UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO
Pedagoška matematika – 2. stopnja

Sara Rolih

NEDESARGUESOVE RAVNINE

Magistrsko delo

Mentor: doc. dr. Aleš Vavpetič

Ljubljana, 2015

Podpisana Sara Rolih izjavljam:

- da sem magistrsko delo z naslovom *Nedesarguesove ravnine* izdelala samostojno pod mentorstvom doc. dr. Aleša Vavpetiča in
- da Fakulteti za matematiko in fiziko Univerze v Ljubljani dovoljujem objavo elektronske oblike svojega dela na spletnih straneh.

Ljubljana, 2015 Podpis: .....

Zahvala

Iz srca se zahvaljujem mentorju doc. dr. Alešu Vavpetiču, boljšega si ne bi mogla želeti. Hvala za vse popravke, komentarje, razlage in predvsem hvala za potrpežljivost.

Zahvaljujem se staršem, sestricama in vsej svoji družini, ki me je podpirala na tej (ne tako kratki) poti in mi vlivala upanje, da zmorem.

Hvala tudi vsem in vsakemu profesorju posebej, da so me vodili skozi študij s prijaznostjo, dostopnostjo in ogromno zakladnico znanja.

Predvsem pa hvala Marku. Za vse.

Kazalo

Slike

Program dela

Magistrsko delo naj opiše nekaj nedesarguesovih afinih in projektivnih ravnin.

Osnovna literatura: D. R. Hughes in F. C. Piper, *Projective planes*, Graduate Texts in Mathematics, Vol. 6. Springer-Verlag, New York-Berlin, 1973.

Ljubljana, 2015

doc. dr. Aleš Vavpetič

Povzetek

V magistrskem delu bomo spoznali nekaj primerov afinih in projektivnih nedesarguesovih ravnin, kjer se bomo v glavnem osredotočili na ravnine končnega reda. V ravnino bomo uvedli koordinate nad ternarnimi kolobarji ter definirali izomorfizem in izotopizem le-teh. Podrobneje bomo predstavili Veblen-Wedderburnove sisteme oziroma kvazi polja ter na njih definirali ternarno operacijo. Z uporabo različnih kvazi polj ter translacij ravnin bomo konstruirali nekaj najbolj znanih primerov afinih in projektivnih nedesarguesovih ravnin.

Abstract

In this masters thesis we shall look at some examples of affine and projective non-Desarguesian planes and we will mainly discuss finite planes. We will coordinatizate plane and introduce ternary rings and later isomorphisms and isotopisms of them. We shall introduce Veblen-Wedderburn systems or quasifileds, which is more common expression and then we will define a ternary operation on them. By using different quasifield and translations we shall expose some of the most known examples of affine and projective non Desarguesian planes.

Math. Subj. Class. (2010): 51A35, 51E15, 12K05, 12K10.

Ključne besede: nedesarguesova ravnina, afina geometrija, projektivna geometrija, obseg, kvazi polje, skoraj polje, polpolje, translacija, izomorfizem, izotopizem.

Keywords: non-Desarguesian plane, affine geometry, projective geometry, skewfield, quasifield, near-field, semifield, translation, isomorphism, isotopism.

1. Uvod

Že tekom študija smo spoznali afino in projektivno geometrijo in prav tako oba Desarguesova izreka v afini geometriji ter enega v projektivni. V splošnem so Desarguesove geometrije tiste geometrije, ki zadoščajo Desarguesovima izrekoma v afini geometriji oziroma izreku v projektivni. Torej so nedesarguesove geometrije tiste, za katere to ne velja. Dokazano je, da so geometrije razsežnosti večje od dva, Desarguesove. Problem nastopi v razsežnosti 2, torej v ravninah.

Za začetek je dobro, da razmislimo, katere afine in projektivne ravnine sploh obstajajo. Vedno obstaja ravnina konstruirana nad poljem ali obsegom. Pri določanju obstoja končne ravnine nam pomaga Bruck-Ryserjev izrek, ki pravi, da n ne more biti red končne ravnine, če je oblike $4k + 1$ ali $4k + 2$ in hkrati ni vsota kvadratov dveh celih števil. Iz tega je jasno, da ne obstaja ravnina reda npr. 6 ali 14, nič pa iz tega izreka ne izvemo o ravninah reda npr. 10, 12, 15 itd. Dolgo časa se ni vedelo, ali obstaja ravnina reda 10, vendar so leta 1989 s pomočjo računalnika dokazali, da takšne ravnine ni.

Kako pa je z Desarguesovimi in nedesarguesovimi ravninami? Vsaka ravnina, ki je definirana nad obsegom, je Desarguesova. V članku [6] vidimo, da so projektivne ravnine do vključno reda 8 Desarguesove. Med ravninami do reda 32 so Desarguesove še ravnine reda 11, 13, 17, 19, 23, 29 in 31. Prvi primer nedesarguesove ravnine sta leta 1907 podala Veblen in Wedderburn za ravnino reda 9, ki sta ga opisala v [8]. Do reda 32 obstajajo nedesarguesove ravnine reda 9, 16, 25 in 27.

