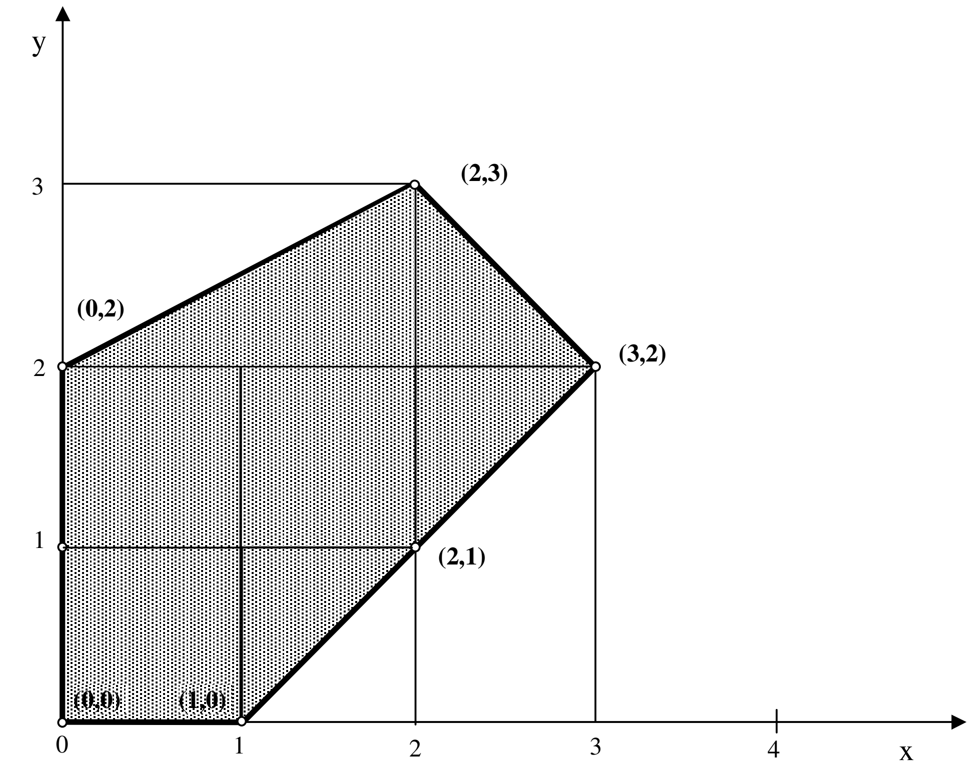
Posmatrajmo vektore eksponenata (e_1,e_2) onih terma gornjeg polinoma sa nenula koeficijentima ($C_{e_1e_2} \neq 0$) kao tačke u $\mathbb{R}^2$. Svakom vektoru (e_1,e_2) pridružimo tačku Dekartove koordinatne ravni sa koordinatama (e_1,e_2). Konveksni omotač ovog skupa tačaka naziva se ***Njutnov poligon polinoma f***, u oznaci P_f.

Napomena 1: Njutnov poligon polinoma f, tj. konveksni omotač efektivno konstruišemo na sledeći način: najpre u Dekartovoj koordinatnoj ravni ucrtamo sve tačke $(e_1,e_2)_i$ koje odgovaraju termima gornjeg polinoma sa nenula koeficijentima, $i=1,...,k$ (pod pretpostavkom da polinom f ima k terma sa nenula koeficijentima). Jasno je da sve tačke $(e_1,e_2)_i$ imaju obe celobrojne, nenegativne koordinate, odnosno nalaze se u prvom kvadrantu Dekartove koordinatne ravni zajedno sa nenegativnim delovima x i y ose. Za prvo teme poligona odaberimo onu tačku $(e_1,e_2)_i$, $i=1,...,k$ sa najmanjom x koordinatom. Ako postoji više od jedne takve tačke, za polaznu tačku biramo tačku sa najmanjom x koordinatom koja pritom ima i najmanju y koordinatu, odnosno koja je bliža koordinatnom početku. Neka je za polaznu tačku odabrana tačka $(e_1,e_2)_p$, $1\leq p\leq k$. Za ciljnu tačku prve duži biramo jednu od preostalih tačaka $(e_1,e_2)_i$, $i=1,...,k$, $i\neq p$, obeležimo je sa $(e_1,e_2)_c$ takvu da se sve ostale tačke $(e_1,e_2)_i$, $i=1,...,k$, $i\neq p, i\neq c$ nalaze u istoj zatvorenoj poluravni u odnosu na pravu određenu tačkama $(e_1,e_2)_p$ i $(e_1,e_2)_c$. Pretpostavimo da postoji više od jedne takve tačke $(e_1,e_2)_c$, neka su to recimo tačke $(e_1,e_2)_{c'}$ i $(e_1,e_2)_{c''}$. Jasno je da su tada tačke $(e_1,e_2)_p$, $(e_1,e_2)_{c'}$ i $(e_1,e_2)_{c''}$ kolinearne, pa važi jedan od rasporeda: $(e_1,e_2)_p$ – $(e_1,e_2)_{c'}$ – $(e_1,e_2)_{c''}$ ili $(e_1,e_2)_p$ – $(e_1,e_2)_{c''}$ – $(e_1,e_2)_{c'}$. Bez umanjenja opštosti, pretpostavimo da važi raspored: $(e_1,e_2)_p$ – $(e_1,e_2)_{c'}$ – $(e_1,e_2)_{c''}$. Tada za sledeće teme Njutnovog poligona polinoma f biramo tačku $(e_1,e_2)_{c''}$. Za sledeće teme poligona biramo jednu od tačaka različitu od $(e_1,e_2)_p$, $(e_1,e_2)_{c'}$ i $(e_1,e_2)_{c''}$, takvu da su sve tačke u istoj zatvorenoj poluravni u odnosu na pravu određenu izabranom tačkom i tačkom $(e_1,e_2)_{c''}$. Potpuno analogno, postupak nastavljamo izborom za sledeće teme poligona tačke koja do tada nije izabrana za teme, niti je odbačena zbog kolinearnosti sa dva uzastopno izabrana temena. Postupak se prekida kada se vratimo u početnu tačku. Njutnov poligon polinoma f je poligon čija su temena redom tačke izabrane opisanim algoritmom.

Primer 1: Posmatrajmo polinom:

$$f(x,y) = x^3y^2 + x^2y^3 + x^2y + y^2 + x + 1.$$

Konstruišimo Njutnov poligon polinoma $f(x,y)$ pomoću prethodno opisanog algoritma. Termima polinoma $f(x,y)$ sa nenula koeficijentima odgovaraju redom sledeći vektori eksponenata: (3,2), (2,3), (2,1), (0,2), (1,0) i (0,0). Najpre ucrtajmo u Dekartovoj koordinatnoj ravni sve tačke čije koordinate odgovaraju datim vektorima eksponenata. Kandidati za prvo teme poligona su tačke sa najmanjom x-koordinatom, tj. tačke (0,2) i (0,0). Za prvo teme biramo onu tačku koja ima manju y-koordinatu, tačku (0,0). S obzirom da se sve tačke u istoj zatvorenoj poluravni u odnosu na pravu određenu tačkama (0,0) i (1,0), za sledeće teme poligona biramo tačku (1,0). Kako su tačke (1,0), (2,1) i (3,2) kolinearne i važi raspored tačaka: (1,0)–(2,1)–(3,2), za sledeće teme poligona biramo tačku (3,2). Pri izboru sledećeg temena poligona iz razmatranja se izuzimaju da sada izabrana temena (tačke (0,0), (1,0) i (3,2)) i tačka koja nije izabrana za teme zbog kolinearnosti sa dva uzastopna temena (tačka (2,1)), kandidati za sledeće teme su tačke (2,3) i (0,2). Kako su sve tačke u istoj zatvorenoj poluravni u odnosu na pravu određenu tačkama (3,2) i (2,3), za sledeće teme poligona biramo tačku (2,3). Rezonujući na potpuno isti način, za sledeće teme poligona (0,2). S obzirom da su sve tačke ili izabrane za temena poligona ili odbačene zbog kolinearnosti sa dva uzastopna temena, postupak se prekida. Njutnov poligon polinoma f je poligon čija su temena redom tačke: (0,0), (1,0), (3,2), (2,3) i (0,2), što je prikazano na slici 1.

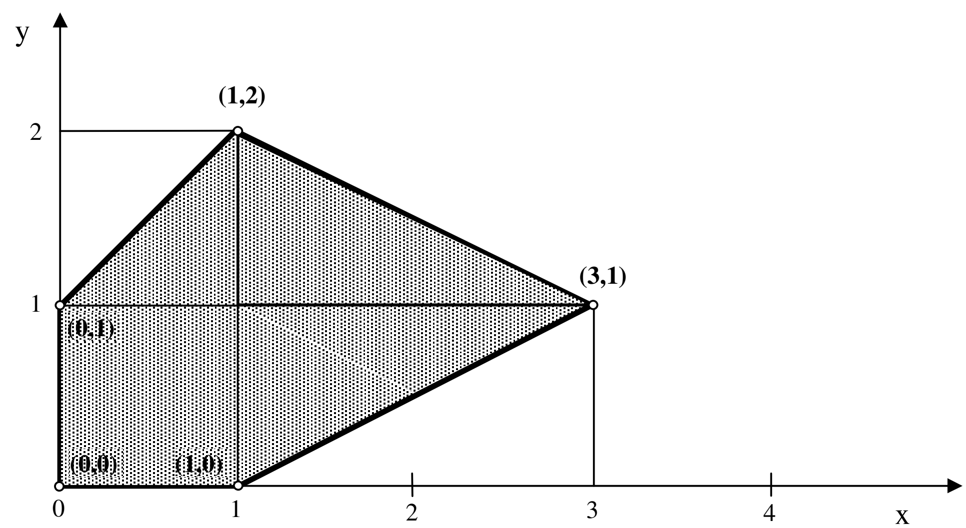


Slika 1

Primer 2: Posmatrajmo polinom:

$$f(x,y) = x^3y + xy^2 + x + y + 1.$$

Termima polinoma $f(x,y)$ sa nenula koeficijentima odgovaraju redom sledeći vektori eksponenata: (3,1), (1,2), (1,0), (0,1) i (0,0). Njutnov poligon polinoma $f(x,y)$ je konveksni omotač ovog skupa tačaka (slika 2).



Slika 2

Teorema 1: Neka su $f,g,h\in \mathbb{F}[x,y]$ i neka je $f=gh$. Tada važi $P_f = P_g+P_h$.

Dokaz:
U ***Teoremi 8*** ćemo pokazati da je suma Minkovskog dva poligona poligon i da teme zbirnog poligona nastaje kao suma Minkovskog temena poligona sabiraka.
Neka je $(\alpha,\beta)\in P_f$ proizvoljno teme Njutnovog poligona polinoma f. Po definiciji Njutnovog poligona, to znači da polinom f sadrži monom $x^{\alpha}y^{\beta}$ sa nenula koeficijentom. Kako je $f=gh$, zaključujemo da polinomi g i h sadrže redom monome $x^{\gamma}y^{\delta}$ i $x^{\alpha-\gamma}y^{\beta-\delta}$ sa nenula koeficijentima. Ovim monomima odgovaraju tačke $(\gamma,\delta)\in P_g$ i $(\alpha-\gamma,\beta-\delta)\in P_h$. Jasno je da važi: $(\gamma,\delta)+(\alpha-\gamma,\beta-\delta)\in P_g+P_h$, odakle dobijamo $(\gamma+\alpha-\gamma,\delta+\beta-\delta)\in P_g+P_h$, tj. $(\alpha,\beta)\in P_g+P_h$. Kako za proizvoljno $(\alpha,\beta)\in P_f$ važi $(\alpha,\beta)\in P_g+P_h$, zaključujemo da je $P_f\subseteq P_g+P_h$.
Pokazaćemo da važi i obrnuta inkluzija, tj. da je $P_g+P_h \subseteq P_f$. Kako je Njutnov poligon konveksni omotač svojih temena, dovoljno je pokazati da se svako teme poligona P_g+P_h nalazi u poligonu P_f. Neka je v teme Njutnovog poligona P_g+P_h. Kako $v\in P_g+P_h$, zaključujemo da postoje tačke $v_g\in P_g$ i $v_h\in P_h$ takve da je $v=v_g+v_h$.
Iz pretpostavke da je v teme Njutnovog poligona P_g+P_h sledi jedinstvenost vektora v_g i v_h. Pretpostavimo suprotno, $v= v_g+v_h= v_g'+v_h'$, gde $v_g, v_g'\in P_g, v_h, v_h'\in P_h$, pri čemu važi $v_g\neq v_g'$ i $v_h\neq v_h'$. Neka je $v = (x,y)$ i $v_g = (a,b)$. Kako je $v = v_g+v_h$, očigledno je $v_h = (x-a,y-b)$. Ako je $v_g' = (c,d)$, potpuno analogno zaključujemo da je $v_h' = (x-c,y-d)$.
Posmatrajmo, sada, tačku v_g+v_h'. Jasno je da $v_g+v_h'\in P_g+P_h$ i važi:

$$v_g+v_h' = (a,b) + (x-c,y-d) = (x+a-c,y+b-d) = (x+(a-c),y+(b-d)).$$

Posmatrajmo, zatim, tačku $v_g'+v_h$. Jasno je da $v_g'+v_h\in P_g+P_h$ i važi:

$$v_g'+v_h= (c,d) + (x-a,y-b) = (x-a+c,y-b+d)=(x-(a-c),y-(b-d)).$$

Potražimo sredinu duži čije su krajnje tačke v_g+v_h' i $v_g'+v_h$ Njutnovog poligona P_g+P_h:

$$\left(\frac{x+(a-c)+x-(a-c)}{2},\frac{y+(b-d)+y-(b-d)}{2}\right)=(x,y).$$

Dakle, sredina duži čije su krajnje tačke v_g+v_h' i $v_g'+v_h$ Njutnovog poligona P_g+P_h je tačka (x,y). Kako je teme poligona tačka koja se ne nalazi ni na jednoj duži koja spaja bilo koje druge dve tačke poligona, zaključujemo da tačka (x,y) nije teme poligona P_g+P_h, što je očigledna kontradikcija. Dakle, za teme v Njutnovog poligona P_g+P_h postoje jedinstveni vektori $v_g\in P_g$ i $v_h\in P_h$ takvi da je $v = v_g+v_h$.
Kako je v teme poligona P_g+P_h, zaključujemo da v_g i v_h moraju biti temena poligona P_g i P_h. S obzirom da su v_g i v_h jedinstveni, očigledno je da postoji jedinstven term u izrazu $g\cdot h$ koji ima v za svoj vektor eksponenta. Odavde sledi $v\in P_f$. Na ovaj način smo pokazali da su sva temena poligona P_g+P_h u poligonu P_f, a kako je Njutnov poligon konveksni omotač svojih temena, važi: $P_g+P_h \subseteq P_f$. □

Napomena 2: Iz dokaza prethodne teoreme možemo primetiti da monomima polinoma f koji se "dobijaju" na bar dva različita načina množenjem monoma faktor-polinoma g i h sigurno ne odgovaraju temena Njutnovog poligona P_f.

Posmatrajmo, recimo, polinom:

$$f(x,y) = 2x^2y^2 + xy^3 + x^3y \in \mathbb{F}[x, y].$$

Polinom $f(x,y)$ se može faktorisati na sledeći način:

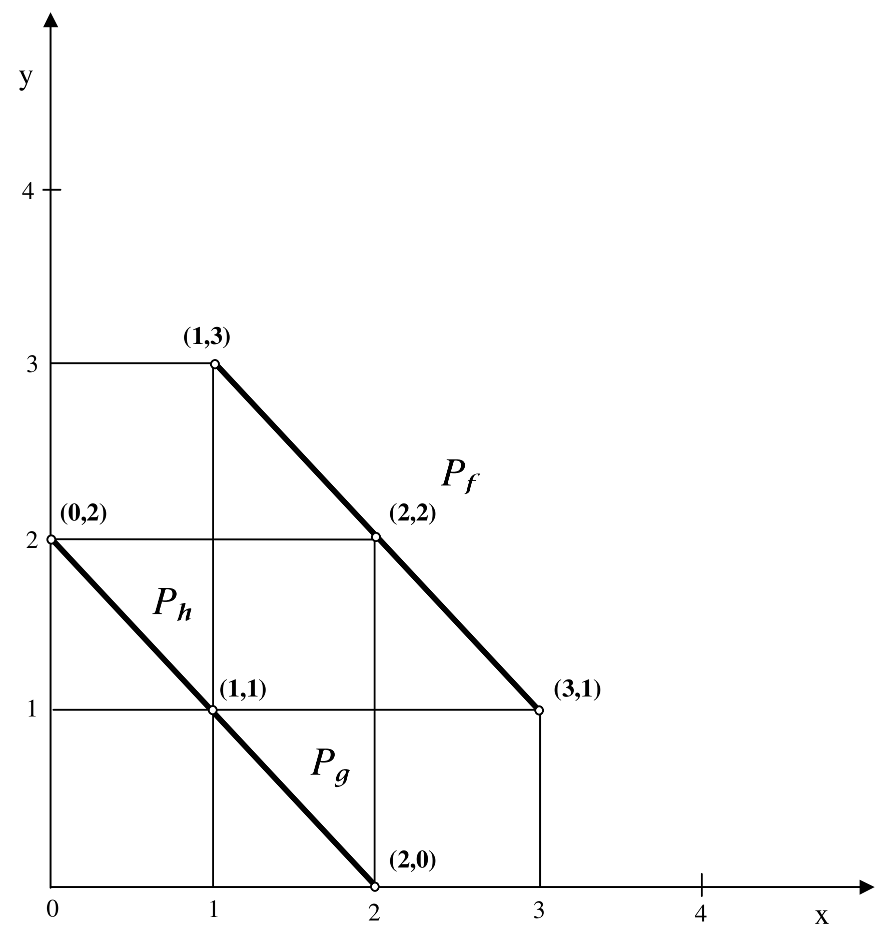
$$f(x,y) = 2x^2y^2 + xy^3 + x^3y = (x^2 + xy)(y^2 + xy) = gh.$$

Monom x^2y^2 polinoma f sa koeficijentom 2 se "dobija" iz faktor-polinoma na dva različita načina:

$$x^2y^2 = (x^2)(y^2) = (xy)(xy).$$

Posmatrajmo, sada, Njutnove poligone polinoma f i njegovih faktor-polinoma g i h.

Jasno, $P_f = conv((2,2), (1,3), (3,1))$ je duž sa krajnjim tačkama u (1,3) i (3,1), $P_g = conv((2,0), (1,1))$ je duž sa krajnjim tačkama u (2,0) i (1,1) i $P_h = conv((0,2), (1,1))$ je duž sa krajnjim tačkama u (0,2) i (1,1). Poligoni P_f, P_g i P_h prikazani su na slici 3.



Slika 3

Zaista, monomu x^2y^2 polinoma f koji se "dobija" na dva različita načina iz faktor-polinoma g i h odgovara tačka (2,2) koja nije teme poligona P_f.

Teorema 2: Neka je $\mathbb{F}$ proizvoljno polje i f nenula polinom iz $\mathbb{F}[x,y]$ koji nije deljiv ni sa x ni sa y. Ako je P_f Njutnov poligon polinoma f integralno nerastavljiv, onda je polinom f apsolutno nesvodljiv nad poljem $\mathbb{F}$.

Dokaz: Kako polinom f nije deljiv ni sa x ni sa y, f u faktorisanom obliku nema nijedan činilac koji se sastoji samo od jednog terma. Pretpostavimo suprotno, polinom f nije apsolutno nesvodljiv nad poljem $\mathbb{F}$, tj. ne ostaje nesvodljiv nad svakim natpoljem polja $\mathbb{F}$. To znači da nad nekim natpoljem polja $\mathbb{F}$ važi $f=gh$, pri čemu g i h imaju bar dva nenula terma. Međutim, kako i g i h imaju bar po dva nenula terma njihovi pridruženi Njutnovi poligoni imaju najmanje dve tačke. Kako je $f=gh$, na osnovu ***Teoreme 1*** zaključujemo da važi $P_f = P_g + P_h$, pri čemu P_g i P_h imaju najmanje dve tačke. Dakle, ovo je netrivijalna dekompozicija Njutnovog poligona P_f, što je u kontradikciji sa pretpostavkom teoreme da je P_f integralno nerastavljiv. Zaključujemo da je polinom f apsolutno nesvodljiv nad poljem $\mathbb{F}$. $\square$

Naš cilj je da pronađemo integralno nerastavljive Njutnove poligone u $\mathbb{R}^2$ i, samim tim, pronađemo njima pridružene apsolutno nesvodljive polinome nad proizvoljnim poljem $\mathbb{F}$.

Napomena 3: Posmatrajmo polinom f nad proizvoljnim poljem $\mathbb{F}$. Ako je Njutnov poligon polinoma f integralno rastavljiv, u zavisnosti od datog polja, f može biti svodljiv ili nesvodljiv. Pretpostavimo da P_f ima m mogućih dekompozicija u smislu sume Minkovskog. Drugim rečima, važi: $P_f = A_i + B_i$, $A_i, B_i \subseteq \mathbb{R}^2$, $i=1,...,m$, za neke integralne poligone A_i i B_i. S obzirom na ***Teoremu 2***, kako je P_f integralno rastavljiv, polinom f mora važiti $f=g_ih_i$, $i=1,...,m$, za odgovarajuće polinome g_i i h_i, pri čemu su Njutnovi poligoni polinoma g_i i h_i upravo A_i i B_i. Ovo važi za svaku moguću dekompoziciju P_f u smislu sume Minkovskog.

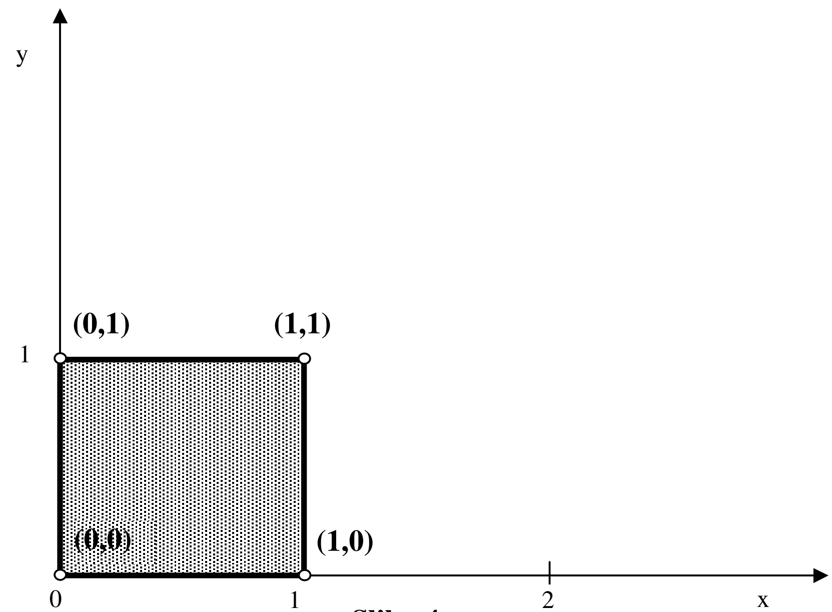
Dakle, ***Teorema 2*** se može koristiti da se pronađu moguće faktorizacije polinoma. U sledećim primerima, analiziraćemo isključivo polinome sa dve promenljive malog stepena. Očigledno, u slučaju polinoma sa velikim stepenom analiza se komplikuje. Ali, poligonalni metod može bar pružiti informaciju o obliku faktora polinoma sa dve promenljive visokog stepena.

Kao što smo ranije istakli, vrednosti koeficijenata nisu važne, važno je jedino koji termi imaju nenula koeficijente. Dakle, ovi koeficijenti se mogu proizvoljno birati nad odgovarajućim poljima, zaključak o svodljivosti polinoma i dalje važi, s tim što se koeficijenti faktor polinoma menjaju.

Primer 3: Posmatrajmo polinom:

$$f(x,y) = xy + x + y + 1 \in \mathbb{F}[x, y], \text{ za proizvoljno polje } \mathbb{F}.$$

Termima polinoma $f(x,y)$ sa nenula koeficijentima odgovaraju redom sledeći vektori eksponenata: (1,1), (1,0), (0,1) i (0,0). Njutnov poligon polinoma $f(x,y)$ je kvadrat sa celobrojnim temenima prikazan na slici 4.

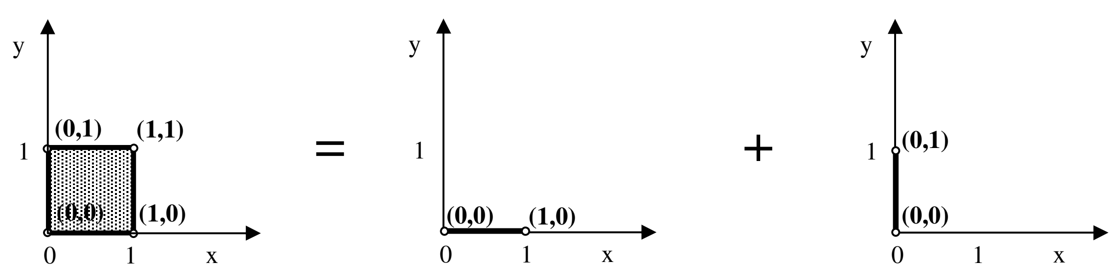


Slika 4

Jasno je da P_f može biti integralno rastavljen u smislu sume Minkovskog samo na jedan način:

$$P_f = conv((1,1), (1,0), (0,1), (0,0)) = conv((0,0), (1,0)) + conv((0,0), (0,1)),$$

što je prikazano na slici 5.



Slika 5

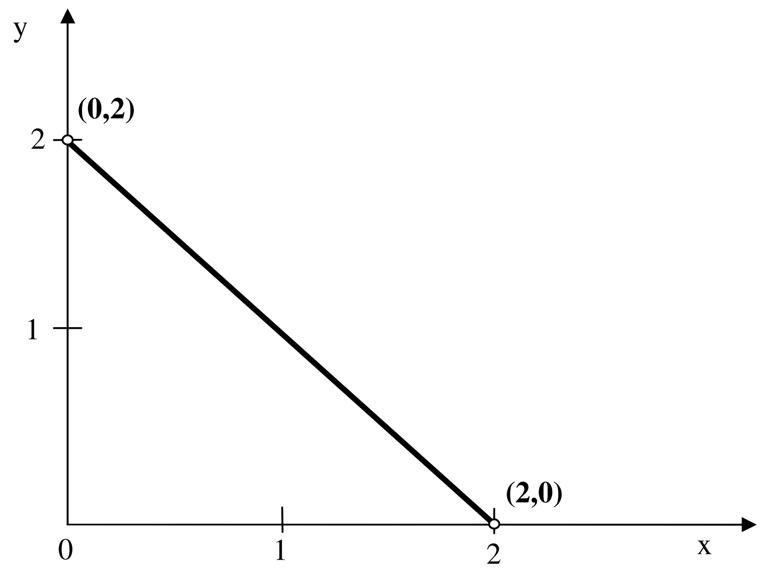
Dakle, $f(x,y)$ može se faktorisati na sledeći način:

$$f(x,y) = (x+1)(y+1).$$

Primer 4: Posmatrajmo polinom:

$$f(x,y) = x^2 + y^2.$$

Termima polinoma $f(x,y)$ sa nenula koeficijentima odgovaraju redom sledeći vektori eksponenata: (2,0) i (0,2). Njutnov poligon polinoma $f(x,y)$ je duž sa celobrojnim temenima prikazana na slici 6.

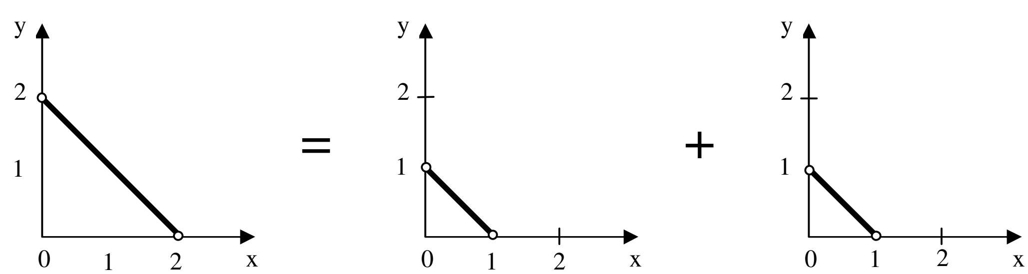


Slika 6

Jasno je da P_f može biti integralno rastavljen u smislu sume Minkovskog samo na jedan način:

$$P_f = conv((2,0),\ (0,2)) = conv((1,0),\ (0,1)) + conv((1,0),\ (0,1)),$$

što je prikazano na slici 7.



Slika 7

Koristeći komutativnost množenja u polju i s obzirom da nad poljem karakteristike 2 važi $xy + xy = 0$, dobijamo:

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

Drugim rečima, nad poljem karakteristike 2 važi:

$$(x+y)(x+y) = x^2 + y^2.$$

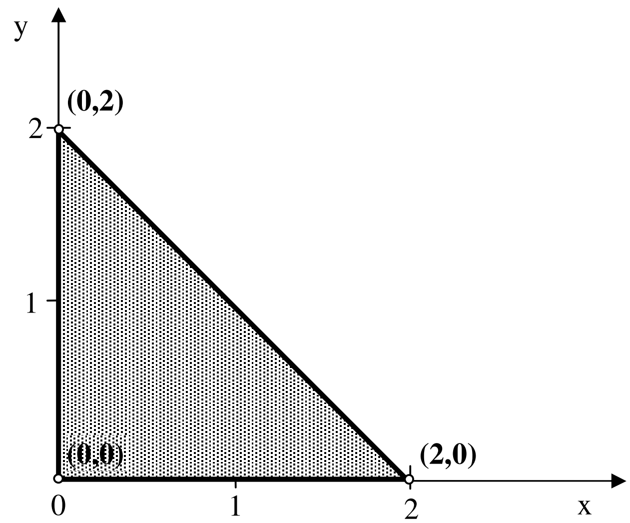
Odavde zaključujemo da se polazni polinom $f(x,y) = x^2 + y^2$ nad poljem karakteristike 2 može faktorisati na sledeći način:

$$f(x,y) = (x+y)(x+y).$$

<u>Primer 5:</u> Posmatrajmo polinom:

$$f(x,y) = x^2 + y^2 + 1.$$

Termima polinoma $f(x,y)$ sa nenula koeficijentima odgovaraju redom sledeći vektori eksponenata: (2,0), (0,2) i (0,0). Njutnov poligon polinoma $f(x,y)$ je trougao sa celobrojnim temenima prikazan na slici 8.

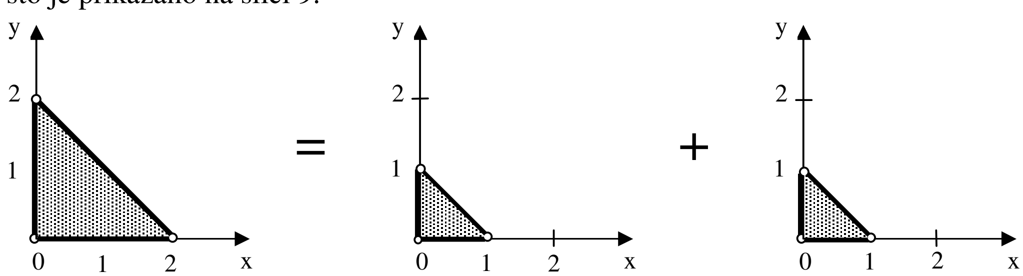


Slika 8

Jasno je da P_f može biti integralno rastavljen u smislu sume Minkovskog samo na jedan način:

$$P_f = conv((2,0), (0,2), (0,0)) = conv((1,0), (0,1), (0,0)) + conv((1,0), (0,1), (0,0)),$$

što je prikazano na slici 9.



Slika 9

Koristeći komutativnost množenja u polju dobijamo:

$$(x+y+1)(x+y+1) = x^2+yx+x+xy+y^2+y+x+y+1 = x^2+xy+x+xy+y^2+y+x+y+1$$

Kako nad poljem karakteristike 2 važi: $xy + xy = 0$, $x + x = 0$, $y + y = 0$, koristeći osobinu asocijativnosti sabiranja u polju iz prethodnog izraza dobijamo:

$$(x+y+1)(x+y+1) = x^2 + y^2 + 1 + (xy + xy) + (x + x) + (y + y) = x^2 + y^2 + 1.$$

Drugim rečima, nad poljem karakteristike 2 važi:

$$(x+y+1)(x+y+1) = x^2 + y^2 + 1.$$

Odavde zaključujemo da se polazni polinom $f(x,y) = x^2 + y^2 + 1$ nad poljem karakteristike 2 može faktorisati na sledeći način:

$$f(x,y) = (x+y+1)(x+y+1).$$

3. NEKE OSOBINE KONVEKSNIH SKUPOVA

Obeležimo sa $\mathbb{R}^2$ dvodimenzionalni Euklidski prostor. Elemente tog prostora $v=(x,y)$ nazivamo vektorima ili tačkama. Sa $\|v\|$ obeležimo Euklidsku normu (dužinu) vektora v:

$$\|v\| = \sqrt{x^2 + y^2}\ .$$

U prostoru $\mathbb{R}^2$ vektorska jednačina prave kroz tačke a i b ima sledeći oblik:

$$x = a + t(b - a) = (1 - t)a + tb,\ -\infty < t < \infty.$$

Zatvorena duž $[a,b]$ usmerena od tačke a ka tački b se dobija kada $t \in [0,1]$. Formalne definicije zatvorene i otvorene usmerene duži u $\mathbb{R}^2$ glase:

Definicija 4: Neka su a i b proizvoljne tačke u $\mathbb{R}^2$. ***Zatvorena duž [a,b] usmerena od tačke a ka tački b*** se definiše na sledeći način:

$$[a,b] = \{z \in \mathbb{R}^2 : z = (1-t)a + tb, \quad 0 \le t \le 1\}$$

ili ekvivalentno:

$$[a,b] = \{z \in \mathbb{R}^2 : z = \alpha a + \beta b,\ \alpha \ge 0,\ \beta \ge 0,\ \alpha + \beta = 1\}.$$

Otvorena duž usmerena od tačke a ka tački b u oznaci (a,b) se definiše na sledeći način:

$$(a,b) = \{z \in \mathbb{R}^2 : z = (1-t)a + tb, \quad 0 < t < 1\}$$

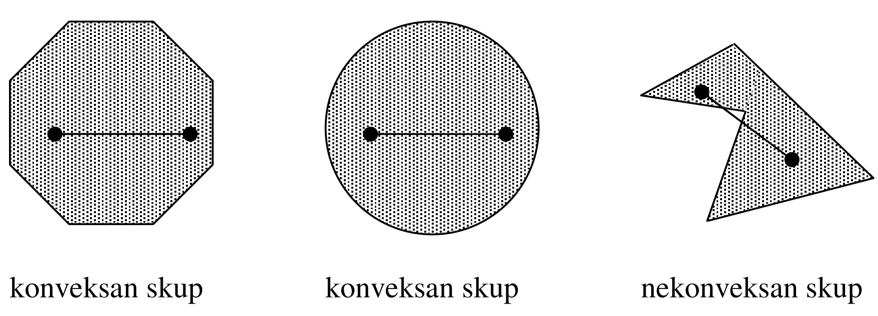
ili ekvivalentno:

$$(a,b) = \{z \in \mathbb{R}^2 : z = \alpha a + \beta b,\ \alpha > 0,\ \beta > 0,\ \alpha + \beta = 1\}.$$

Poluotvorena usmerena duž $[a,b)$ koja sadrži tačku a, ali ne sadrži tačku b se dobija kada parametar $t \in [0,1)$, odnosno za uslov $\alpha > 0$, $\beta \ge 0$, $\alpha + \beta = 1$. Poluotvorena usmerena duž $(a,b]$ se definiše potpuno analogno.

Definicija 5: Za skup $\mathcal{S}$, $\mathcal{S} \subseteq \mathbb{R}^2$, kažemo da je ***konveksan*** ako za bilo koje dve tačke a i b, $a,b \in \mathcal{S}$ važi $[a,b] \subseteq \mathcal{S}$.

Drugim rečima, skup je konveksan ako za svake svoje dve tačke sadrži i celu duž koja ih spaja. Na primer, tačka, prava i kružnica zajedno sa svojim unutrašnjim tačkama su konveksni skupovi u $\mathbb{R}^2$. Prazan skup i $\mathbb{R}^2$ su takođe konveksni. Primeri konveksnih i nekonveksnih skupova dati su na slici 10.



konveksan skup konveksan skup nekonveksan skup

Slika 10

Teorema 3: Neka je $\{C_i\}_{i\in \mathcal{I}}$ proizvoljna kolekcija konveksnih skupova u $\mathbb{R}^2$. Tada je i skup $\bigcap\limits_{i\in I} C_i$ konveksan.

Dokaz: Neka $a,b\in \bigcap\limits_{i\in I} C_i$. Po definiciji preseka skupova, to znači da $a,b\in C_i$, za sve $i\in \mathcal{I}$. Kako su C_i, $i\in \mathcal{I}$, konveksni skupovi, sledi da $[a,b]\subseteq C_i$, za sve $i\in \mathcal{I}$. Koristeći ponovo definiciju preseka skupova, zaključujemo da $[a,b]\subseteq \bigcap\limits_{i\in I} C_i$. Dakle, $\bigcap\limits_{i\in I} C_i$ je konveksan skup. □

Neka je $\mathcal{S}$, $\mathcal{S}\subseteq \mathbb{R}^2$, proizvoljan podskup $\mathbb{R}^2$. Primetimo da je konveksan omotač skupa $\mathcal{S}$ ($conv(\mathcal{S})$), definisan kao najmanji konveksan skup koji sadrži skup $\mathcal{S}$, zapravo presek svih konveksnih skupova koji sadrže $\mathcal{S}$. Dakle:

$$conv(\mathcal{S}) = \bigcap_{S\subseteq K_i} K_i,\ K_i \text{ konveksan skup.}$$

Kako je prazan skup konveksan, jasno je da važi $conv(\emptyset) = \emptyset$.

Napomena 4: Ako je skup $\mathcal{S}$, $\mathcal{S}\subseteq \mathbb{R}^2$, konačan, tj. $\mathcal{S}=\{a_1,..., a_k\}$, skup $conv(\mathcal{S})$ obeležavamo sa $conv(a_1,..., a_k)$ i nazivamo ga ***konveksni omotač tačaka $a_1,..., a_k$.***

Definicija 6: Neka $a_1,..., a_k\in \mathbb{R}^2$. Za tačku x kažemo da je ***konveksna kombinacija tačaka $a_1,..., a_k$*** ako postoje realni brojevi $\lambda_1,...,\lambda_k$ takvi da važi:

$$x = \lambda_1 a_1 + ... + \lambda_k a_k,\ \lambda_1 \ge 0,...,\lambda_k \ge 0,\ \lambda_1 + ... + \lambda_k = 1.$$

Sledećom teoremom ćemo pokazati da je konveksni omotač skupa $\mathcal{S}$ zapravo skup svih mogućih konveksnih kombinacija elemenata skupa $\mathcal{S}$.

Teorema 4: Neka je skup $\mathcal{S}$ proizvoljan podskup $\mathbb{R}^2$. Tada važi:

(1) $conv(\mathcal{S}) =\{ \sum\limits_{i=1}^{k} \lambda_i a_i :\ k \in \mathbb{N},\{a_1,..., a_k\}\subseteq\mathcal{S},\ \lambda_i \ge 0,\ i=1,...,k,\ \sum\limits_{i=1}^{k} \lambda_i = 1\}$

(2) Skup $\mathcal{S}$ je konveksan ako i samo ako $\mathcal{S} = conv(\mathcal{S})$

(3) Ako je skup $\mathcal{S}$ konačan, tj. $\mathcal{S}=\{a_1,...,a_m\}\subseteq \mathbb{R}^2$, tada je:

$$conv(\mathcal{S}) =\{ \lambda_1 a_1 + ... + \lambda_m a_m,\ \lambda_i \ge 0, i = 1,...,m,\ \sum_{i=1}^{m} \lambda_i = 1 \}$$

Dokaz:

(1) Označimo desnu stranu gornje jednakosti sa $\mathcal{D}$. Najpre ćemo dokazati da je skup $\mathcal{D}$ konveksan. Neka $x=\sum\limits_{i=1}^{k} \lambda_i x_i$, $y=\sum\limits_{i=1}^{m} \eta_i y_i \in \mathcal{D}$, pri čemu $x_1,...,x_k, y_1,..., y_m \in \mathcal{S}$, $\lambda_1,...,\lambda_k, \eta_1,...,\eta_m \ge 0$, $\lambda_1 + ... + \lambda_k = \eta_1 + ... + \eta_m = 1$. Treba pokazati da i $(1-\lambda)x + \lambda y \in \mathcal{D}$. Kako je $(1-\lambda)x + \lambda y = (1-\lambda)\sum\limits_{i=1}^{k} \lambda_i x_i + \lambda \sum\limits_{i=1}^{m} \eta_i y_i$, pri čemu: $(1-\lambda)\lambda_1,...,(1-\lambda)\lambda_k$, $\lambda\eta_1,..., \lambda\eta_m \ge 0$,

$$(1-\lambda)(\lambda_1 + ... + \lambda_k) + \lambda(\eta_1 + ... + \eta_m) = (1-\lambda) + \lambda = 1.$$

Zaključujemo da:

$$\left(1-\lambda\right)x+\lambda y\in \mathcal{D}.$$

Kako je $conv(\mathcal{S})$ najmanji konveksan skup koji sadrži skup $\mathcal{S}$, a $\mathcal{D}$ je konveksan skup koji sadrži skup $\mathcal{S}$, očigledno je da važi: $conv(\mathcal{S})\subseteq\mathcal{D}$.

Indukcijom po k pokažimo da važi i obrnuta inkluzija $\mathcal{D}\subseteq conv(\mathcal{S})$. Za $k=1$, jasno je da važi: $1x_1 = x_1\in\mathcal{S}\subseteq conv(\mathcal{S})$.

Pretpostavimo da inkluzija $\mathcal{D}\subseteq conv(\mathcal{S})$ važi za $k-1$. Posmatrajmo, zatim, bilo koji konačan skup $\{x_1,...,x_k\}\subseteq\mathcal{S}$ i parametre $\lambda_1,...,\lambda_k \geq 0$, $\lambda_1+...+\lambda_k=1$ i pokažimo da se tačka $\lambda_1 x_1+...+\lambda_k x_k$ nalazi u $conv(\mathcal{S})$. Zaista:

$$\lambda_1 x_1+...+\lambda_k x_k=\left(1-\lambda_k\right)\left(\tfrac{\lambda_1}{1-\lambda_k}x_1+...+\tfrac{\lambda_{k-1}}{1-\lambda_k}x_{k-1}\right)+\lambda_k x_k .$$

Naravno, pretpostavka je da je $\lambda_k<1$. Naime, ako je $\lambda_k=1$ iz gornjih uslova dobijamo da je $\lambda_1 x_1+...+\lambda_k x_k=x_k$, a $x_k\in\mathcal{S}\subseteq conv(\mathcal{S})$.

Uvedimo oznaku: $z=\tfrac{\lambda_1}{1-\lambda_k}x_1+...+\tfrac{\lambda_{k-1}}{1-\lambda_k}x_{k-1}$. S obzirom da je $\tfrac{\lambda_1}{1-\lambda_k}+...+\tfrac{\lambda_{k-1}}{1-\lambda_k}=\tfrac{\lambda_1+\lambda_{k-1}}{1-\lambda_k}=\tfrac{1-\lambda_k}{1-\lambda_k}=1$, po indukcijskoj pretpostavci zaključujemo da $z\in conv(\mathcal{S})$. Dalje dobijamo:

$$\lambda_1 x_1+...+\lambda_k x_k=\left(1-\lambda_k\right)z+\lambda_k x_k ,$$

pri čemu $z\in conv(\mathcal{S})$, $x_k\in\mathcal{S}\subseteq conv(\mathcal{S})$ i $\left(1-\lambda_k\right)+\lambda_k=1, \lambda_k\geq 0$.