V končnih primerih je vsak obseg polje in je vsaka končna ravnina bodisi nedesarguesova bodisi definirana nad končnim poljem. V slednjem primeru je red afine ali projektivne ravnine enak $n = p^k$, kjer je p praštevilo, k pa pozitivno celo število.

V delu bomo spoznali nekatere primere afinih in projektivnih nedesarguesovih ravnin. V ravnine bomo vpeljali koordinatni sistem nad ternarnimi kolobarji. Če ternarni kolobar ni izomorfen obsegu, je ravnina nedesarguesova. Več primerov bomo prikazali tudi s pomočjo kvazi polj in translacij.

Red ravnine n	Število izomorfnih ravnin reda n	Opomba
2	1	Desarguesova
3	1	Desarguesova
4	1	Desarguesova
5	1	Desarguesova
7	1	Desarguesova
8	1	Desarguesova
9	4	Obstaja nedesarguesova
11	≥ 1	Desarguesova
13	≥ 1	Desarguesova
16	≥ 22	Obstaja nedesarguesova
17	≥ 1	Desarguesova
19	≥ 1	Desarguesova
23	≥ 1	Desarguesova
25	≥ 193	Obstaja nedesarguesova
27	≥ 13	Obstaja nedesarguesova
29	≥ 1	Desarguesova
31	≥ 1	Desarguesova

Tabela 1.1: Število ravnin do reda 32

1.1 Ponovitev osnovnih pojmov

V magistrskem delu bom uporabljala nekatere pojme, ki smo jih tekom študija že spoznali, za lažje razumevanje pa ponovimo nekaj le-teh in spoznajmo nekatere, ki so mogoče novi in jih bomo potrebovali.

Množica skupaj z binarno operacijo se imenuje *grupoid*. Grupoid v katerem je operacija asociativna se imenuje *polgrupa*. Polgrupa z nevtralnim elementom (enoto) se imenuje *monoid* (ali *polgrupa z enoto*, če je operacija pisana multiplikativno). Monoid, v katerem ima vsak element inverz imenujemo *grupa*.

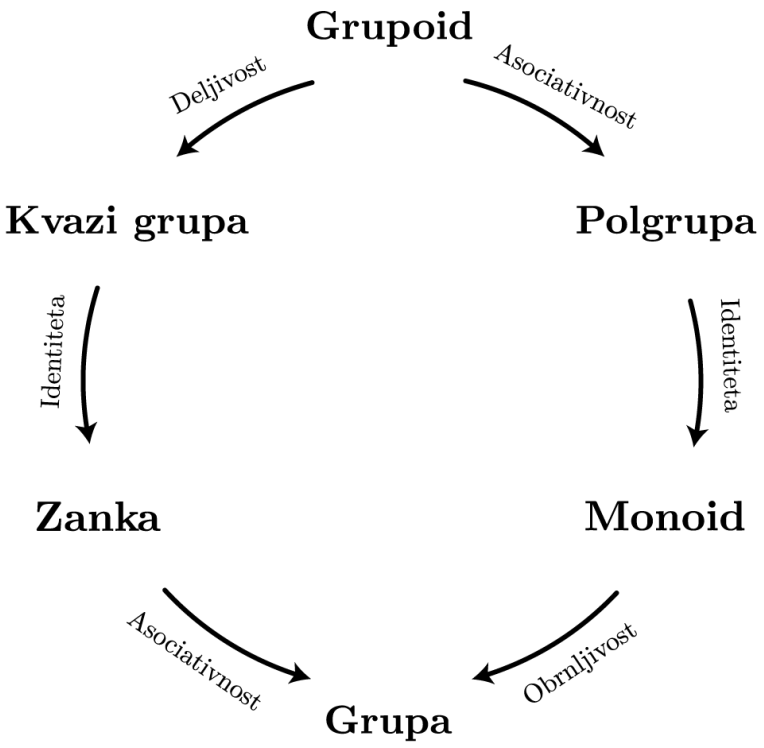
Kvazi grupa $(Q, \cdot)$ je množica Q z binarno operacijo $\cdot$, v kateri za vsaka $a, b \in Q$ obstajata natanko določena elementa $x, y \in Q$, da velja:

$$a \cdot x = b,$$
$$y \cdot a = b.$$

Zanka je kvazi grupa z nevtralnim elementom, tj. obstaja $e \in Q$, da za vsak $x \in Q$

velja:

$$x \cdot e = x,$$
$$e \cdot x = x.$$



Slika 1.1: Diagram

Naj bosta G in G' grupi. Preslikavi $\varphi\colon G \to G'$ pravimo *homomorfizem (grup)*, če je $\varphi(xy) = \varphi(x)\varphi(y)$ za vse $x, y \in G$.