Kako je $0\leq\lambda_k\leq 1$, jasno je da važi i $1-\lambda_k\geq 0$. Odavde na osnovu indukcijske pretpostavke zaključujemo da:

$$\left(1-\lambda_k\right)z+\lambda_k x_k\in conv(\mathcal{S}),$$

pa važi i

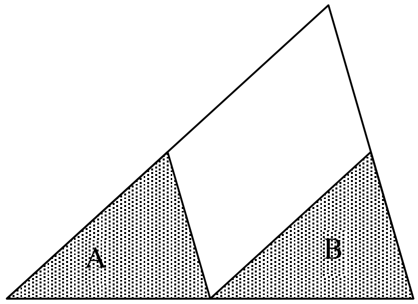
$$\lambda_1 x_1+...+\lambda_k x_k\in conv(\mathcal{S}).$$

(2) Neka je $\mathcal{S}$ konveksan skup. Uvek važi $\mathcal{S}\subseteq conv(\mathcal{S})$. Kako je $conv(\mathcal{S})$ najmanji konveksan skup koji sadrži skup $\mathcal{S}$, a $\mathcal{S}$ konveksan skup koji, očigledno, sadrži skup $\mathcal{S}$ važi i $conv(\mathcal{S})\subseteq\mathcal{S}$.

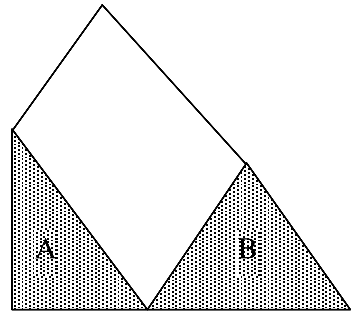
Neka važi $\mathcal{S}= conv(\mathcal{S})$. Kako je $conv(\mathcal{S})$ konveksan skup, zaključujemo da je i $\mathcal{S}$ konveksan.

(3) Ovo tvrđenje je očigledna posledica tvrđenja ***(1)***. □

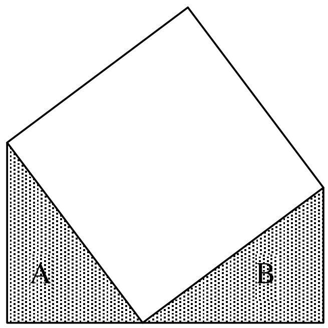
Sada ćemo se podsetiti nekih važnih osobina sume Minkovskog. Suma dva trougla A i B u ravni je trougao, četvorougao, petougao ili šestougao, što je prikazano na slikama 11.1-11.4.



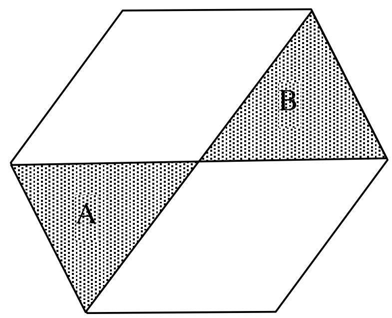
Slika 11.1



Slika 11.2

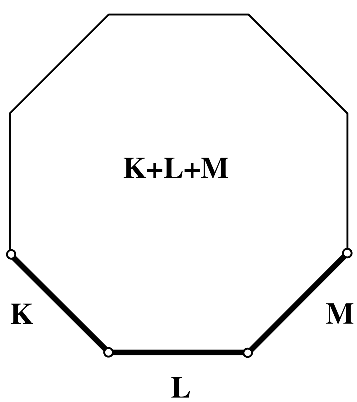


Slika 11.3



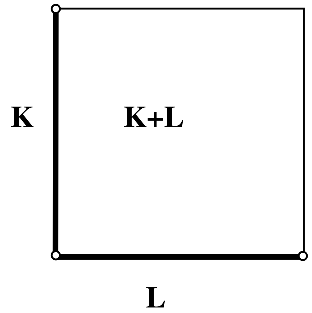
Slika 11.4

Svaki centralno simetričan dvodimenzionalni $2n$-gon može se predstaviti kao suma n duži. Pravilan šestougao u ravni može se predstaviti kao suma tri duži K, L i M (slika 12), ali i kao suma dva trougla A i B, kao što je prikazano na slici 11.4. Dakle, predstavljanje konveksnog i kompaktnog skupa kao konačne sume konveksnih i kompaktnih skupova, ako je moguće, nije jedinstveno.



Slika 12

Jasno, pravougaonik - centralno simetričan dvodimenzionalni četvorougao u ravni može se predstaviti kao suma dve duži, što je prikazano na slici 13.



Slika 13

Teorema 5: ***(1)*** Neka je sa τ obeležena translacija, tada za proizvoljne skupove A i B u $\mathbb{R}^2$ važi:

$$\tau(A)+B=\tau(A+B)=A+\tau(B)$$

(2) Ako su A i B oba konveksni, zatvoreni i konveksni ili kompaktni i konveksni skupovi u $\mathbb{R}^2$, onda je i $A+B$ konveksan, zatvoren i konveksan ili kompaktan i konveksan skup.

Dokaz:

(1) Ako je translacija τ definisana vektorom t, važi:

$$(t+A)+B=t+(A+B)=A+(t+B),$$

a odavde direktno sledi tvrđenje teoreme.

(2) Pokažimo da ako su A i B konveksni skupovi u $\mathbb{R}^2$, onda je to i skup $A+B$. Skup $A+B$ je konveksan ako za proizvoljne $a+b\in A+B$ i $a'+b'\in A+B$ i proizvoljno λ, $0\le\lambda\le 1$, važi da:

$$\lambda(a+b)+(1-\lambda)(a'+b')\in A+B.$$

Kako $a+b\in A+B$ i $a'+b'\in A+B$, jasno je da $a, a'\in A$ i $b, b'\in B$.

$$\lambda(a+b)+(1-\lambda)(a'+b')=\lambda a+\lambda b+(1-\lambda)a'+(1-\lambda)b'=\lambda a+(1-\lambda)a'+\lambda b+(1-\lambda)b',$$

Kako $a, a'\in A$, a skup A konveksan pa sadrži svaku konveksnu kombinaciju svojih elemenata, zaključujemo da važi: $\lambda a+(1-\lambda)a'\in A$. Potpuno analogno zaključujemo da $\lambda b+(1-\lambda)b'\in B$. Konačno dobijamo:

$$\lambda(a+b)+(1-\lambda)(a'+b')\in A+B,$$

što je i trebalo pokazati.

Ako su A i B zatvoreni i ograničeni skupovi u $\mathbb{R}^2$, onda je to i skup $A+B$, jer je suma Minkovskog neprekidna operacija i preslikava parove ograničenih skupova na ograničen skup. □

Napomena 5:

(1) Suma Minkovskog može se zapisati u formi: $A+B=\bigcup\limits_{b\in B}(A+b)$.

(2) Ako $\lambda\in\mathbb{R}$ i $A\subseteq\mathbb{R}^2$, onda skup λA definišemo na sledeći način:

$$\lambda A=\{\lambda a : a\in A\}.$$

Ako su dati $\lambda_1,...,\lambda_k \in \mathbb{R}$ i skupovi $A_1,...,A_k \subseteq \mathbb{R}^2$, onda $\lambda_1 A_1 + ... + \lambda_k A_k$ nazivamo ***linearnom kombinacijom skupova*** $A_1,...,A_k$, pri čemu neki od koeficijenata $\lambda_1,...,\lambda_k$ mogu biti negativni.

Međutim, $(-1)A = -A$ nije suprotan element za A u smislu sume Minkovskog. Zaista, na slici 11.4. jasno je da je $B = -A$, ali $A + B$ nije prazan skup, nego šestougao.

Teorema 6: Ako su $A_1,...,A_k$ konveksni skupovi u $\mathbb{R}^2$ i $\lambda_1,...,\lambda_k$ realni brojevi, onda je $\lambda_1 A_1 + ... + \lambda_k A_k$ konveksan.

Dokaz:

Neka x, $y \in \lambda_1 A_1 + ... + \lambda_{k-1} A_{k-1} + \lambda_k A_k$ i neka je λ proizvoljno $0 \le \lambda \le 1$ fiksirano, treba pokazati da:

$$\lambda x + (1-\lambda)\, y \in \lambda_1 A_1 + ... + \lambda_{k-1} A_{k-1} + \lambda_k A_k .$$

Kako $x \in \lambda_1 A_1 + ... + \lambda_{k-1} A_{k-1} + \lambda_k A_k$, to znači da je $x = \lambda_1 x_1 + ... + \lambda_{k-1} x_{k-1} + \lambda_k x_k$, za neke $x_1,..., x_{k-1}, x_k$ takve da je: $x_1 \in A_1,...,\ x_{k-1} \in A_{k-1},\ x_k \in A_k$.

Kako $y \in \lambda_1 A_1 + ... + \lambda_{k-1} A_{k-1} + \lambda_k A_k$, to znači da je $y = \lambda_1 y_1 + ... + \lambda_{k-1} y_{k-1} + \lambda_k y_k$, za neke $y_1,..., y_{k-1}, y_k$ takve da je: $y_1 \in A_1,...,\ y_{k-1} \in A_{k-1},\ y_k \in A_k$.

Dobijamo:

$$\lambda x + (1-\lambda)\, y = \lambda\left(\lambda_1 x_1 + ... + \lambda_{k-1} x_{k-1} + \lambda_k x_k\right) + (1-\lambda)\left(\lambda_1 y_1 + ... + \lambda_{k-1} y_{k-1} + \lambda_k y_k\right),$$

odnosno:

$$\lambda x + (1-\lambda)\, y = \lambda\lambda_1 x_1 + ... + \lambda\lambda_{k-1} x_{k-1} + \lambda\lambda_k x_k + (1-\lambda)\lambda_1 y_1 + ... + (1-\lambda)\lambda_{k-1} y_{k-1} + (1-\lambda)\lambda_k y_k .$$

Kako je množenje realnih brojeva komutativno, sledi:

$$\lambda x + (1-\lambda)\, y = \lambda_1 \lambda x_1 + ... + \lambda_{k-1} \lambda x_{k-1} + \lambda_k \lambda x_k + \lambda_1 (1-\lambda)\, y_1 + ... + \lambda_{k-1} (1-\lambda)\, y_{k-1} + \lambda_k (1-\lambda)\, y_k .$$

Dalje dobijamo:

$$\lambda x + (1-\lambda)\, y = \lambda_1 \left(\lambda x_1 + (1-\lambda)\, y_1\right) + ... + \lambda_{k-1} \left(\lambda x_{k-1} + (1-\lambda)\, y_{k-1}\right) + \lambda_k \left(\lambda x_k + (1-\lambda)\, y_k\right).$$

Kako je A_1 konveksan, jasno je da za $x_1, y_1 \in A_1$ važi da i $\lambda x_1 + (1-\lambda)\, y_1 \in A_1$.

Potpuno analogno zaključujemo da:

$$\lambda x_2 + (1-\lambda)\, y_2 \in A_2,...,\ \lambda x_{k-1} + (1-\lambda)\, y_{k-1} \in A_{k-1},\ \lambda x_k + (1-\lambda)\, y_k \in A_k .$$

Konačno dobijamo:

$$\lambda x + (1-\lambda)\, y \in \lambda_1 A_1 + ... + \lambda_{k-1} A_{k-1} + \lambda_k A_k ,$$

što je i trebalo pokazati. □

4. POTPORNE PRAVE I LICA POLIGONA

Neka je $P \subset \mathbb{R}^2$ konveksan poligon u ravni. Kao što je poznato, skalarni proizvod je neprekidna funkcija, a konveksan poligon kompaktan skup, tako da za proizvoljan nenula vektor $v = (v_1, v_2) \in \mathbb{R}^2$ važi:

$$\sup_{p \in P} p \cdot v = \max\{p \cdot v \mid p \in P\},$$

gde je:

$$p \cdot v = p_1 v_1 + p_2 v_2$$

skalarni proizvod vektora $p = (p_1, p_2)$ i $v = (v_1, v_2)$.

Definicija 7: Neka je $P \subset \mathbb{R}^2$ konveksan poligon u ravni. Preslikavanje:

$$h_P(v) : \mathbb{R}^2 \to \mathbb{R},\ v \to \sup_{p \in P} p \cdot v$$

naziva se ***potporna funkcija*** poligona *P*.

Definicija 8: Neka $v \in \mathbb{R}^2$ i $s \in \mathbb{R}$. Skup tačaka:

$$H = \{x \in \mathbb{R}^2 : v \cdot x = s\}$$

je prava u $\mathbb{R}^2$. ***Zatvorene poluravni određene sa H*** definisane su na sledeći način:

$$H^- = \{x \in \mathbb{R}^2 : v \cdot x \le s\},\ H^+ = \{x \in \mathbb{R}^2 : v \cdot x \ge s\}.$$

Definicija 9: Prava H_P naziva se ***potporna prava*** konveksnog poligona $P \subset \mathbb{R}^2$ ako $P \subset H_P^-$ ili $P \subset H_P^+$ i $P \cap H_P \ne \emptyset$, tj. H_P sadrži rubnu tačku poligona *P*.
Potporna prava H_P konveksnog poligona $P \subset \mathbb{R}^2$ naziva se ***netrivijalna potporna prava*** ako skup *P* nije sadržan u H_P.
Skupovi H_P^- i H_P^+ nazivaju se ***potpornim poluravnima*** poligona *P*.

Napomena 6: Jedini konveksan poligon koji ima trivijalnu potpornu pravu je duž.

Teorema 7:
(1) Ako je $P + a$ translacija konveksnog poligona $P \subset \mathbb{R}^2$, onda je:

$$h_{P+a}(v) = h_P(v) + av,\ \text{za sve}\ v \in \mathbb{R}^2.$$

(2) Za svaki nenula vektor $v \in \mathbb{R}^2$, prava

$$H_P(v) = \{x \in \mathbb{R}^2 : x \cdot v = h_P(v)\},\ (\square)$$

je potporna prava konveksnog poligona *P*.
(3) Svaka potporna prava poligona *P* ima reprezentaciju u formi $(\square)$.

Dokaz:
(1) Za svaki vektor $v \in \mathbb{R}^2$ važi:

$h_{P+a}(v) = \sup_{x\in P+a} x\cdot v = \sup_{x\in P}(x+a)\cdot v = \sup_{x\in P}(x\cdot v + a\cdot v) = \sup_{x\in P} x\cdot v + a\cdot v = h_P(v) + a\cdot v$

(2) Kako je funkcija skalarnog proizvoda $f(x) = x\cdot v$ neprekidna, očigledno je neprekidna i potporna funkcija konveksnog poligona P, $h_P(v) = \sup_{x\in P} x\cdot v$.

Konveksan poligon je zatvoren i ograničen, tj. kompaktan skup, a neprekidna funkcija $h_P(v)$ na kompaktnom skupu P dostiže maksimum, jasno je da postoji $x_0 \in P$ takav da važi:

$$h_P(v) = x_0\cdot v.$$

Dakle, za bilo koje $x\in P$ važi:

$$x\cdot v \le x_0\cdot v,$$

što znači:

$$P \subset H_P^-(v),$$

tj. $H_P(v)$ je potporna prava poligona P.

(3) Neka je $H_P(v) = \{x\in\mathbb{R}^2 : x\cdot v = x_0\cdot v\}$ potporna prava poligona P u tački x_0. Jasno, možemo izabrati nenula vektor $v\in\mathbb{R}^2$ za koji važi:

$$P \subset H_P^-(v).$$

Tada za taj vektor v važi:

$$x_0\cdot v = \sup_{x\in P} x\cdot v = h_P(v).$$

Dakle, $H_P(v)$ potporna prava poligona P u tački x_0 može se zapisati i na sledeći način:

$$H_P(v) = \{x\in\mathbb{R}^2 : x\cdot v = h_P(v)\},$$

što je i trebalo pokazati. □

Napomena 7: Pojmovi potporne funkcije i potporne prave mogu se definisati za proizvoljan konveksan i kompaktan skup, ne obavezno konveksan poligon. Stoga, tvrđenje prethodne teoreme važi i za proizvoljan konveksan i kompaktan skup, ne samo za konveksan poligon. S obzirom da je Njutnov poligon proizvoljnog polinoma sa dve promenljive konveksan, definicije i tvrđenja u ovom radu su data za konveksne poligone.

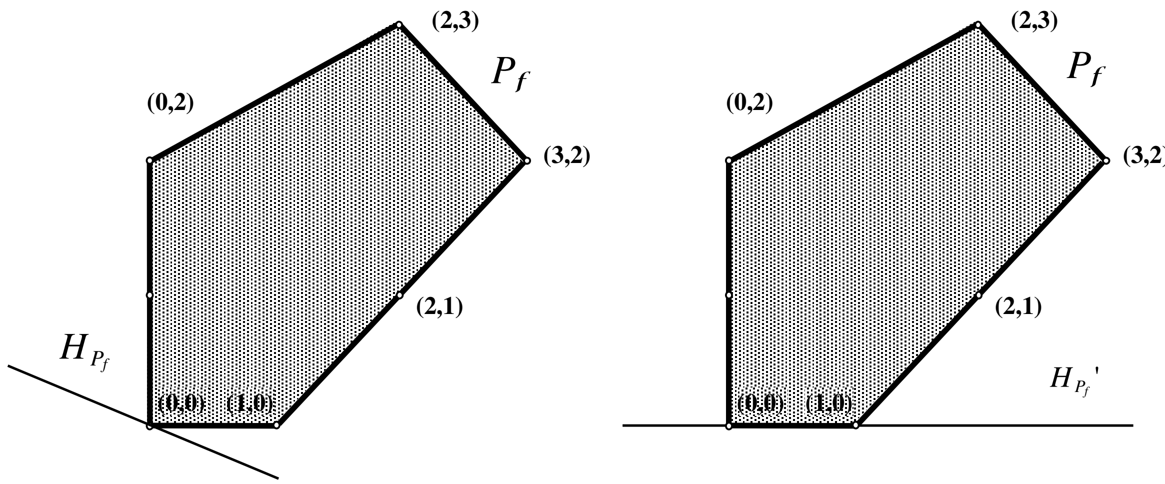
Definicija 10: Neka je P_f Njutnov poligon polinoma $f(x,y)$ i H_{P_f} njegova potporna prava. Presek poligona P_f i prave H_{P_f} se naziva ***lice poligona*** P_f ***u odnosu na potpornu pravu*** H_{P_f}.

Napomena 8: Kako svaka potporna prava poligona P_f ima neprazan presek sa tim poligonom i poligon je sadržan u jednoj od dve zatvorene poluravni određene tom pravom, zaključujemo da lice Njutnovog poligona polinoma $f(x,y)$ može biti teme ili ivica poligona P_f, u zavisnosti od potporne prave.

Primer 6: Posmatrajmo polinom:

$$f(x,y) = x^3y^2 + x^2y^3 + x^2y + y^2 + x + 1.$$

Konstrukciju Njutnovog poligona polinoma $f(x,y)$ (P_f) opisali smo u primeru 1. Na slici 14 dajemo primer dve potporne prave poligona P_f. U prvom slučaju lice poligona u odnosu na potpornu pravu H_{P_f} je teme (0,0), a u drugom slučaju lice poligona u odnosu na potpornu pravu H_{P_f}' ivica poligona P_f koja spaja temena (0,0) i (1,0).



Slika 14

Sledeća teorema daje najvažnije osobine dekompozicije poligona. Kao što ćemo videti, suma Minkovskog očuvava aditivnost potporne funkcije.

Teorema 8:

(1) Neka su $h_K(v)$ i $h_L(v)$ potporne funkcije konveksnih poligona $K, L \subset \mathbb{R}^2$ u odnosu na proizvoljan vektor $v \in \mathbb{R}^2$, $v = (u, w)$, gde su $u, w > 0$. Tada je $h_K(v) + h_L(v)$ potporna funkcija kompaktnog i konveksnog skupa $K + L$, tj.

$$h_{K+L}(v) = h_K(v) + h_L(v).$$

(2) $H_{K+L}(v) = H_K(v) + H_L(v)$.

(3) Ako je F lice kompaktnog i konveksnog skupa $K + L$, onda postoje jedinstvena lica F_K i F_L skupova K i L takva da važi:

$$F = F_K + F_L.$$

Svako teme $K + L$ je suma temena K i L.

(4) Ako su K i L konveksni poligoni, onda je to i $K + L$.

Dokaz:

(1) Kako su konveksni poligoni K, L kompaktni, znamo da je i $K + L$ kompaktan.

Pokažimo da je $K+L$ konveksan skup. Ako su K i L dve duži u ravni koje nisu paralelne tada je $K+L$ paralelogram. Ako su K i L dve duži u ravni koje su paralelne tada je $K+L$ duž paralelna K i L čija je dužina zbir dužina K i L. Neka su K i L dva konveksne figure i $P=K+L$. Uzmimo proizvoljne $C,D\in P$. Po definiciji sume Minkovskog, postoje tačke $A_1,A_2\in K$ (koje mogu da se poklapaju) i $B_1,B_2\in L$ (koje mogu da se poklapaju), takve da je:

$$C=A_1+B_1 \text{ i } D=A_2+B_2.$$

Kako je K konveksna figura duž $conv(A_1,A_2)\in K$. Potpuno analogno dobijamo da $conv(B_1,B_2)\in L$. Paralelogram (ili duž) dobijen kao suma Minkovskog:

$$conv(A_1,A_2)+conv(B_1,B_2)$$

pripada P zajedno sa unutrašnjim tačkama.

Tačke duži $conv(C,D)$ pripadaju dijagonali tog paralelograma. Kako smo tačke C,D birali proizvoljno, sledi da je P konveksna figura.

Uzmimo, sada, proizvoljan vektor $v\in\mathbb{R}^2$, $v=(u,w)$, gde su $u,w>0$. Za taj vektor v važi:

$$h_{K+L}(v)=\sup_{x\in K,y\in L}(x+y)\cdot v=\sup_{x\in K,y\in L}(x\cdot v+y\cdot v)=\sup_{x\in K}x\cdot v+\sup_{y\in L}y\cdot v=h_K(v)+h_L(v)$$

(2) Pokažimo najpre: $H_{K+L}(v)\subseteq H_K(v)+H_L(v)$. Neka je:

$$(x,y)\in H_{K+L}(v)=\left\{(a,b)\in\mathbb{R}^2\,\middle|\,(a,b)\cdot(u,w)=h_{K+L}(v)\right\}, \text{ gde je } v=(u,w).$$

Na osnovu ***(1)*** znamo da je:

$$(\ast)\quad (x,y)\cdot(u,w)=h_{K+L}(v)=h_K(v)+h_L(v).$$

Jasno:

$$h_K(v)=\sup_{(a,b)\in K}\left[(a,b)\cdot(u,w)\right]$$

i

$$h_L(v)=\sup_{(c,d)\in L}\left[(c,d)\cdot(u,w)\right].$$

Pošto su K i L kompaktni skupovi, supremum se na njima dostiže, tj. postoje tačke $(a_0,b_0)\in K$ i $(c_0,d_0)\in L$ takve da važi:

$$(\ast\ast)\quad h_K(v)=\sup_{(a,b)\in K}\left[(a,b)\cdot(u,w)\right]=(a_0,b_0)\cdot(u,w)$$

i

$$(\ast\ast\ast)\quad h_L(v)=\sup_{(c,d)\in L}\left[(c,d)\cdot(u,w)\right]=(c_0,d_0)\cdot(u,w).$$

Uvrštavanjem $(\ast\ast)$ i $(\ast\ast\ast)$ u $(\ast)$ dobijamo:

$$(x,y)\cdot(u,w)=(a_0,b_0)\cdot(u,w)+(c_0,d_0)\cdot(u,w),$$

odnosno:

$$(x,y)\cdot(u,w)=(a_0+c_0,b_0+d_0)\cdot(u,w).$$

Odavde dobijamo:

$$(x,y)\cdot(u,w)-(a_0+c_0,b_0+d_0)\cdot(u,w)=0,$$

odnosno:

$$\left[(x,y)-(a_0+c_0,b_0+d_0)\right]\cdot(u,w)=0,$$

pa je:

$$\left[x-(a_0+c_0),\,y-(b_0+d_0)\right]\cdot(u,w)=0.$$

S obzirom da je $u,w>0$, zaključujemo da važi:

$$\left(x-(a_0+c_0),\,y-(b_0+d_0)\right)=(0,0),$$

tj.

$$x=a_0+c_0 \text{ i } y=b_0+d_0.$$

Dakle:

$$(x,y)=(a_0+c_0,b_0+d_0)=(a_0,b_0)+(c_0,d_0).$$

Kako $(a_0,b_0)\in H_K(v)$ i $(c_0,d_0)\in H_L(v)$, očigledno je:

$$(x,y)\in H_K(v)+H_L(v).$$

Pokažimo i obrnutu inkluziju $H_K(v)+H_L(v)\subseteq H_{K+L}(v)$. Neka

$$(x,y)\in H_K(v)+H_L(v).$$

Tada postoje $(x_K,y_K)\in H_K$ i $(x_L,y_L)\in H_L$ takvi da važi:

$$x=x_K+x_L \text{ i } y=y_K+y_L.$$

S obzirom da $(x_K,y_K)\in H_K$ važi:

$$\sup_{(a,b)\in K}\left[(a,b)\cdot(u,w)\right]=(x_K,y_K)\cdot(u,w)=h_K(v).$$

Kako $(x_L,y_L)\in H_L$ važi:

$$\sup_{(c,d)\in L}\left[(c,d)\cdot(u,w)\right]=(x_L,y_L)\cdot(u,w)=h_L(v).$$

Sabiranjem poslednje dve jednakosti dobijamo:

$$(x_K,y_K)\cdot(u,w)+(x_L,y_L)\cdot(u,w)=h_K(v)+h_L(v),$$

odnosno:

$$(x_K+x_L,\,y_K+y_L)\cdot(u,w)=h_K(v)+h_L(v).$$

Na osnovu ***(1)*** sledi:

$$(x_K+x_L,\,y_K+y_L)\cdot(u,w)=h_{K+L}(v).$$

Odavde sledi da je:

$$(x_K+x_L,\,y_K+y_L)\in H_{K+L}(v),$$

tj.

$$(x,y)\in H_{K+L}(v).$$

(3) Na osnovu ***Teoreme 7***, slučaj ***(2)***, za kompaktan i konveksan skup *K+L* i nenula vektor *v* sa ciljnom tačkom izvan skupa *K+L*, prava $H_{K+L}(v)=\left\{x\in\mathbb{R}^2 : x\cdot v=h_{K+L}(v)\right\}$ je potporna prava skupa *K+L*. Onda je $F=(K+L)\cap H_{K+L}(v)$ lice poligona *K+L* u odnosu na potpornu pravu $H_{K+L}(v)$. Potpuno analogno, za kompaktne i konveksne skupove *K* i *L* i odabrani vektor *v* biramo njihove potporne prave $H_K(v)=\left\{x\in\mathbb{R}^2 : x\cdot v=h_K(v)\right\}$ i $H_L(v)=\left\{x\in\mathbb{R}^2 : x\cdot v=h_L(v)\right\}$. Neka su lica skupova *K* i *L* u odnosu na date potporne prave su: $F_K=K\cap H_K(v)$ i

$F_L = L \cap H_L(v)$. Očigledno je da su prave $H_{K+L}(v)$, $H_K(v)$ i $H_L(v)$ paralelne i važi: $H_{K+L}(v) = H_K(v) + H_L(v)$. Možemo pretpostaviti da važi $H_K(v) = H_L(v)$, do na translaciju skupa *L*. Dalje dobijamo:

$$F = (K+L) \cap H_{K+L}(v) = (K+L) \cap (H_K(v) + H_L(v)) = (K \cap H_K(v)) + (L \cap H_L(v)) = F_K + F_L$$

Jedinstvenost F_K i F_L sledi iz ***(1)***.

(4) Za konveksne poligone K i L, pokazali smo da je $K+L$ kompaktan i konveksan skup. Uočimo dva proizvoljna temena poligona K i L - v_K i v_L. Odaberimo vektor v tako da lica poligona K i L u odnosu na potporne prave $H_K(v)$ i $H_L(v)$ budu v_K i v_L. Tada: $v_K + v_L \in H_K(v) + H_L(v)$. Na osnovu ***(2)*** sledi: $v_K + v_L \in H_{K+L}(v)$. Drugim rečima, suma Minkovskog dva temena je svakako tačka ruba skupa $K+L$. Pokazaćemo da je $K+L$ poligon koji nastaje kao konveksan omotač svih tačaka oblika $v_K + v_L$, gde su v_K i v_L temena poligona K i L. S obzirom na konveksnost skupa $K+L$ dovoljno je pokazati da, osim tačaka oblika $v_K + v_L$, ne postoji ni jedna tačka $K+L$ čije je lice u odnosu na neku potpornu pravu samo ta tačka. Naime, ako bi postojala takva tačka F, onda bi prema ***(3)*** ove teoreme postojala jedinstvena lica poligona K i L - F_K i F_L takva da je: $F = F_K + F_L$. Kako je F tačka, očigledno je da i F_K i F_L moraju biti tačke, tj. temena poligona K i L, odnosno F je oblika $F = v_K + v_L$, što je kontradikcija. $\square$

Sledeća teorema je važna posledica Teoreme 8.

<u>Teorema 9:</u>
Ako za konveksne poligone $A, B, C \subset \mathbb{R}^2$ važi: $A + C = B + C$, tada je: $A = B$.

Dokaz:
Neka je v nenula vektor sa ciljnom tačkom izvan skupa $A+C$. Dalje, za taj vektor v definišemo: $h_{A+C}(v) = \sup_{p \in A+C} p \cdot v$, potpornu funkciju poligona $A+C$ u odnosu na vektor dati vektor *v*. Tada je prava:

$$H_{A+C}(v) = \{x \in \mathbb{R}^2 : x \cdot v = h_{A+C}(v)\}$$

potporna prava skupa $A+C$. Neka je $F_{A+C} = (A+C) \cap H_{A+C}(v)$ lice poligona $A+C$ u odnosu na pravu $H_{A+C}(v)$. Bez umanjenja opštosti, pretpostavimo da je lice poligona $A+C$ u odnosu na pravu tačka - teme poligona $A+C$. Naime, ako za izabrani vektor v dobijamo da je lice poligona $A+C$ duž, odaberimo drugi vektor v' sa ciljnom tačkom izvan skupa $A+C$ tako da za taj vektor odgovarajuće lice poligona bude teme.
Na osnovu ***Teoreme 8***, stavka ***(3)*** za teme F_{A+C} poligona $A+C$ postoje jedinstvena temena poligona A i C, F_A i F_C, čija je suma upravo F_{A+C}:

$$F_{A+C} = F_A + F_C .$$

Potpuno analogno, za teme F_{A+C} poligona $B+C$ postoje jedinstvena temena poligona B i C, F_B i F_C', čija je suma upravo F_{A+C}:

$$F_{A+C} = F_B + F_C'.$$

Kako se svako teme poligona $A+C$ na jedinstven način može predstaviti kao suma Minkovskog jednog temena poligona A i jednog temena poligona C, zaključujemo da važi:

$$F_A = F_B \text{ i } F_C = F_C'.$$

S obzirom da je izbor vektora v bio slučajan, pravac potporne prave smo slobodno birali, zaključujemo da poligoni A i B imaju ista temena. Kako je svaki poligon konveksan omotač svojih temena, dobijamo: $A = B$. □

Napomena 9: U daljem tekstu ćemo skup konveksnih poligona u $\mathbb{R}^2$ obeležavati sa $\mathcal{K}(\mathbb{R}^2)$. Na osnovu prethodne teoreme zaključujemo da je $(\mathcal{K}(\mathbb{R}^2),+)$ komutativna polugrupa sa zakonom kancelacije.

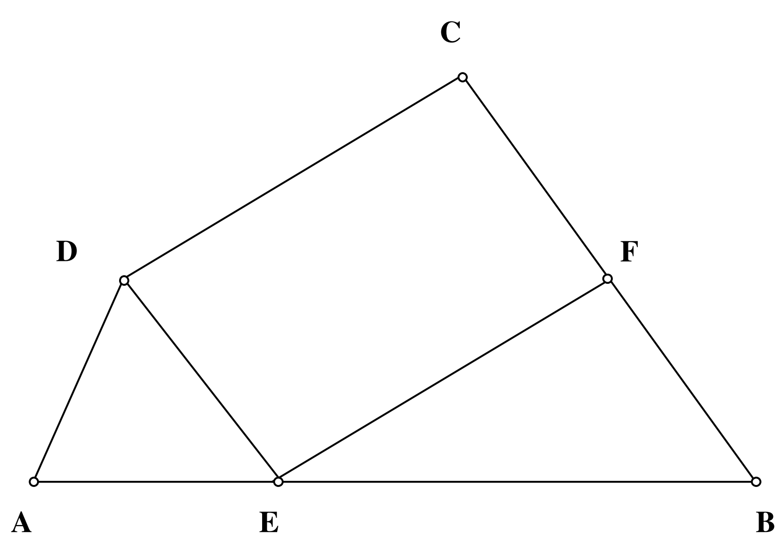
Napomena 10: Primetimo da obrat ***Teoreme 8***, stavka ***(3)*** ne važi. Dakle, ako su F_Q i F_P lica Q i P, tada $F_Q + F_P$ nije obavezno lice $Q+P$. Zaista, posmatrajmo četvorougao $conv(A,B,C,D)$ prikazan slici 15 koji se može predstaviti kao suma Minkovskog dva trougla, $\triangle AED$ i $\triangle EBF$. Dakle važi:

$$conv(A,B,C,D) = conv(A,E,D) + conv(E,B,F).$$

Međutim, jasno je da važi:

$$conv(E,D) + conv(E,F) = conv(E,F,C,D),$$

odnosno, duži $conv(E,D)$ i $conv(E,F)$ su lica poligona $\triangle AED$ i $\triangle EBF$, ali njihova suma – paralelogram $conv(E,F,C,D)$ nije lice poligona $conv(A,B,C,D)$.



Slika 15

Napomena 11: Neka su A, B i C konveksni poligoni u $\mathbb{R}^2$ takvi da važi: $C = A + B$. Na osnovu ***Teoreme 8***, stavka **(*3*)**, svaka ivica poligona C može se predstaviti jedinstveno kao suma Minkovskog jedne ivice poligona A i jedne ivice poligona B, pri čemu jedna od njih može biti tačka. Obrnuto, svaka ivica poligona A i B je poligon sabirak tačno jedne ivice poligona C.

5. INTEGRALNO NERASTAVLJIVI POLIGONI

U ovom poglavlju bavićemo se pronalaženjem integralno nerastavljivih poligona i daćemo primere apsolutno nesvodljivih polinoma nad proizvoljnim poljem pridruženih ovim poligonima.
Za konveksan poligon sa celobrojnim temenima u Euklidskoj ravni $\mathbb{R}^2$ možemo konstruisati konačan niz vektora pridruženih njegovim ivicama na dole opisan način. Neka su redom $v_0, v_1, ..., v_{n-1}, v_n = v_0$ temena poligona u smeru suprotnom od smera kretanja kazaljke na satu.
Ivice poligona mogu se predstaviti vektorima $E_i = v_i - v_{i-1} = (a_i, b_i), 1 \le i \le n$, pri čemu $a_i, b_i \in \mathbb{Z}$. Vektore E_i nazivamo ***ivičnim vektorima***.

<u>Definicija 11:</u> Vektor $v = (x, y) \in \mathbb{Z}^2$ se naziva ***primitivni vektor*** ako je $NZD(x, y) = 1$.

Ako definišemo $c_i = NZD(a_i, b_i)$, tada su vektori $e_i = \left(\frac{a_i}{c_i}, \frac{b_i}{c_i}\right)$, $1 \le i \le n$ primitivni vektori.
Jasno, $E_i = c_i e_i$, $1 \le i \le n$.
Svaki ivični vektor E_i sadrži tačno $c_i + 1$ celobrojnih tačaka, uključujući svoje krajnje tačke, što će biti pokazano u ***Teoremi 11***.

<u>Definicija 12:</u> Niz vektora $\{c_i e_i\}_{1 \le i \le n}$ se naziva ***poligonalni niz vektora (ivični niz vektora)***.

<u>Napomena 12:</u> Poligonalni niz vektora jedinstveno određuje poligon do na translaciju. Kako je rub poligona zatvorena putanja, jasno je da važi: $\sum_{i=1}^{n} c_i e_i = (0,0)$.

<u>Teorema 10:</u> Neka je P poligon sa celobrojnim temenima čiji je poligonalni niz vektora $\{c_i e_i\}_{1 \le i \le n}$, pri čemu su $e_i \in \mathbb{Z}^2$ primitivni vektori. Tada je poligon sa celobrojnim temenima Q poligon sabirak poligona P ako i samo ako je poligonalni niz vektora poligona Q oblika $\{d_i e_i\}_{1 \le i \le n}$, pri čemu važi $0 \le d_i \le c_i$ i $\sum_{i=1}^{n} d_i e_i = (0,0)$.

Dokaz:
(⇒) Neka je $\{e_i'\}_{1 \le i \le n}$ niz ivičnih vektora poligona Q. Iz ***Napomene 11*** zaključujemo da se svaka ivica poligona Q pojavljuje kao ivica - sabirak neke ivice ce poligona P, gde je e primitivni vektor. Jasno je da toj ivici poligona Q odgovara ivični vektor oblika de, pri čemu važi $0 \le d \le c$. Kako je omotač poligona, sa aspekta ivičnih vektora, zatvorena putanja, zaključujemo da važi:

$$\sum_{i=1}^{n} d_i e_i = (0,0).$$

(⇐) Proizvoljan niz vektora $\{d_i e_i\}_{1\le i\le n}$ za koji važi $0 \le d_i \le c_i$ i $\sum_{i=1}^{n} d_i e_i = (0,0)$ definiše zatvorenu putanju. Kako je $\{c_i e_i\}_{1\le i\le n}$ poligonalni niz vektora poligona *P*, $\{d_i e_i\}_{1\le i\le n}$ definiše omotač konveksnog poligona koji je poligon sabirak poligona *P* i koji daje poligon *P* u zbiru sa poligonom čiji je ivični niz $\{(c_i - d_i)e_i\}_{1\le i\le n}$. □

Napomena 13: Za svaki poligon sa celobrojnim temenima koji ima dve paralelne ivice možemo reći da tim ivicama odgovaraju primitivni vektori e_i i e_j za koje važi: $e_i = -e_j$, odnosno $e_i + e_j = 0$. Odavde iz ***Teoreme 10*** direktno sledi da je ovaj poligon integralno rastavljiv u smislu sume Minkovskog. Zbog toga će, za sve poligone koji će biti razmatrani u ovom poglavlju, standardna pretpostavka biti da su im sva temena celobrojna i da nemaju paralelnih ivica.
Takođe, poligon sabirak poligona sa celobrojnim temenima se naziva ***trivijalnim poligonom sabirkom*** ako je duž ili celobrojna tačka.
Iz ***Teoreme 10*** je očigledno da bilo koji n-tougao sa celobrojnim temenima, $n \ge 3$, koji nema paralelnih ivica može jedino imati celobrojne poligone sabirke sa sa i ivica, pri čemu $i \in \{3,4,...,n-1,n\}$. Na primer, petougao sa celobrojnim temenima koji nema paralelnih ivica može imati samo trougaone, četvorougaone ili petougaone poligone sabirke sa celobrojnim temenima.

U ovom poglavlju bavićemo se pronalaženjem kriterijuma nerastavljivosti za poligone sa celobrojnim temenima u dvodimenzionalnoj Euklidskoj ravni $\mathbb{R}^2$ i predstavićemo važne rezultate u vezi sa nerastavljivošću četvorouglova i petouglova sa celobrojnim temenima. Iz razloga kompletnosti, analizu počinjemo dužima.

5.1. DUŽI

Definicija 13: Za bilo koje dve tačke a_1 i a_2 iz $\mathbb{R}^2$ ***duž*** $[a_1, a_2]$ koja spaja tačke a_1 i a_2 je skup svih tačaka oblika:

$$a = a_1 + \lambda(a_2 - a_1),\ 0 \le \lambda \le 1.$$

Napomena 14: Neka su v_1, v_2, a_1, a_2, b_1, b_2 tačke iz $\mathbb{R}^2$ za koje važi: $v_1 = a_1 + b_1$ i $v_2 = a_2 + b_2$. Tada je: $[v_1, v_2] \subseteq [a_1, a_2] + [b_1, b_2]$.
Ako važi: $[v_1, v_2] = [a_1, a_2] + [b_1, b_2]$, onda su duži $[v_1, v_2]$, $[a_1, a_2]$ i $[b_1, b_2]$ paralelne jer:

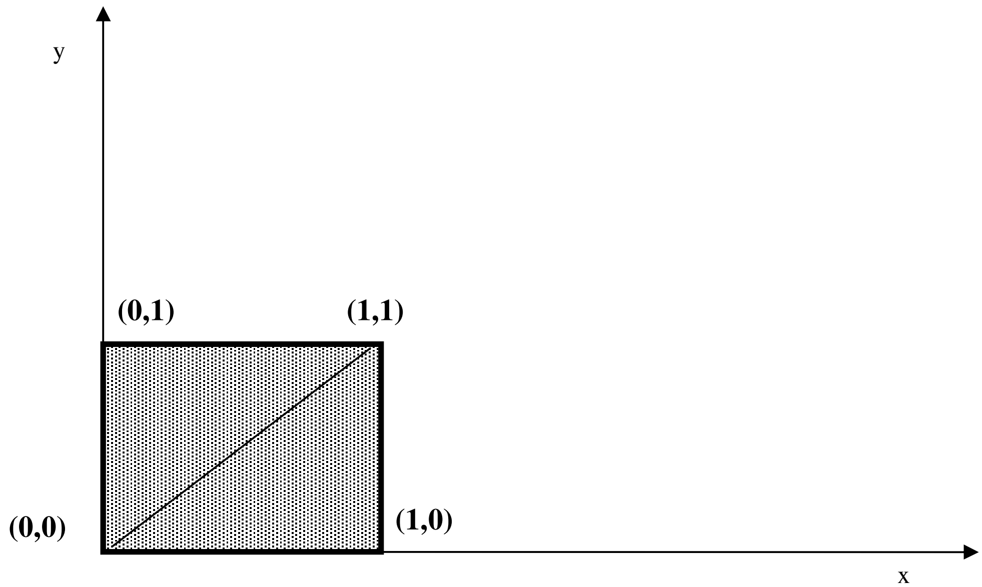
$$[v_1, v_2] = \bigcup_{b\in[b_1,b_2]} \left([a_1, a_2] + b\right) = \bigcup_{a\in[a_1,a_2]} \left(a + [b_1, b_2]\right)$$

Zaista, na slici 16 vidimo: (0,0)= (0,0) + (0,0) i (1,1)= (0,1) + (1,0), pa važi i:

$$conv\left((0,0),(1,1)\right) \subseteq conv\left((0,0),(0,1)\right) + conv\left((0,0),(1,0)\right) = conv\left((0,0),(0,1),(1,1),(1,0)\right),$$

jer je duž $conv\left((0,0),(1,1)\right)$ dijagonala kvadrata $conv\left((0,0),(0,1),(1,1),(1,0)\right)$. Međutim, kako duži $conv\left((0,0),(1,1)\right)$, $conv\left((0,0),(0,1)\right)$, $conv\left((0,0),(1,0)\right)$ nisu paralelne, ne važi:

$$conv\big((0,0),(1,1)\big) = conv\big((0,0),(0,1)\big) + conv\big((0,0),(1,0)\big).$$



Slika 16

Na slici 3, vidimo da je: $(2,0)+(1,1)=(3,1)$ i $(1,1)+(0,2)=(1,3)$. Očigledno je da su duži $conv\big((2,0),(1,1)\big)$, $conv\big((1,1),(0,2)\big)$, $conv\big((3,1),(1,3)\big)$ paralelne, pa važi:

$$conv\big((3,1),(1,3)\big) = conv\big((2,0),(1,1)\big) + conv\big((1,1),(0,2)\big).$$

Sledeća teorema nam daje mogućnost da odredimo broj tačaka sa celobrojnim koordinatama na proizvoljnoj duži. U daljem tekstu, sa $NZD(a)$ ćemo obeležavati $NZD(a_x, a_y)$, gde je $a = (a_x, a_y)$ proizvoljna tačka iz $\mathbb{R}^2$ sa celobrojnim koordinatama. Slično, $NZD(a,b)$ će označavati $NZD\big(NZD(a), NZD(b)\big)$, gde su a,b proizvoljne tačke iz $\mathbb{R}^2$ sa celobrojnim koordinatama.

<u>Teorema 11:</u> Neka su a_1 i a_2 dve različite tačke sa celobrojnim koordinatama iz $\mathbb{R}^2$. Tada na duži $[a_1, a_2]$ ima tačno $NZD(a_2 - a_1) + 1$ tačka sa celobrojnim koordinatama, računajući a_1 i a_2. Štaviše, ako je a_3 proizvoljna tačka sa celobrojnim koordinatama na otvorenoj duži (a_1, a_2), tj. $a_3 = \alpha a_1 + \beta a_2$, za neke $\alpha > 0$ i $\beta > 0$ takve da je $\alpha + \beta = 1$, tada važi:

$$\frac{NZD(a_3 - a_1)}{NZD(a_3 - a_2)} = \frac{\|a_3 - a_1\|}{\|a_3 - a_2\|} = \frac{\beta}{\alpha}.$$

Dokaz:
Neka je a_3 tačka na otvorenoj duži (a_1, a_2). Tada važi $a_3 = \alpha a_1 + \beta a_2$, za neke $\alpha > 0$ i $\beta > 0$ takve da je $\alpha + \beta = 1$.
Očigledno je da važi:

$$a_3 - a_1 = \alpha a_1 + \beta a_2 - a_1 = (1-\beta) a_1 + \beta a_2 - a_1 = \beta(a_2 - a_1),$$

kao i:

$$a_3 - a_2 = \alpha a_1 + \beta a_2 - a_2 = \alpha a_1 + (1-\alpha) a_2 - a_2 = \alpha (a_1 - a_2).$$

Odavde direktno sledi:

$$\frac{\|a_3-a_1\|}{\|a_3-a_2\|} = \frac{\|\beta(a_2-a_1)\|}{\|\alpha(a_1-a_2)\|} = \frac{\beta\|a_2-a_1\|}{\alpha\|a_1-a_2\|} = \frac{\beta}{\alpha}.$$

Jasno je da prethodna jednakost važi za bilo koju tačku na otvorenoj duži (a_1, a_2), bez obzira da su njene koordinate celobrojne.

Iz jednakosti $a_3 - a_1 = \beta(a_2 - a_1)$ očigledno je da je a_3 tačka sa celobrojnim koordinatama ako i samo ako je $\beta(a_2 - a_1)$ tačka sa celobrojnim koordinatama. Neka je a_3 tačka sa celobrojnim koordinatama. Kako je $a_2 - a_1$ tačka sa celobrojnim koordinatama i $a_3 \neq a_1$, zaključujemo da je β racionalan broj oblika:

$$\beta = \tfrac{m}{n}, \text{ za neke } 0<m<n, \text{ takve da je } NZD(m,n)=1.$$

Jasno je da je $\beta(a_2 - a_1)$ tačka sa celobrojnim koordinatama ako i samo ako n deli $d = NZD(a_2 - a_1)$. Dakle, da bi a_3 bila tačka sa celobrojnim koordinatama, potrebno je da važi:

$$\beta = \tfrac{g}{d}, \text{ gde je } g = \tfrac{md}{n}, \text{ pa važi: } 0<g<d.$$

Odavde sledi da g biramo na $d-1$ način, pa zaključujemo da na zatvorenoj duži $[a_1, a_2]$ ima $(d-1)+2 = d+1$ tačka sa celobrojnim koordinatama.

Dalje dobijamo:

$$a_3 - a_1 = \beta(a_2 - a_1) = \tfrac{g}{d} dv',$$

za neki primitivni vektor v'.

Slično dobijamo:

$$a_3 - a_2 = \alpha(a_1 - a_2) = (1-\beta)(a_1 - a_2) = \left(1-\tfrac{g}{d}\right)(a_1 - a_2) = \tfrac{d-g}{d}(a_1 - a_2) = \tfrac{d-g}{d}(-dv''),$$

za neki primitivni vektor v''.

Kako su v' i v'' primitivni vektori, sledi da je:

$$NZD(a_3 - a_1) = g \text{ i } NZD(a_3 - a_2) = d - g.$$

Odavde dobijamo:

$$\frac{NZD(a_3-a_1)}{NZD(a_3-a_2)} = \frac{g}{d-g} = \frac{\frac{g}{d}}{\frac{d-g}{d}} = \frac{\frac{g}{d}}{1-\frac{g}{d}} = \frac{\beta}{1-\beta} = \frac{\beta}{\alpha},$$

čime je dokaz završen. □

<u>Teorema 12:</u> Neka su a_1 i a_2 dve različite tačke sa celobrojnim koordinatama iz $\mathbb{R}^2$. Duž $[a_1, a_2]$ je integralno nerastavljiva u smislu sume Minkovskog ako i samo ako je $NZD(a_2 - a_1) = 1$.

Dokaz:

(⇒) Neka je duž $[a_1, a_2]$ integralno nerastavljiva u smislu sume Minkovskog. Pokažimo da je tada $NZD(a_2 - a_1) = 1$. Pretpostavimo suprotno: $NZD(a_2 - a_1) = d>1$.

Tada na duži $[a_1,a_2]$ ima tačno $d+1$ tačka sa celobrojnim koordinatama, računajući a_1 i a_2. Kako je $d>1$, zaključujemo da je $d+1>2$, odnosno $d+1\geq 3$. Dakle, na duži $[a_1,a_2]$ ima bar 3 tačke sa celobrojnim koordinatama, računajući a_1 i a_2. Odavde je jasno da se na otvorenoj duži (a_1,a_2) nalazi bar jedna tačka c sa celobrojnim koordinatama. Tada za nju važi:

$$[a_1,a_2]=[a_1,c]+[0,a_2-c],$$

odnosno duž $[a_1,a_2]$ je integralno rastavljiva u smislu sume Minkovskog, što je kontradikcija. Dakle, važi $NZD(a_2-a_1)=1$.

(⇐) Neka je $NZD(a_2-a_1)=1$. Pokažimo da je duž $[a_1,a_2]$ integralno nerastavljiva u smislu sume Minkovskog. Pretpostavimo suprotno: $[a_1,a_2]=[b_1,b_2]+[c_1,c_2]$, za neke duži $[b_1,b_2]$, $[c_1,c_2]$ sa celobrojnim koordinatama za koje važi $\|(b_1,b_2)\|$, $\|(c_1,c_2)\|>0$. Na osnovu ***Napomene 14*** zaključujemo da su duži $[a_1,a_2]$, $[b_1,b_2]$ i $[c_1,c_2]$ paralelne. Ovo je očigledna kontradikcija s obzirom da je duž $[a_1,a_2]$ primitivna. Dakle, duž $[a_1,a_2]$ je integralno nerastavljiva. □

Primer 7: Polinom $f(x,y)=x^n+y^m$ je apsolutno nesvodljiv nad proizvoljnim poljem ako i samo ako je $NZD(n,m)=1$.

5.2. TROUGLOVI

Neka je $conv(v_1,v_2,v_3)$ trougao sa celobrojnim koordinatama u Dekartovoj pravougaonoj ravni $\mathbb{R}^2$. Pokazaćemo da je taj trougao rastavljiv u smislu sume Minkovskog ako i samo ako važi:

$$NZD(v_1-v_2,v_1-v_3)=d>1.$$

Prethodni uslov je ekvivalentan uslovu:

$$NZD(v_1-v_2,v_1-v_3)=NZD(v_2-v_1,v_2-v_3)=NZD(v_3-v_1,v_3-v_2)=d.$$

Teorema 13: Trougao $conv(v_1,v_2,v_3)$ u $\mathbb{R}^2$ sa celobrojnim temenima v_1,v_2,v_3 je integralno nerastavljiv u smislu sume Minkovskog ako i samo ako je:

$$NZD(v_1-v_2,v_1-v_3)=1.$$

Dokaz:

(⇐) Neka je $T=conv(v_1,v_2,v_3)$ trougao sa celobrojnim temenima u $\mathbb{R}^2$. Formirajmo ivične vektore trougla T na sledeći način:

$$E_1=v_2-v_1=c_1e_1,\ E_2=v_3-v_2=c_2e_2 \text{ i } E_3=v_1-v_3=c_3e_3,$$

pri čemu su:

$$c_1=NZD(v_2-v_1),\ c_2=NZD(v_3-v_2) \text{ i } c_3=NZD(v_1-v_3)$$

pozitivni, celi brojevi, a e_1, e_2 i e_3 su primitivni ivični vektori trougla T. Kako T nema paralelnih ivica, na osnovu ***Napomene 14*** zaključujemo da svaki konveksan poligon S sa celobrojnim temenima koji je poligon sabirak trougla T mora biti trougao i njegov ivični niz vektora je oblika:

$$E_1' = d_1 e_1,\ E_2' = d_2 e_2 \text{ i } E_3' = d_3 e_3,$$

gde su $0 \le d_i \le c_i$, za $i = 1,2,3$, pri čemu važi:

$$E_1' + E_2' + E_3' = 0.$$

Stoga, svaki poligon sabirak trougla T mora biti trougao koji je sličan trouglu T. Drugim rečima, važi:

$$\frac{\|E_1'\|}{\|E_1\|} = \frac{\|E_2'\|}{\|E_2\|} = \frac{\|E_3'\|}{\|E_3\|} = \frac{d_1}{c_1} = \frac{d_2}{c_2} = \frac{d_3}{c_3} = \frac{m}{n}.$$

gde je $\frac{m}{n}$ racionalan broj, $0 \le m \le n$ i $NZD(m,n) = 1$.

Kako su d_i, $i = 1,2,3$ celi brojevi, jasno je da n deli c_j, $j = 1,2,3$.

Pretpostavimo da je $NZD(v_1 - v_2, v_1 - v_3) = 1$. S obzirom da važi:

$$NZD(v_1 - v_2, v_1 - v_3) = NZD(NZD(v_1 - v_2), NZD(v_1 - v_3)) = NZD(c_1, c_3) = 1,$$

tj. c_1 i c_3 su uzajamno prosti. Kako n deli i c_1 i c_3, zaključujemo da je $n = 1$. Iz relacije $0 \le m \le n$ sledi da je $m = 0$ ili $m = 1$. Odavde dobijamo $S = \{0\}$ ili $S = T$. Dakle, trougao T nema netrivijalnu dekompoziciju, pa je integralno nerastavljiv u smislu sume Minkovskog.

(⇒) Neka je trougao T integralno nerastavljiv. Treba pokazati da je:

$$NZD(v_1 - v_2, v_1 - v_3) = 1.$$

Pretpostavimo suprotno, $NZD(v_1 - v_2, v_1 - v_3) = NZD(c_1, c_3) = d > 1$. Tada je $S = conv(0, v_2 - v_1, v_3 - v_1)$ trougao sa celobrojnim temenima i važi: $T = v_1 + d\left(\frac{1}{d}S\right)$. Dakle, dobijamo da je trougao T rastavljiv u smislu sume Minkovskog, što je kontradikcija. Dakle, važi $NZD(v_1 - v_2, v_1 - v_3) = 1$. □

<u>Napomena 15:</u> Na osnovu dokaza ***Teoreme 13*** vidimo da je trougao u $\mathbb{R}^2$ sa celobrojnim temenima v_1, v_2, v_3 integralno nerastavljiv u smislu sume Minkovskog ako važi:

$$NZD(v_i - v_j, v_i - v_k) = 1, \text{ za neke } i,j,k,\ \{i,j,k\} = \{1,2,3\}.$$

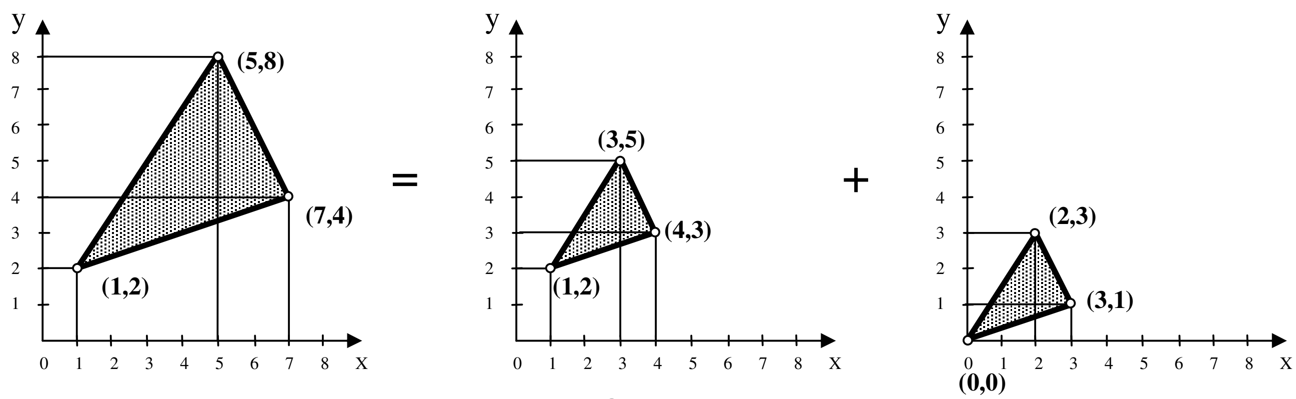
<u>Primer 8:</u> Posmatrajmo trougao $conv((1,2),(7,4),(5,8))$. Kako je:

$$NZD((7,4)-(1,2),(7,4)-(5,8)) = NZD((6,2),(2,-4)) = 2 > 1$$

zaključujemo da je trougao $conv((1,2),(7,4),(5,8))$ rastavljiv u smislu sume Minkovskog i njegova dekompozicija je:

$$conv((1,2),(7,4),(5,8)) = conv((1,2),(4,3),(3,5)) + conv((0,0),(3,1),(2,3)),$$

što je prikazano na slici 17.



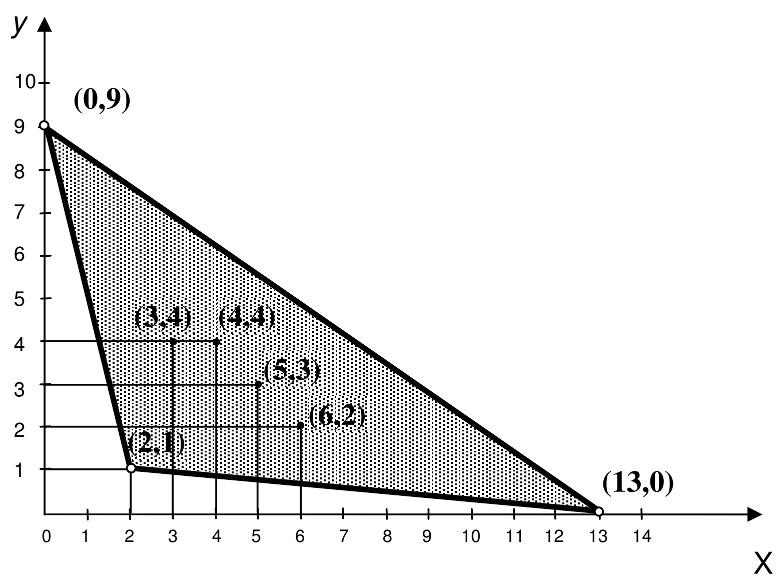
Slika 17

Primer 9: Posmatrajmo polinom:

$$f(x,y) = a_1x^{13} + a_2y^9 + a_3x^2y + a_4x^4y^4 + a_5x^5y^3 + a_6x^6y^2 + a_7x^3y^4,$$

pri čemu je $a_1,...,a_7 \in \mathbb{F}\backslash\{0\}$, gde je $\mathbb{F}$ proizvoljno polje.

Termima polinoma $f(x,y)$ sa nenula koeficijentima odgovaraju redom sledeći vektori eksponenata: (13,0), (0,9), (2,1), (4,4), (5,3), (6,2) i (3,4). Njutnov poligon polinoma $f(x,y)$ je trougao $P_f = conv((13,0),(0,9),(2,1))$ prikazan na slici 18.



Slika 18

Kako je:

$$NZD((13,0)-(0,9),(13,0)-(2,1)) = NZD((13,-9),(11,-1)) = NZD(NZD(13,-9),NZD(11,-1)) = NZD(1,1) = 1,$$

zaključujemo da je trougao $P_f = conv((13,0),(0,9),(2,1))$ integralno nerastavljiv u smislu sume Minkovskog, pa je polinom $f(x,y)$ apsolutno nesvodljiv nad poljem $\mathbb{F}$.

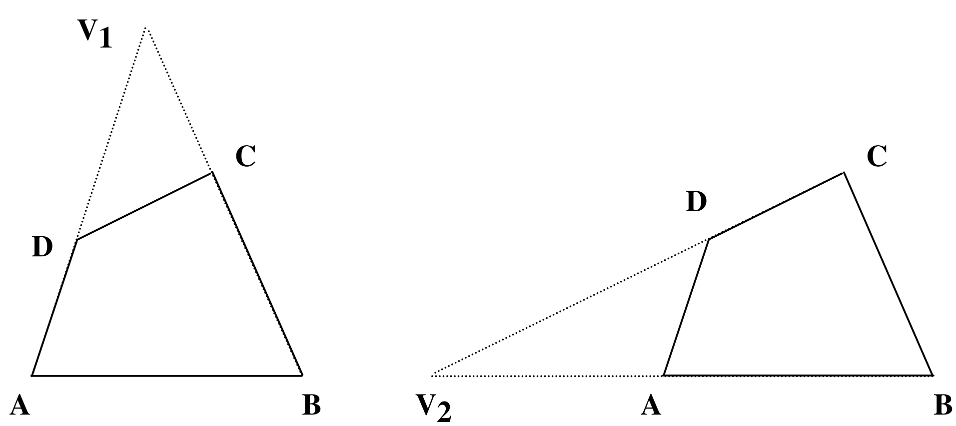
Polinom $f(x,y)$ "ostaje" apsolutno nesvodljiv nad poljem $\mathbb{F}$ ako mu dodamo nove terme čiji vektori eksponenata leže u Njutnovom poligonu polinoma $f(x,y)$.
S obzirom da njihovi vektori eksponenata leže u P_f, možemo dodati terme x^8y^2, x^7y^3 itd sa proizvoljnim koeficijentima.
Drugim rečima, svaki polinom oblika:

$$f(x,y)=a_1x^{13}+a_2y^9+a_3x^2y+a_4x^4y^4+a_5x^5y^3+a_6x^6y^2+a_7x^3y^4+\sum c_{ij}x^iy^j,$$

gde $a_1,\ldots,a_7\in\mathbb{F}\backslash\{0\}$ i $(i,j)\in P_f$,
je apsolutno nesvodljiv nad $\mathbb{F}$.

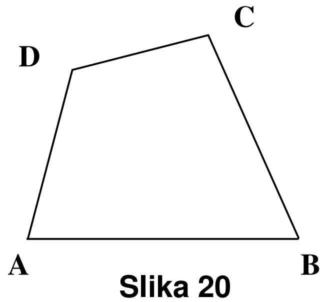
5.3. ČETVOROUGLOVI

Na osnovu ***Napomene 13*** zaključujemo da je četvorougao sa celobrojnim temenima u $\mathbb{R}^2$ koji ima dve paralelne ivice integralno rastavljiv. Najpre primetimo da proizvoljan četvorougao $Q=conv(A,B,C,D)$ sa celobrojnim temenima koji nema paralelnih ivica leži u unutrašnjosti tačno dva trougla $T_1=conv(A,B,v_1)$ i $T_2=conv(B,C,v_2)$ za neke tačke $v_1,v_2\in\mathbb{R}^2$, pri čemu svaki od tih trouglova ima tačno jednu zajedničku ivicu sa Q, što je prikazano na slici 19. Za četvorougao Q koji leži u unutrašnjosti trougla, njihovu zajedničku ivicu nazivamo ***osnovna ivica***. Jasno je da četvorougao Q ima tačno dve osnovne ivice koje odgovaraju trouglovima T_1 i T_2. Očigledno je da su osnovne ivice četvorougla Q susedne. Osnovne ivice četvorougla Q prikazanog na slici 19 su $[AB]$ i $[BC]$.



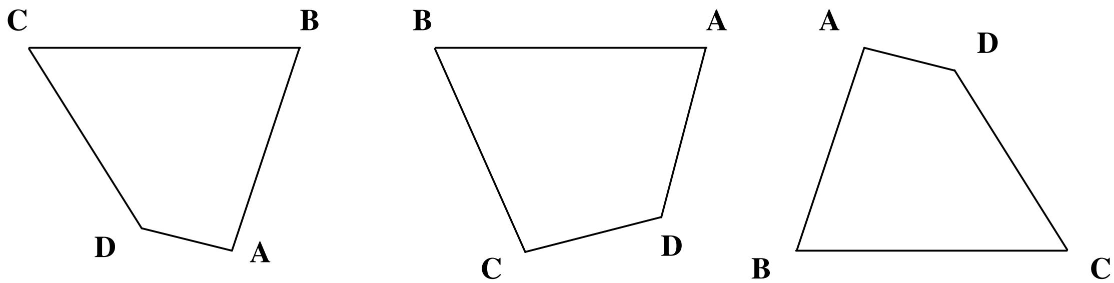
Slika 19

Bez umanjenja opštosti, u daljim razmatranjima možemo pretpostaviti da je četvorougao $ABCD$ sa celobrojnim temenima u $\mathbb{R}^2$ koji nema paralelnih ivica oblika prikazanog na slici 20.



Slika 20

Naime, ako je četvorougao $ABCD$ u nekom od položaja prikazanih na slici 21, analiza je analogna kao u slučaju četvorougla prikazanog na slici 20 koju ćemo izložiti.



Slika 21

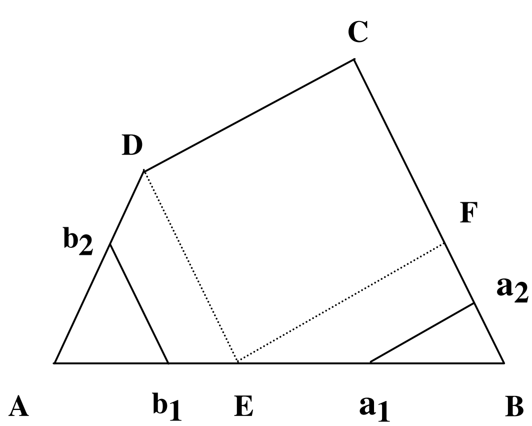
Formirajmo, najpre, paralelograme $CDEF$ i $AGHD$ na način prikazan na slikama 22 i 23. Primetimo da tačke E, F, G i H nisu obavezno celobrojne.

Na osnovu ***Teoreme 10*** zaključujemo da je proizvoljan poligon sabirak četvorougla $ABCD$ trougao ili četvorougao.

Očigledno je da četvorougao $ABCD$ ima netrivijalne trougaone ili četvorougaone poligone sabirke sa celobrojnim temenima ako važi neki od uslova ***(1)***,...,***(5)***.

(1) Postoje tačke a_1 i a_2 sa celobrojnim koordinatama, $a_1 \in (B,E]$, $a_2 \in (B,F]$ takve da je duž $[a_1,a_2]$ paralelna duži $[D,C]$ (slika 22).

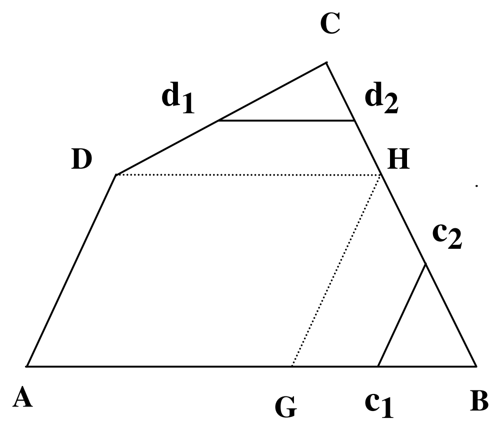
(2) Postoje tačke b_1 i b_2 sa celobrojnim koordinatama, $b_1 \in (A,E]$, $b_2 \in (A,D]$ takve da je duž $[b_1,b_2]$ paralelna duži $[B,C]$ (slika 22).



Slika 22

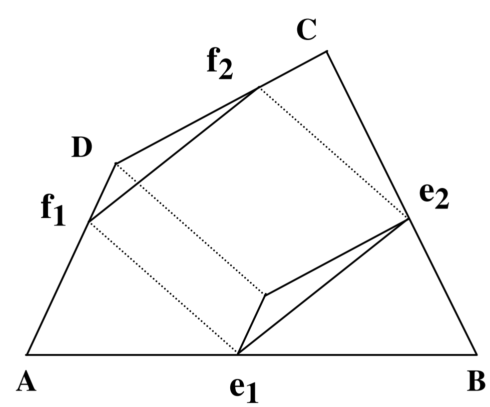
(3) Postoje tačke c_1 i c_2 sa celobrojnim koordinatama, $c_1 \in (B,G]$, $c_2 \in (B,H]$ takve da je duž $[c_1,c_2]$ paralelna duži $[A,D]$ (slika 23).

(4) Postoje tačke d_1 i d_2 sa celobrojnim koordinatama, $d_1 \in (C,D]$, $d_2 \in (C,H]$ takve da je duž $[d_1,d_2]$ paralelna duži $[A,B]$ (slika 23).



Slika 23

(5) Postoje tačke e_1, e_2, f_1 i f_2 sa celobrojnim koordinatama, $e_1 \in (A,B)$, $e_2 \in (B,C)$, $f_1 \in (D,A)$, $f_2 \in (C,D)$ takve da je duž $[e_1,e_2]$ paralelna duži $[f_1,f_2]$ i važi $\|e_1,e_2\| = \|f_1,f_2\|$ (slika 24).



Slika 24

<u>Napomena 16:</u> Uslovi *(1)*, *(2)*, *(3)* i *(4)* netrivijalne trougaone, a uslov *(5)* netrivijalne četvorougaone poligone sabirke sa celobrojnim temenima. Primetimo da je ***(1)⇔(4)*** i ***(2)⇔(3)***.

Formulišimo, sada, teoremu za četvorouglove.

Teorema 14: Četvorougao $Q = conv(A,B,C,D)$ prikazan na slici 20 je integralno nerastavljiv u smislu sume Minkovskog ako i samo ako uslovi ***(1)***, ***(2)*** i ***(5)*** ne važe.

Dokaz:
(⇐) Neka su $E_1 = B - A$, $E_2 = C - B$, $E_3 = D - C$ i $E_4 = A - D$ ivični vektori četvorougla Q.
Neka je ***(1)***, ***(2)*** i ***(5)*** ne važe. Treba pokazati da je četvorougao Q integralno nerastavljiv. Pretpostavimo suprotno, da se četvorougao Q može rastaviti u smislu sume Minkovskog. Pretpostavimo, najpre, da je netrivijalni poligon sabirak četvorougla Q trougao sa celobrojnim temenima. Na osnovu ***Teoreme 10*** jasno je da svaka ivica netrivijalnog poligona sabirka mora biti poligon sabirak tačno jedne ivice četvorougla Q. Dakle, očigledno je da ivični vektori trougaonog poligona sabirka mogu biti iz jednog od skupova:

a) $\{E_1, E_2, E_3\}$

b) $\{E_1, E_2, E_4\}$

c) $\{E_2, E_3, E_4\}$

d) $\{E_3, E_4, E_1\}$

Jasno, ivični vektori trougaonog poligona sabirka četvorougla Q su redom istog pravca i smera kao vektori u jednom od skupova ***a)***, ***b)***, ***c)***, ***d)***, ali ne moraju biti istog intenziteta.
Ako ivični vektori trougaonog poligona sabirka Q odgovaraju vektorima iz stavke ***a)*** ili ***b)***, onda su uslovi iz stavke ***(1)*** ili ***(2)*** ispunjeni, što je očigledna kontradikcija. Dakle, Q integralno nerastavljiv. Sa slike 20 je jasno da ***c)*** i ***d)*** ne mogu dati trougaone poligone sabirke zato što odgovarajući vektori ne mogu formirati zatvorenu putanju.
Pretpostavimo, zatim, da je netrivijalni poligon sabirak S četvorougla Q četvorougao sa celobrojnim temenima takav da važi $Q = S + T$, gde je T netrivijalni poligon sabirak četvorougla Q. Tada je uslov ***(5)*** ispunjen. Naime, sve ivice poligona sabirka S moraju biti sabirci ivica poligona Q. Neka su F_1, F_2, F_3 i F_4 ivični vektori četvorougla S koji su redom netrivijalni sabirci ivica E_1, E_2, E_3 i E_4. Neka su $e_1 = B - F_1$, $e_2 = B + F_2$, $f_1 = D + F_4$ i $f_2 = D - F_3$ celobrojne tačke na ivicama četvorougla Q.
Tada važi:

$$\overrightarrow{e_1 e_2} = \overrightarrow{e_1 B} + \overrightarrow{B e_2} = \big(B - (B - F_1)\big) + \big((B + F_2) - B\big) = F_1 + F_2$$

i

$$\overrightarrow{f_1 f_2} = \overrightarrow{f_1 D} + \overrightarrow{D f_2} = \big(D - (D + F_4)\big) + \big((D - F_3) - D\big) = -(F_3 + F_4).$$

S obzirom da ivični vektori četvorougla S formiraju zatvorenu putanju, važi:

$$F_1 + F_2 + F_3 + F_4 = 0.$$

odnosno:

$$F_1 + F_2 = -(F_3 + F_4).$$

Odavde je jasno da važi:

$$\overrightarrow{e_1 e_2} = \overrightarrow{f_1 f_2}.$$

Drugim rečima:

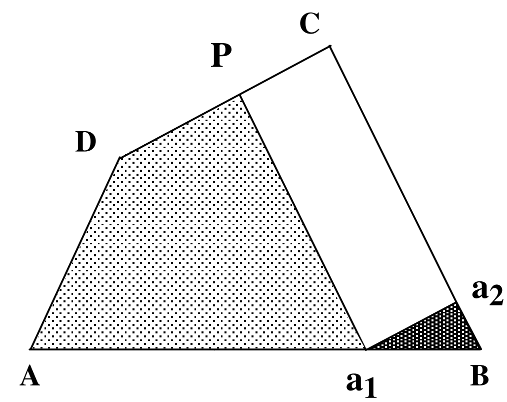
$$[e_1 e_2] \text{ je paralelno sa } [f_1 f_2] \text{ i } \|e_1 e_2\| = \|f_1 f_2\|,$$

odnosno uslov ***(5)*** je ispunjen, što je kontradikcija sa pretpostavkom.
Dakle, četvorougao Q je integralno nerastavljiv.

(⇒) Pretpostavimo da je četvorougao Q integralno nerastavljiv. Treba pokazati da uslovi ***(1)***, ***(2)*** i ***(5)*** ne važe. Pretpostavimo suprotno, neki od uslova ***(1)***, ***(2)*** ili ***(5)*** važi.
Pretpostavimo, najpre, da važi uslov ***(1)***. Dakle, postoje tačke a_1 i a_2 sa celobrojnim koordinatama, $a_1 \in (B,E]$, $a_2 \in (B,F]$ takve da je duž $[a_1,a_2]$ paralelna duži $[D,C]$. Tada se četvorougao Q može rastaviti u smislu sume Minkovskog na sledeći način:

$$Q = conv(A,B,C,D) = conv(A,a_1,P,D) + conv(a_1,B,a_2),$$

što je prikazano na slici 25.

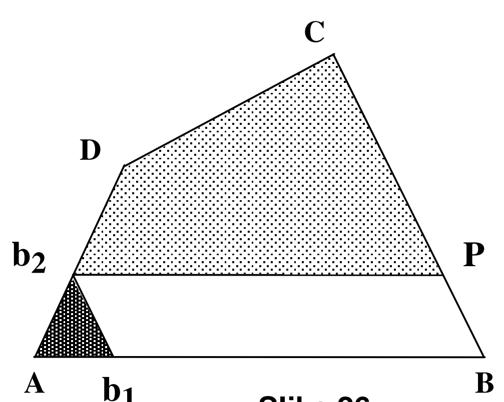


Slika 25

Na slikama 25-27 ćemo ilustrovati rastavljanje četvorougla u smislu sume Minkovskog gde je tačka dodira poligona sabiraka koordinatni početak. Ovo možemo učiniti bez gubitka opštosti na osnovu ***Teoreme 5***.
Pretpostavimo, zatim, da važi uslov ***(2)***. Dakle, postoje tačke b_1 i b_2 sa celobrojnim koordinatama, $b_1 \in (A,E]$, $b_2 \in (A,D]$ takve da je duž $[b_1,b_2]$ paralelna duži $[B,C]$. Tada se četvorougao Q može rastaviti u smislu sume Minkovskog na sledeći način:

$$Q = conv(A,B,C,D) = conv(A,b_1,b_2) + conv(b_2,P,C,D),$$

što je prikazano na slici 26.

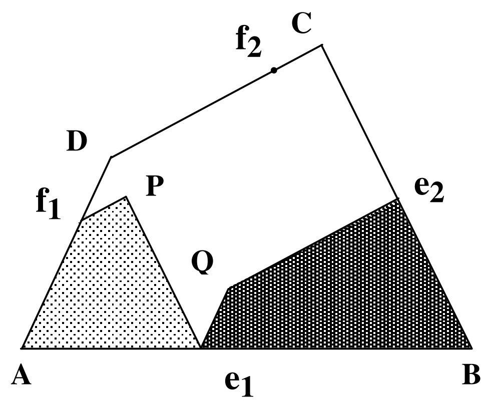


Slika 26

Konačno, pretpostavimo da važi uslov *(5)*, odnosno da postoje tačke e_1, e_2, f_1 i f_2 sa celobrojnim koordinatama, $e_1 \in (A,B)$, $e_2 \in (B,C)$, $f_1 \in (D,A)$, $f_2 \in (C,D)$ takve da je duž $[e_1,e_2]$ paralelna duži $[f_1,f_2]$ i važi $\|e_1,e_2\| = \|f_1,f_2\|$. Tada se četvorougao Q može rastaviti u smislu sume Minkovskog na sledeći način:

$$Q = conv(A,B,C,D) = conv(A,e_1,P,f_1) + conv(e_1,B,e_2,Q),$$

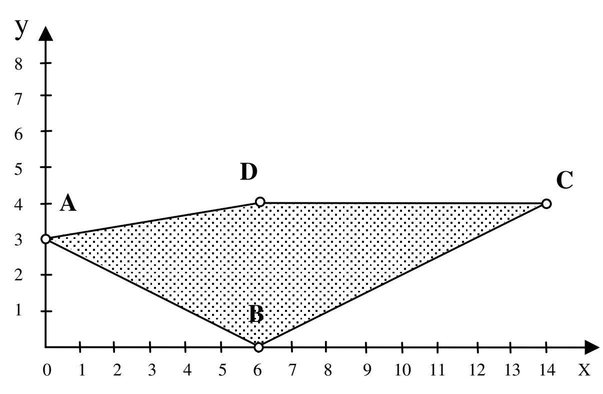
što je prikazano na slici 27.



Slika 27

Pretpostavka da važi neki od uslova *(1)*, *(2)* ili *(5)* implicira da se četvorougao Q može rastaviti u smislu sume Minkovskog, što je kontradikcija. Dakle, zaključujemo da uslovi *(1)*, *(2)* i *(5)* ne važe. □

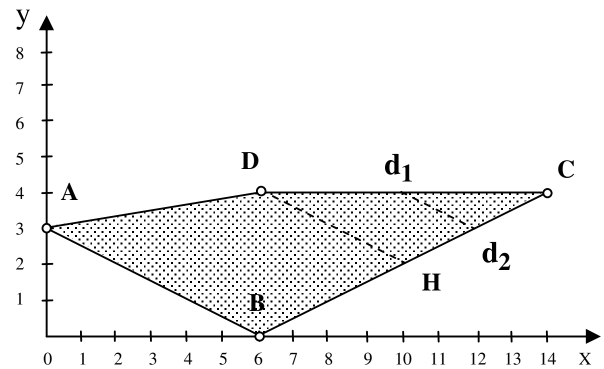
Primer 10: Posmatrajmo četvorougao $Q = conv(A,B,C,D)$, gde su $A = (0,3)$, $B = (6,0)$, $C = (14,4)$ i $D = (6,4)$ prikazan na slici 28.



Slika 28

Očigledno je da je tačka $H = (10,2)$ takva da je $[D,H]$ paralelno sa $[A,B]$. Postoje tačke

$d_1 = (10,4)$ i $d_2 = (12,3)$ sa celobrojnim koordinatama, $d_1 \in (C,D]$, $d_2 \in (C,H]$ takve da je duž $[d_1,d_2]$ paralelna duži $[A,B]$, što je prikazano na slici 29.



Slika 29

Dakle, ispunjene su pretpostavke uslova ***(4)***, pa je Q integralno rastavljiv.

Jasno, d_1 i d_2 možemo birati i na sledeći način:

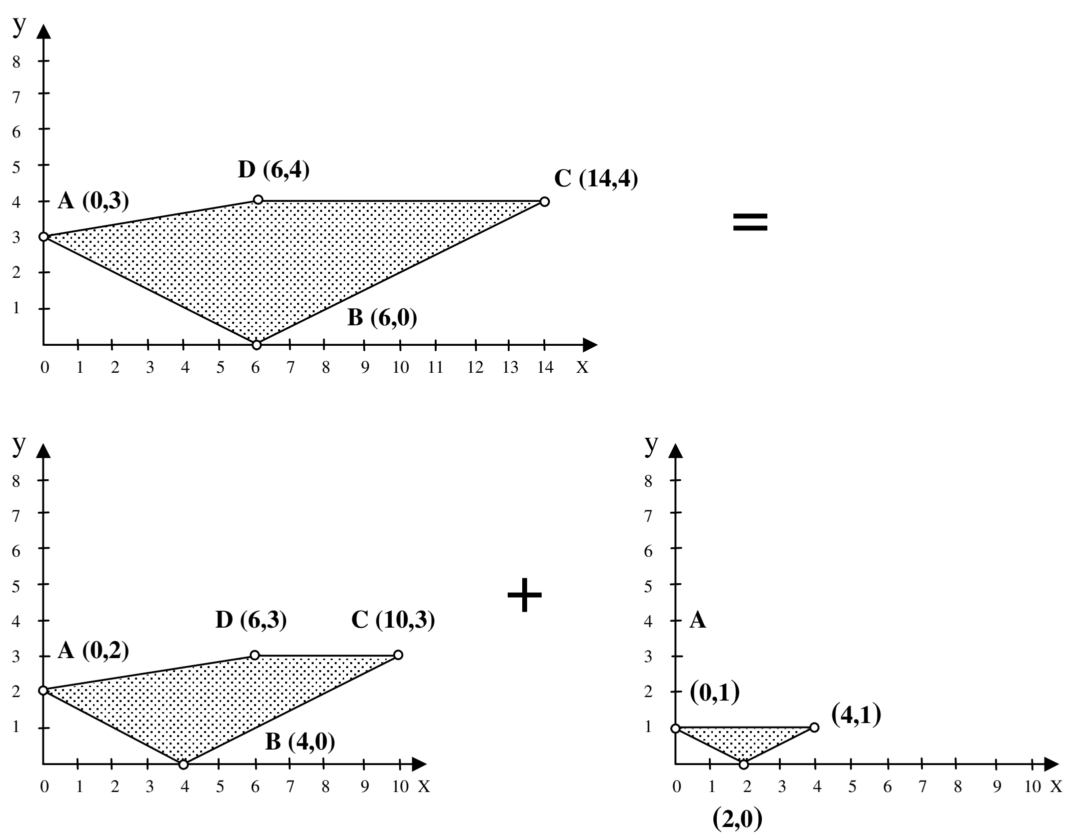
$$d_1 = D \in (C,D] \text{ i } d_2 = H \in (C,H].$$

Kako tačke d_1 i d_2 biramo na dva načina, četvorougao Q se može rastaviti u smislu sume Minkovskog na dva načina.

Dekompozicija četvorougla Q:

$$Q = conv((0,2),(4,0),(10,3),(6,3)) + conv((0,1),(2,0),(4,1)),$$

prikazana je na slici 30.

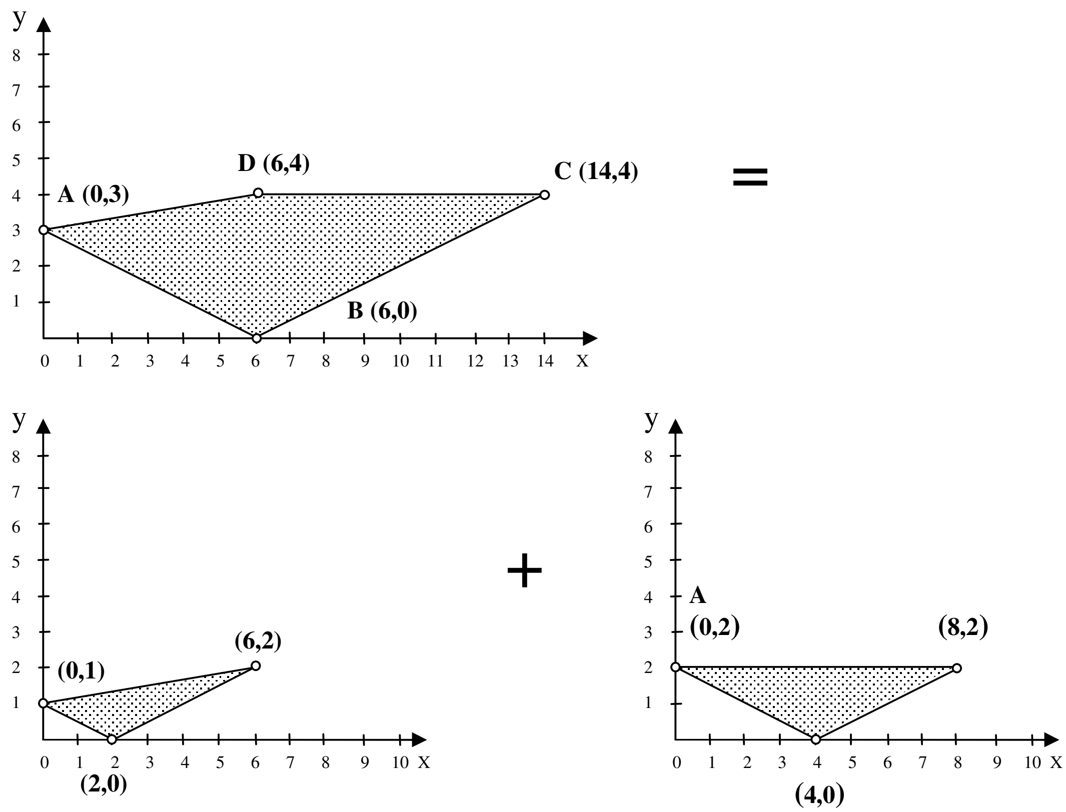


Slika 30

Druga dekompozicija četvorougla Q:

$$Q = conv\big((0,1),(2,0),(6,2)\big) + conv\big((0,2),(4,0),(8,2)\big),$$

je prikazana na slici 31.



Slika 31

Sledeća teorema je direktna posledica ***Teoreme 10***.

<u>Teorema 15:</u> Neka je m pozitivan ceo broj i $Q = conv(A,B,C,D)$ četvorougao sa celobrojnim temenima bez paralelnih ivica čiji je ivični niz vektora $\{me_1, me_2, e_3, e_4\}$. Četvorougao Q je integralno nerastavljiv u smislu sume Minkovskog ako i samo ako je $ie_1 + je_2 + e_3 \neq 0$, za sve celobrojne uređene parove (i, j), gde je $1 \leq i, j \leq m-1$ i $i \neq j$.

Dokaz:

(⇒) Neka je Q je integralno nerastavljiv. Treba pokazati da je $ie_1 + je_2 + e_3 \neq 0$, za sve celobrojne uređene parove (i, j), gde je $1 \leq i, j \leq m-1$ i $i \neq j$. Pretpostavimo suprotno, postoji uređen par celih brojeva (i, j), $1 \leq i, j \leq m-1$ i $i \neq j$ takav da važi $ie_1 + je_2 + e_3 = 0$. Na osnovu ***Teoreme 10*** dobijamo da je trougao sa ivičnim nizom vektora $\{ie_1, je_2, e_3\}$ poligon sabirak četvorougla Q, što je kontradikcija sa pretpostavkom da je Q je integralno nerastavljiv.

(⇐) Pokažimo, najpre, da proizvoljan celobrojni poligon sabirak četvorougla Q oblika $c_1e_1+c_2e_2+c_3e_3+c_4e_4=0$, $0\le c_1,c_2\le m$, $0\le c_3,c_4\le 1$ ne može sadržati obe ivice e_3 i e_4, odnosno da postoje samo dve mogućnosti:

$$(c_3,c_4)=(1,0) \text{ ili } (c_3,c_4)=(0,1).$$

Zaista, kada bi važilo $(c_3,c_4)=(1,1)$ poligon sabirak bi bio oblika:

$$(\mathbf{\mathit{1}})\quad c_1e_1+c_2e_2+e_3+e_4=0,\ 0\le c_1,c_2\le m-1.$$

Kako je $\{me_1,me_2,e_3,e_4\}$ ivični niz vektora četvorougla Q važi:

$$(\mathbf{\mathit{2}})\quad me_1+me_2+e_3+e_4=0.$$

Oduzimanjem jednakosti (***1***) od jednakosti (***2***) dobijamo:

$$(m-c_1)e_1+(m-c_2)e_2=0.$$

Dobijamo da su vektori e_1 i e_2 paralelni što je nemoguće jer četvorougao Q nema paralelnih ivica.

Na osnovu prethodne analize zaključujemo da za poligon sabirak četvorougla Q sa celobrojnim temenima postoje dve mogućnosti:

- **a)** $ie_1+je_2+e_3=0$, $1\le i,j\le m-1$, $i\ne j$
- **b)** $ie_1+je_2+e_4=0$, $1\le i,j\le m-1$, $i\ne j$.

Za i,j uzimamo $1\le i,j$ jer ako bi bilo, recimo, $1\le i$ i $j=0$ dobili bismo: $ie_1+e_3=0$, što bi značilo da Q ima dve paralelne stranice. Potpuno analogno razmatranje važi i za slučaj $1\le j$ i $i=0$. Ako bi bilo $i=j=0$, dobijamo $e_3=0$. Kako je $e_3=v_4-v_3$, to bi značilo da se temena v_3 i v_4 četvorougla Q poklapaju. Kako sve druge mogućnosti za donju granicu za i i j vode u kontradikciju, zaključujemo da je $1\le i,j$.

Obrazložimo, sada, izbor gornje granice za i i j. Kako je $i\ne j$, slučaj $i=j=m$ je nemoguć. Razmotrimo slučaj $i=m$, $j\le m-1$, tj. $me_1+je_2+e_3=0$. Oduzimanjem prethodne jednakosti od jednakosti (**2**) dobijamo $(m-j)e_2+e_4=0$, odnosno dobijamo da Q ima dve paralelne stranice. S obzirom da i slučaj $j=m$, $i\le m-1$ vodi u kontradikciju, mora važiti $i,j\le m-1$.

S obzirom da važi $me_1+me_2+e_3+e_4=0$, jasno je da svakom slučaju tipa **a**) odgovara tačno jedan slučaj tipa **b**). Dakle, analizirajući slučajeve tipa **a**) zapravo analiziramo sve moguće poligone sabirke četvorougla Q.

Takođe, pretpostavili smo da je $i\ne j$. Zaista, slučajeve $i=j$ možemo odbaciti jer kad bi važilo:

$$ie_1+ie_2+e_3=0,$$

dobijamo:

$$mie_1+mie_2+me_3=0,$$

a odavde:

$$mie_1+mie_2+me_3=i(me_1+me_2)+me_3=i(-e_3-e_4)+me_3=(m-i)e_3-ie_4=0.$$

Drugim rečima, dobijamo da su vektori e_3 i e_4 paralelni što je nemoguće jer četvorougao Q nema paralelnih ivica.

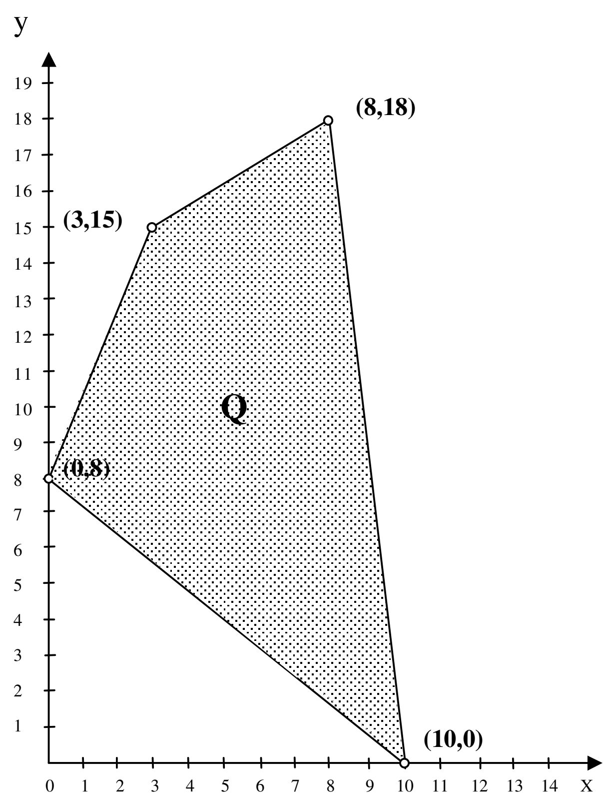
Dakle, pokazali smo da je svaki poligon sabirak četvorougla Q sa celobrojnim temenima oblika $ie_1 + je_2 + e_3 = 0$, $1 \le i, j \le m-1$, $i \ne j$, gde su i, j celi brojevi. S obzirom da je pretpostavka teoreme da za sve celobrojne uređene parove (i, j), gde je $1 \le i, j \le m-1$ i $i \ne j$ važi: $ie_1 + je_2 + e_3 \ne 0$, zaključujemo da se četvorougao Q ne može rastaviti u smislu sume Minkovskog, što je i trebalo pokazati. $\square$

U sledećim primerima ilustrovaćemo primenu ***Teoreme 15*** za nalaženje apsolutno nesvodljivih polinoma sa dve promenljive.

Primer 11: Posmatrajmo četvorougao Q sa celobrojnim temenima:

$$Q = conv\big((0,8),(10,0),(8,18),(3,15)\big),$$

prikazan je na slici 32.



Slika 32

Ivični niz vektora četvorougla Q je:

$$\{(10,0)-(0,8),(8,18)-(10,0),(3,15)-(8,18),(0,8)-(3,15)\}.$$

Odnosno:

$$\{(10,-8),(-2,18),(-5,-3),(-3,-7)\} = \{2(5,-4),2(-1,9),(-5,-3),(-3,-7)\}.$$

Sa slike 32 je očigledno da Q nema paralelnih ivica.

Na osnovu ***Teoreme 15***, četvorougao Q sa ivičnim nizom vektora $\{2e_1, 2e_2, e_3, e_4\}$, gde su $e_1 = (5,-4), e_2 = (-1,9), e_3 = (-5,-3), e_4 = (-3,-7)$ primitivni vektori, je nerastavljiv u smislu sume Minkovskog.
S obzirom da je četvorougao Q Njutnov poligon polinoma:

$$f(x,y) = a_1x^{10} + a_2y^8 + a_3x^8y^{18} + a_4x^3y^{15},\ a_1,...,a_4 \in \mathbb{F}\backslash\{0\},$$

zaključujemo da je polinom $f(x,y)$ apsolutno nesvodljiv nad $\mathbb{F}$, gde je $\mathbb{F}$ proizvoljno polje.
Polinom $f(x,y)$ "ostaje" apsolutno nesvodljiv nad poljem $\mathbb{F}$ ako mu dodamo nove terme čiji vektori eksponenata leže u Njutnovom poligonu polinoma $f(x,y)$ - četvorouglu Q.
Drugim rečima, svaki polinom oblika:

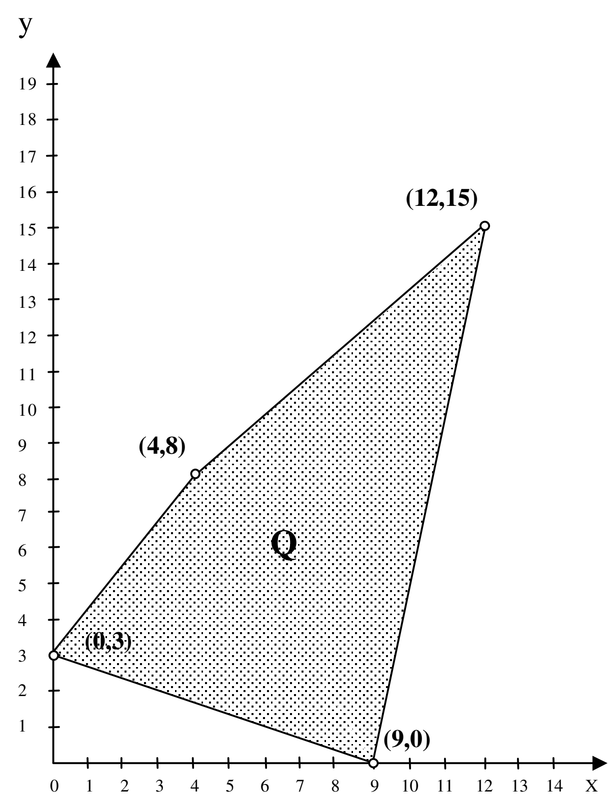
$$f(x,y) = a_1x^{10} + a_2y^8 + a_3x^8y^{18} + a_4x^3y^{15} + \sum c_{ij}x^iy^j,\ a_1,...,a_4 \in \mathbb{F}\backslash\{0\} \text{ i } (i,j) \in Q,$$

je apsolutno nesvodljiv nad $\mathbb{F}$.

Primer 12: Posmatrajmo četvorougao Q sa celobrojnim temenima:

$$Q = conv((0,3),(9,0),(12,15),(4,8)),$$

prikazan je na slici 33.



Slika 33

Ivični niz vektora četvorougla Q je:

$$\{(9,0)-(0,3),(12,15)-(9,0),(4,8)-(12,15),(0,3)-(4,8)\}.$$

Odnosno:

$$\{(9,-3),(3,15),(-8,-7),(-4,-5)\}=\{3(3,-1),3(1,5),(-8,-7),(-4,-5)\}.$$

Sa slike 33 je očigledno da Q nema paralelnih ivica.

Na osnovu ***Teoreme 15***, četvorougao Q sa ivičnim nizom vektora $\{3e_1,3e_2,e_3,e_4\}$, gde su $e_1=(3,-1),e_2=(1,5),e_3=(-8,-7),e_4=(-4,-5)$ primitivni vektori, je nerastavljiv u smislu sume Minkovskog ako i samo ako je:

$$e_1+2e_2+e_3\neq 0 \text{ i } 2e_1+e_2+e_3\neq 0.$$

S obzirom da je:

$$e_1+2e_2+e_3=(3,-1)+2(1,5)+(-8,-7)=(3,-1)+(2,10)+(-8,-7)=(-3,2)\neq(0,0)$$

i

$$2e_1+e_2+e_3=2(3,-1)+(1,5)+(-8,-7)=(6,-2)+(1,5)+(-8,-7)=(-1,-4)\neq(0,0),$$

dobijamo da je četvorougao Q nerastavljiv u smislu sume Minkovskog.

S obzirom da je četvorougao Q Njutnov poligon polinoma:

$$f(x,y)=a_1x^9+a_2y^3+a_3x^{12}y^{15}+a_4x^4y^8,\ a_1,...,a_4\in\mathbb{F}\backslash\{0\},$$

zaključujemo da je polinom $f(x,y)$ apsolutno nesvodljiv nad $\mathbb{F}$, gde je $\mathbb{F}$ proizvoljno polje.

Polinom $f(x,y)$ "ostaje" apsolutno nesvodljiv nad poljem $\mathbb{F}$ ako mu dodamo nove terme čiji vektori eksponenata leže u Njutnovom poligonu polinoma $f(x,y)$ - četvorouglu Q.

Drugim rečima, svaki polinom oblika:

$$f(x,y)=a_1x^9+a_2y^3+a_3x^{12}y^{15}+a_4x^4y^8+\sum c_{ij}x^iy^j,\ a_1,...,a_4\in\mathbb{F}\backslash\{0\} \text{ i } (i,j)\in Q,$$

je apsolutno nesvodljiv nad $\mathbb{F}$.

Primer 13: Posmatrajmo četvorougao Q sa celobrojnim temenima:

$$Q=conv((0,4),(8,0),(12,8),(3,9)),$$

prikazan je na slici 34.

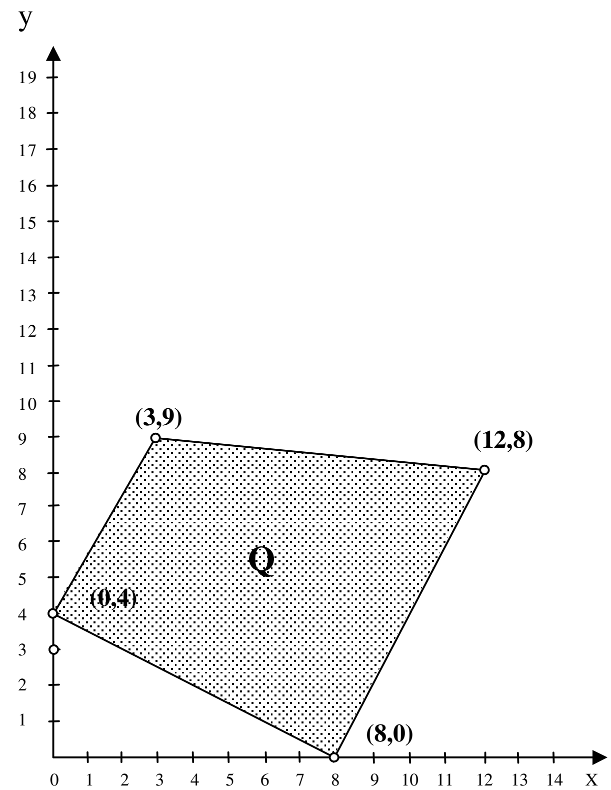
Ivični niz vektora četvorougla Q je:

$$\{(8,0)-(0,4),(12,8)-(8,0),(3,9)-(12,8),(0,4)-(3,9)\}.$$

Odnosno:

$$\{(8,-4),(4,8),(-9,1),(3,5)\}=\{4(2,-1),4(1,2),(-9,1),(-3,-5)\}.$$

Sa slike 34 je očigledno da Q nema paralelnih ivica.



Slika 34

Na osnovu ***Teoreme 15***, četvorougao Q sa ivičnim nizom vektora $\{4e_1, 4e_2, e_3, e_4\}$, gde su $e_1 = (2,-1), e_2 = (1,2), e_3 = (-9,1), e_4 = (-3,-5)$ primitivni vektori, je nerastavljiv u smislu sume Minkovskog ako i samo ako je:

$$e_1 + 2e_2 + e_3 \neq 0,\ 2e_1 + e_2 + e_3 \neq 0,\ e_1 + 3e_2 + e_3 \neq 0,\ 3e_1 + e_2 + e_3 \neq 0,\ 3e_1 + 2e_2 + e_3 \neq 0 \text{ i } 2e_1 + 3e_2 + e_3 \neq 0.$$

S obzirom da je:

$$e_1 + 2e_2 + e_3 = (2,-1) + 2(1,2) + (-9,1) = (2,-1) + (2,4) + (-9,1) = (-5,4) \neq (0,0),$$

$$2e_1 + e_2 + e_3 = 2(2,-1) + (1,2) + (-9,1) = (4,-2) + (1,2) + (-9,1) = (-4,1) \neq (0,0),$$

$$e_1 + 3e_2 + e_3 = (2,-1) + 3(1,2) + (-9,1) = (2,-1) + (3,6) + (-9,1) = (-4,6) \neq (0,0),$$

$$3e_1 + e_2 + e_3 = 3(2,-1) + (1,2) + (-9,1) = (6,-3) + (1,2) + (-9,1) = (-2,0) \neq (0,0),$$

$$3e_1 + 2e_2 + e_3 = 3(2,-1) + 2(1,2) + (-9,1) = (6,-3) + (2,4) + (-9,1) = (-1,2) \neq (0,0),$$

$$2e_1 + 3e_2 + e_3 = 2(2,-1) + 3(1,2) + (-9,1) = (4,-2) + (3,6) + (-9,1) = (-2,5) \neq (0,0),$$

dobijamo da je četvorougao Q nerastavljiv u smislu sume Minkovskog.

S obzirom da je četvorougao Q Njutnov poligon polinoma:

$$f(x,y) = a_1x^9 + a_2y^3 + a_3x^{12}y^{15} + a_4x^4y^8,\ a_1,\dots,a_4 \in \mathbb{F}\backslash\{0\},$$

zaključujemo da je polinom $f(x,y)$ apsolutno nesvodljiv nad $\mathbb{F}$, gde je $\mathbb{F}$ proizvoljno polje.

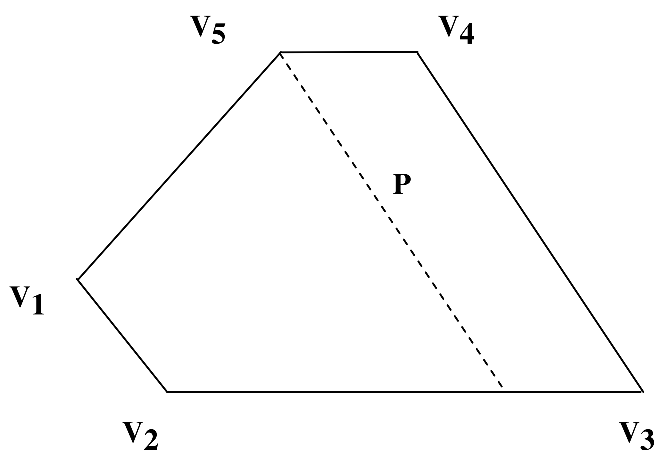
Polinom $f(x, y)$ "ostaje" apsolutno nesvodljiv nad poljem $\mathbb{F}$ ako mu dodamo nove terme čiji vektori eksponenata leže u Njutnovom poligonu polinoma $f(x, y)$ - četvorouglu Q. Drugim rečima, svaki polinom oblika:

$$f(x, y) = a_1x^9 + a_2y^3 + a_3x^{12}y^{15} + a_4x^4y^8 + \sum c_{ij}x^iy^j,\ a_1, ..., a_4 \in \mathbb{F}\backslash\{0\} \text{ i } (i, j) \in Q,$$

je apsolutno nesvodljiv nad $\mathbb{F}$.

5.4. PETOUGLOVI

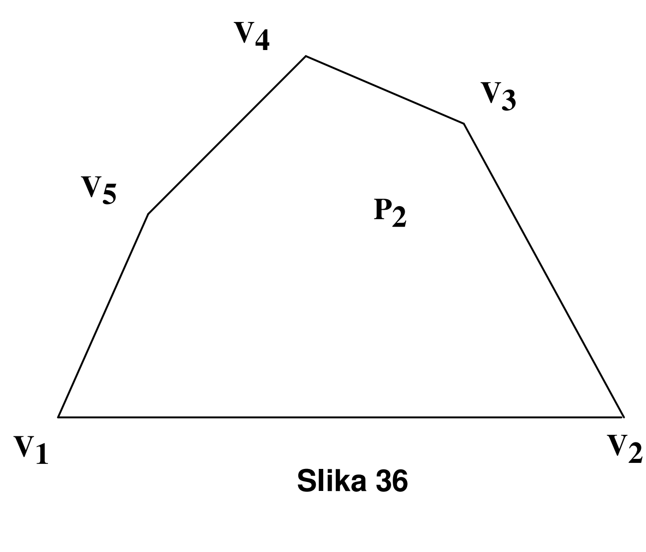
Neka je P_1 petougao sa celobrojnim temenima koji ima dve paralelne ivice, prikazan na slici 35.



Slika 35

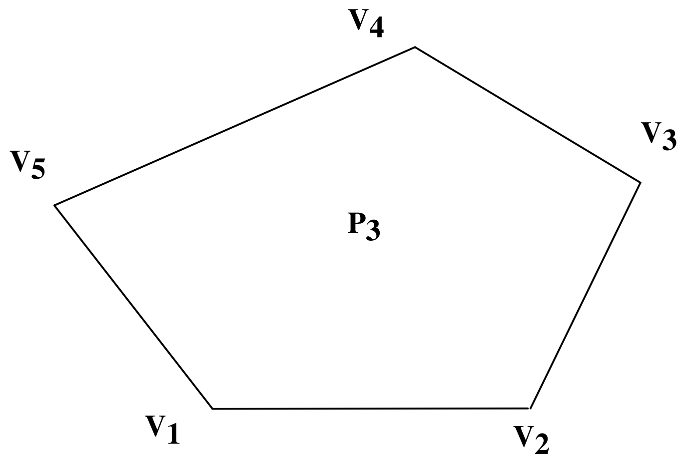
Na osnovu ***Napomene 13*** P_1 je integralno rastavljiv u smislu sume Minkovskog.

Neka je P_2 petougao sa celobrojnim temenima bez paralelnih ivica kod koga je zbir svaka dva susedna unutrašnja ugla striktno manji od π, prikazan na slici 36.



Slika 36

Neka je P_3 petougao sa celobrojnim temenima bez paralelnih ivica kod koga je zbir svaka dva susedna unutrašnja ugla striktno veći od π, prikazan na slici 37.

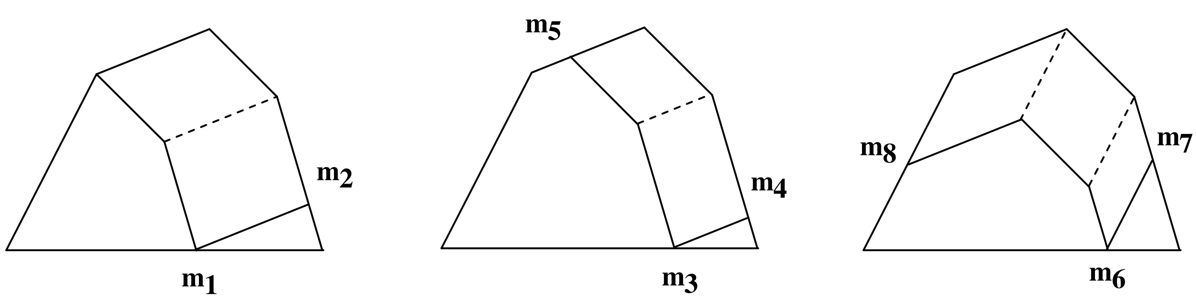


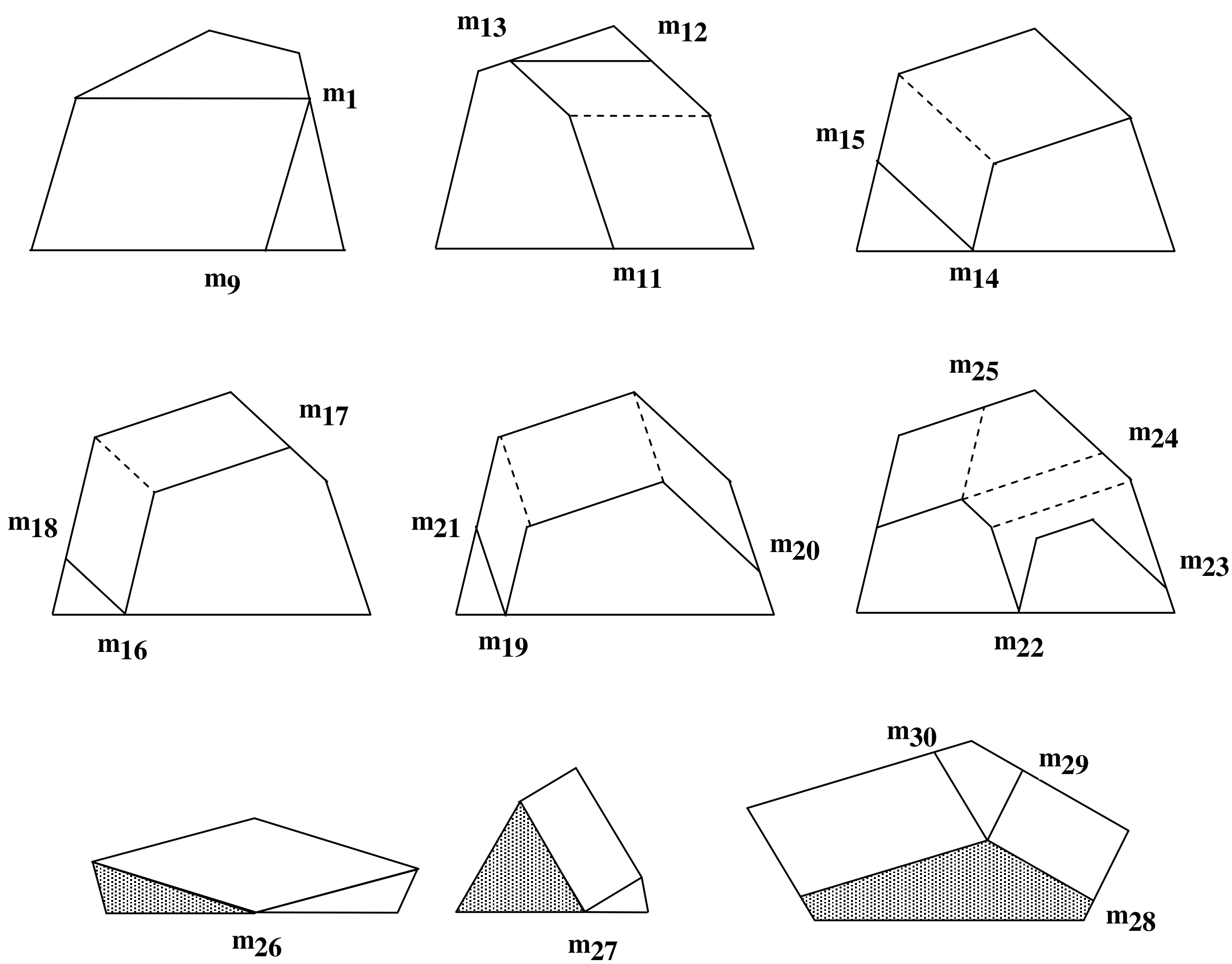
Slika 37

Na slici 38 dajemo neke postupke dekompozicije integralno rastavljivih petouglova tipa P_2 i P_3. Na osnovu ***Teoreme 12***, na duži otvorenoj (v_1, v_2) postoji celobrojna tačka m_1 ako i samo ako važi:

$$NZD(v_2 - v_1) \neq 1 .$$

Dakle, pretpostavljamo da je $NZD(v_2 - v_1) \neq 1$ čime obezbeđujemo da tačka m_1 bude celobrojna.
Potpuno analogno obezbeđujemo da ostale tačke m_i budu celobrojne.





Slika 38

<u>Teorema 16:</u> Petougao P bez paralelnih ivica sa ivičnim nizom vektora $\{e_1, e_2, e_3, e_4, e_5\}$, gde su e_1, e_2, e_3, e_4, e_5 primitivni vektori je integralno nerastavljiv u smislu sume Minkovskog.

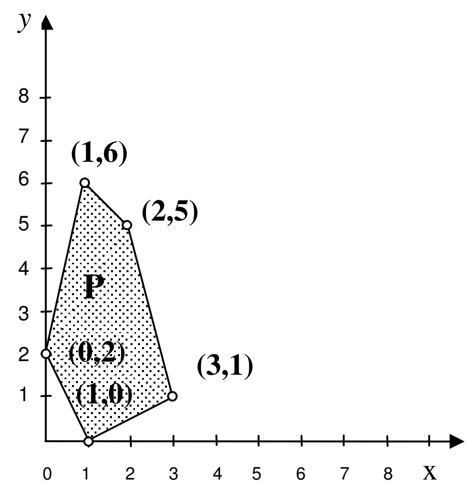
Dokaz:
Ivični niz vektora $\{e_1, e_2, e_3, e_4, e_5\}$ petougla P ne može imati podniz čija je suma nula, s obzirom da važi $e_1 + e_2 + e_3 + e_4 + e_5 = 0$. □

Ilustrujmo primenu ***Teoreme 16*** sledećim primerima.

<u>Primer 14:</u> Posmatrajmo petougao P sa celobrojnim temenima:

$$P = conv\big((0,2),(1,0),(3,1),(2,5),(1,6)\big),$$

prikazan je na slici 39.



Slika 39

Ivični niz vektora petougla P je:

$$\{(1,0)-(0,2),(3,1)-(1,0),(2,5)-(3,1),(1,6)-(2,5),(0,2)-(1,6)\}.$$

Odnosno:

$$\{(1,-2),(2,1),(-1,4),(-1,1),(-1,-4)\}.$$

Sa slike 39 je očigledno da P nema paralelnih ivica.

Na osnovu ***Teoreme 16***, petougao P sa ivičnim nizom vektora $\{e_1,e_2,e_3,e_4,e_5\}$, gde su $e_1=(1,-2),e_2=(2,1),e_3=(-1,4),e_4=(-1,1),e_5=(-1,-4)$ primitivni vektori, je nerastavljiv u smislu sume Minkovskog.

S obzirom da je četvorougao P Njutnov poligon polinoma:

$$f(x,y)=a_1x+a_2y^2+a_3x^3y+a_4x^2y^5+a_5xy^6,\ a_1,...,a_5\in\mathbb{F}\backslash\{0\},$$

zaključujemo da je polinom $f(x,y)$ apsolutno nesvodljiv nad $\mathbb{F}$, gde je $\mathbb{F}$ proizvoljno polje.

Polinom $f(x,y)$ "ostaje" apsolutno nesvodljiv nad poljem $\mathbb{F}$ ako mu dodamo nove terme čiji vektori eksponenata leže u Njutnovom poligonu polinoma $f(x,y)$ - petouglu P.

Drugim rečima, svaki polinom oblika:

$$f(x,y)=a_1x+a_2y^2+a_3x^3y+a_4x^2y^5+a_5xy^6+\sum c_{ij}x^iy^j,\ a_1,...,a_5\in\mathbb{F}\backslash\{0\}\text{ i }(i,j)\in P,$$

je apsolutno nesvodljiv nad $\mathbb{F}$.

<u>Primer 15:</u> Neka su m,n pozitivni celi brojevi takvi da važi:

$$NZD(m,n)=1.$$

Posmatrajmo petougao $P_{m,n}$ sa celobrojnim temenima:

$$P_{m,n}=conv((m,0),(0,n),(m+1,n+1),(m,n+m+1),(0,m+1)).$$

Ivični niz vektora petougla $P_{m,n}$ je:

$$\{(0,n)-(m,0),(m+1,n+1)-(0,n),(m,n+m+1)-(m+1,n+1),(0,m+1)-(m,n+m+1),(m,0)-(0,m+1)\}.$$

Odnosno:

$$\{(-m,n),(m+1,1),(-1,m),(-m,-n),(m,-(m+1))\}.$$

Očigledno je da su vektori:

$$e_2=(m+1,1) \text{ i } e_3=(-1,m)$$

primitivni vektori jer je $NZD(\pm 1,c)=1$, gde je c proizvoljan prirodan broj.
Vektori:

$$e_1=(-m,n) \text{ i } e_4=(-m,-n)$$

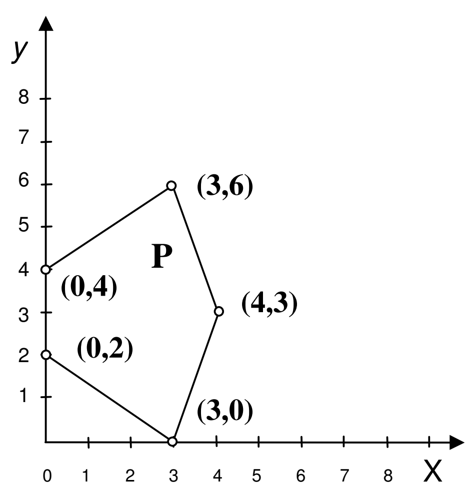
su primitivni vektori jer je $NZD(m,n)=1$.
Vektor:

$$e_5=(m,-(m+1))$$

je primitivni vektor jer je $NZD(c,-(c+1))=1$, gde je c proizvoljan prirodan broj.
Dakle, ivični niz $\{e_1,e_2,e_3,e_4,e_5\}$, $e_1=(-m,n)$, $e_2=(m+1,1)$, $e_3=(-1,m)$, $e_4=(-m,-n)$, $e_5=(m,-(m+1))$ petougla $P_{m,n}$ je niz primitivnih vektora, pa je na osnovu ***Teoreme 15*** petougao $P_{m,n}$ nerastavljiv u smislu sume Minkovskog.
Odavde zaključujemo da je svaki polinom sa dve promenljive čiji je Njutnov poligon petougao $P_{m,n}$ apsolutno nesvodljiv nad proizvoljnim poljem $\mathbb{F}$.
Na primer, uzmimo da je $m=3$, $n=2$. Jasno, $NZD(3,2)=1$ tako da je petougao:

$$P_{3,2}=conv((3,0),(0,2),(4,3),(3,6),(0,4)),$$

prikazan na slici 40 nerastavljiv u smislu sume Minkovskog.



Slika 40

Sa slike 40 je očigledno da $P_{m,n}$ nema paralelnih ivica za proizvoljne pozitivne cele brojeve m,n, tako da možemo primeniti ***Teoremu 16***.

S obzirom da je petougao $P_{3,2}$ Njutnov poligon polinoma:

$$f(x,y)=a_1x^3+a_2y^2+a_3x^4y^3+a_4x^3y^6+a_5y^3,\ a_1,\dots,a_5\in\mathbb{F}\backslash\{0\},$$

zaključujemo da je polinom $f(x,y)$ apsolutno nesvodljiv nad proizvoljnim poljem $\mathbb{F}$.

Jasno, svaki polinom oblika:

$$f(x,y)=a_1x^3+a_2y^2+a_3x^4y^3+a_4x^3y^6+a_5y^3+\sum c_{ij}x^iy^j,\ a_1,\dots,a_5\in\mathbb{F}\backslash\{0\}\text{ i }(i,j)\in P,$$

je apsolutno nesvodljiv nad $\mathbb{F}$.

6. LITERATURA

1. Abu Salem F., Gao S., Lauder A. G. B., Factoring polynomials via polytopes: extended version, Report PRG-RR-04-07, Oxford University Computing Laboratory, 2004.
2. Carlitz L., The distribution of irreducible polynomials in several indeterminates, Illinois J. Math. 7, 371-375, 1963.
3. Cohen S., The distribution of irreducible polynomials in several indeterminates over a finite field. Proc. Edinburgh Math. Soc. 16 1–17, 1968/1969.
4. Duval D., Absolute factorization of polynomials: a geometric approach, SIAM J. Comput. 20, 1-21, 1991.
5. Ewald G., Combinatorial Convexity and Algebraic Geometry, GTM 168, Springer, 1996.
6. Gale D., Irreducible convex sets, Proc. Intern. Congr. Math., Amsterdam, Vol. 2, 217-18, 1954.
7. Gao S., Absolute irreducibility of polynomials via Newton polytopes, Journal of Algebra 237, No.2 501-520, 2001.
8. Gao S., Factoring multivariate polynomials via partial diferential equations, Mathematics of Computation 72, 242, 801-822, 2003.
9. Gao S., Lauder A. G. B., Decomposition of polytopes and polynomials, Discrete and Computational Geometry 26, 89–104, 2001.
10. Gao S., Lauder A.G.B., Fast absolute irreducibility testing via Newton polytopes, preprint 2003.
11. von zur Gathen J., Irreducibility of multivariate polynomials J. Comput. System Sci. 31, no. 2, 225-264, 1985.
12. von zur Gathen J., Kaltofen E., Factorization of multivariate polynomials over finite fields, Math. Comp. 45, no. 171, 251-261, 1985.
13. Gruber P. M., Wills J. M., Handbook of Convex Geometry, Vol. A and B, Elsevier Science, Amsterdam, 1993.
14. Grünbaum B., Convex Polytopes, Interscience Publ., London, New York, Sydney, 1967.
15. Kallay M., Indecomposable polytopes, Israel J. Math. 41, no. 3, 235-43, 1982.
16. Kaltofen E., Fast parallel absolute irreducibility testing, J. Symbolic Computation 1, 57-67, 1985.
17. Kaltofen E., Polynomial factorization 1987-1991, Proc. LATIN '92 (Sao Paulo, 1992), I. Simon (Ed.), Lecture Notes Comput. Sci., vol. 583, 294-313, Springer, Berlin, 1992.
18. Koyuncu F., A geometric approach to absolute irreducibility of polynomials, The Middle East Technical University – The Department of Mathematics, 2004.
19. Koyuncu F., An application of the polytope method, JFS, Vol 28, 13-19, 2005.
20. Lenstra A. K., Factoring multivariate polynomials over finite fields, J. Comput. System Sci. 30, no. 2, 235-248, 1985.
21. Lipkovski A., Newton polyhedra and irreducibility, Math. Z. 199, 119-127, 1988.
22. McMullen P., Indecomposable convex polytopes, Israel J. Math. 58, no.3, 321-323, 1987.
23. Meyer W., Indecomposable polytopes, Trans. Amer. Math. Soc. 190, 77-86, 1974.
24. Musser D. R., Multivariate Polynomial Factorization. J. ACM 22, 291-308, 1976.
25. Ostrowski A. M., On multiplication and factorization of polynomials, I. Lexicographic ordering and extreme aggregates of terms, Aequationes Math. 13, 201-228, 1975.
26. Ostrowski A. M., On multiplication and factorization of polynomials, II. Irreducibility discussion, Aequationes Math. 14, 1-32, 1976.
27. Schinzel A., Polynomials with special regard to reducibility, Encyclopedia of Mathematics and its Applications 77. Cambridge University, 2000.
28. Schneider R., Convex bodies: the Brunn-Minkowski theory, Encyclopedia of Mathematics and its Applications, 44. Cambridge University Press, Cambridge, 1993.
29. Shanok C., Convex polyhedra and criteria for irreducibility, Duke Mathematical Journal 2 , 103-111, 1936.
30. Shephard G. C., Decomposable convex polyhedra, Mathematika 10, 89-95, 1963.
31. Smilansky Z., An indecomposable polytope all of whose facets are decomposable, Mathematika 33, no. 2, 192-196, 1986.
32. Smilansky Z., Decomposability of polytopes and polyhedra, Geometriae Dedicata 24, no. 1, 29-49, 1987.
33. Wang, P. S., Rothschild, L. P. : Factoring Multivariate Polynomials over the Integers. Math. Comp. 29, 935-950 1975.
34. Webster R., Convexity, Oxford University Press, Oxford, 1994.
35. Ziegler G. M., Lectures on Polytopes, GTM 152, Springer-Verlag, 1995.

BIOGRAFIJA

Rođen sam 01.08.1978. u Novom Sadu gde sam završio osnovnu školu "Đura Daničić", gimnaziju "Jovan Jovanović - Zmaj" i Prirodno – matematički fakultet, odsek za matematiku, smer diplomirani inženjer matematike. Akademske master studije na Prirodno – matematičkom fakultetu, studijski program diplomirani matematičar – master primenjene matematike upisao sam školske 2008./09. Nakon polaganja planom i programom predviđenih ispita za ovaj smer, pristupio sam izradi master teze "Nesvodljivost polinoma dve promenljive" pod mentorstvom prof. dr Siniše Crvenkovića.
Zaposlen sam na Visokoj poslovnoj školi strukovnih studija u Novom Sadu kao saradnik u nastavi za matematičke nastavne discipline gde držim vežbe iz predmeta "Matematika" za studente prve i "Primena informacionih tehnologija" za studente druge godine.

UNIVERZITET U NOVOM SADU
PRIRODNO-MATEMATIČKI FAKULTET
KLJUČNA DOKUMENTACIJSKA INFORMACIJA

Redni broj:
RBR
Identifikacioni broj:
IBR
Tip dokumentacije: Monografska dokumentacija
TD
Tip zapisa: Tekstualni štampani materijal
TZ
Vrsta rada: Završni rad
VR
Autor: Ivan Pavkov
AU
Mentor: Prof. dr Siniša Crvenković
MN
Naslov rada: Nesvodljivost polinoma dve promenljive
MR
Jezik publikacije: Srpski (latinica)
JP
Jezik izvoda: srpski/engleski
JI
Zemlja publikovanja: Srbija
ZP
Uže geografsko područje: Vojvodina
UGP
Godina: 2010.
GO
Izdavač: Autorski reprint
IZ
Mesto i adresa: Novi Sad, Departman za matematiku i informatiku, PMF, Trg Dositeja Obradovića 4
MA
Fizički opis rada: 6 glava, 4 poglavlja, 53 strane
FO
Naučna oblast: Matematika
NO
Naučna disciplina: Algebra
ND
Ključne reči: redak polinom, polinom sa dve promenljive, konveksni omotač, Njutnov poligon polinoma sa dve promenljive , integralno nerastavljiv konveksan poligon sa celobrojnim temenima , suma Minkovskog, apsolutna nesvodljivost

PO
UDK:

Čuva se: U biblioteci Departmana za matematiku i informatiku
ČU
Važna napomena:
VN
Izvod:
IZ

Tema ovog rada je nesvodljivost jedne specijalne klase polinoma sa dve promenljive – potklase klase retkih ("sparse") polinoma. Svakom polinomu sa dve promenljive pridužujemo konveksan poligon sa celobrojnim temenima, tzv. Njutnov poligon. Polinom sa dve promenljive je apsolutno nesvodljiv nad proizvoljnim poljem ako je njemu pridruženi Njutnov poligon integralno nerastavljiv u smislu sume Minkovskog. Zbog toga je glavni cilj rada pronalaženje nerastavljivih poligona sa celobrojnim temenima i odgovarajućih apsolutno nesvodljivih polinoma. U radu će biti prezentovani kriterijumi nerastavljivosti za duži, trouglove, konveksne četvorouglove i konveksne petouglove.

Datum prihvatanja teme od strane NN veća: 24.09.2009.
DP
Datum odbrane:.
DO
Članovi komisije:
KO
Predsednik**:** Dr. Petar Marković, vanredni profesor Prirodno-matematičkog fakulteta u Novom Sadu
Član**:** Dr. Siniša Crvenković, redovni profesor Prirodno-matematičkog fakulteta u Novom Sadu, mentor
Član**:** Dr. Petar Đapić, docent Prirodno-matematičkog fakulteta u Novom Sadu

UNIVERSITY OF NOVI SAD
FAKULTY OF NATURAL SCIENCES AND MATHEMATICS
KEY WORDS DOCUMENTATION

Accession number:
ANO
Identification number:
INO
Document type: Monograph type
DT
Type of record: Printed text
TR
Contents Code: Master thesis
CC
Author: Ivan Pavkov
AU
Mentor: Ph. D. Siniša Crvenković
MN
Title: Irreducibility of polynomials in two variables
TI
Language of text: Serbian
LT
Language of abstract: English
LA
Country of publication: Serbia
CP
Locality of publication: Vojvodina
LP
Publication year: 2010.
PY
Publisher: Author's reprint
PU
Publ. place: Novi Sad, Faculty of Natural Sciences and Mathematics, Trg Dositeja Obradovića 4
PP
Physical description: 6 chapters, 4 subchapters, 53 pages
PD
Scientific field: Mathematics
SF
Scientific discipline: Algebra
SD
Key words: sparse polynomial, polynomial in two variables, convex hull, Newton polygon of a polynomial in two variables, integrally indecomposable integral convex polygon, Minkowski sum, absolute irreducibility

UC:

Holding data: In library of Department of Mathematics
HD
Note:
N
Abstract:
AB
The main subject of this thesis is irreducibility of a subclass of sparse polynomials in two variables. Any polynomial in two variables is associated with a integral convex polygon in Euclidan plane called Newton polygon. Polynomial in two variables is absolute irreducibile over arbitrary field if its Newton polygon is integrally indecomposable in sense of Minkowski sum. Therefore, the focus of this paper is determining indecomposable integral convex polygons and corresponding polynomials. We shall give some indecomposability criteria for line segments, triangles, convex quadrangles and convex pentagons.
Accepted by the Scientific Board on: 24.09.2009.
ASB
Defended:
Thesis defend board:
DB
President: Ph. D. Petar Marković, Associated Profesor, Faculty of Natural Sciences and Mathematics, University of Novi Sad
Member: Ph. D. Siniša Crvenković, Full Profesor, Faculty of Natural Sciences and Mathematics, University of Novi Sad, menthor
Member: Ph. D. Petar Đapić, Assistant Profesor, Faculty of Natural Sciences and Mathematics, University of Novi Sad