Endomorfizem je homomorfizem iz G v G, *izomorfizem* je bijektivni homomorfizem, *avtomorfizem* je izomorfizem iz G v G, *monomorfizem* je injektivni homomorfizem oz. *vložitev*, *epimorfizem* je surjektivni homomorfizem.

Naj bo $\varphi\colon G \to G'$ homomorfizem. *Jedro* homomorfizma φ je množica $\ker \varphi = \{x \in G \mid \varphi(x) = e_G\}$, kjer je e_G enota grupe G. *Slika* homomorfizma φ je množica $\operatorname{Im} \varphi = \{\varphi(x) \mid x \in G\}$.

Poglejmo še množice, v katerih sta definirani dve računski operaciji. Množici K pravimo *kolobar*, če je K za seštevanje Abelova grupa (torej komutativna), za

množenje velja asociativnostni zakon in množenje ter seštevanje povezuje distributivnostni zakon. Kolobar, ki vsebuje tudi nevtralni element za množenje, imenujemo kolobar z enoto. Če ima poleg tega vsak element kolobarja (razen elementa 0) svoj inverzni element za množenje, pravimo taki množici *obseg*. Obseg, v katerem je množenje komutativno, imenujemo komutativni obseg ali *polje*.

Vektorski prostor V nad obsegom O je Abelova grupa za $(V, +)$ skupaj s preslikavo

$$O \times V \to V, \quad (a, x) \mapsto ax,$$

ki izpolnjuje pogoje

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

za vsaka $a, b \in O$ in za vsaka $x, y \in V$.

2. Nedesarguesove afine ravnine

V tem poglavju v glavnem sledimo razlagi iz [4] in [3].

2.1 Uvod

Afina ravnina $\mathbb{A}$ je množica točk skupaj s množico premic, ki je podmnožica potenčne množice $P(\mathbb{A})$, če zadošča spodnjim trem aksiomom:

A1. Skozi poljubni točki poteka natanko ena premica.

A2. Za vsako premico l in točko P, ki ne leži na premici, obstaja natanko ena premica, ki poteka skozi P in je l vzporedna. (Premici sta vzporedni ($p \parallel q$), če se ne sekata v nobeni točki ali če sovpadata.)

A3. Obstajajo tri nekolinearne točke. (Točke so nekolinearne, če ne ležijo na isti premici.)

V afini ravnini sta poljubni premici enako močni, kar bomo dokazali v razdelku 2.2. Afini ravnini $\mathbb{A}$ in $\mathbb{A}'$ sta *izomorfni*, če obstaja bijekcija $\mathbb{A} \to \mathbb{A}'$, ki slika premice v premice.

Izrek 2.1. *(po [2, stran 84]) Če je $\mathbb{A}$ končna afina ravnina, obstaja celo število $n \geq 2$, ki mu pravimo red afine ravnine $\mathbb{A}$, da velja:*

i) afina ravnina $\mathbb{A}$ vsebuje n^2 točk in $n^2 + n$ premic,

ii) vsaka premica vsebuje n točk,

iii) vsaka točka leži na $n + 1$ premicah,

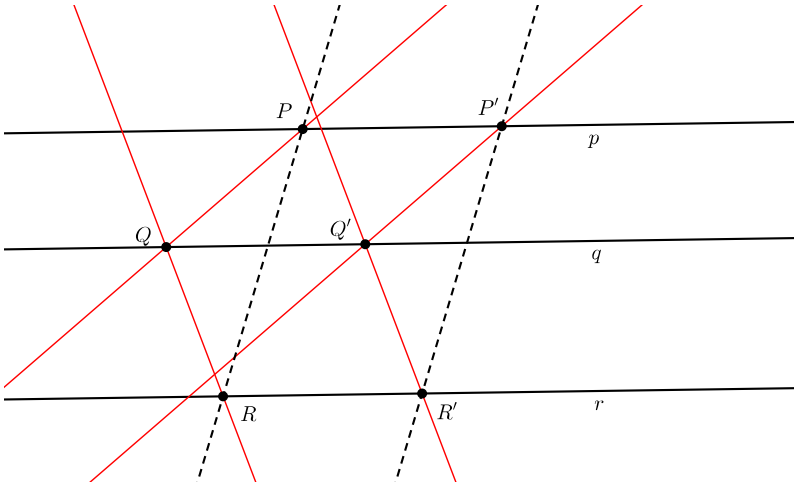
iv) vsak razred vzporednic vsebuje n premic in obstaja $n + 1$ razredov vzporednic.

Osnovne primere afinih ravnin lahko podamo z obsegi. Za obseg K lahko vzamemo $\mathbb{A} = K^2$ z množico premic $P = \{(x, ax + b) \mid x, a, b \in K\}$ ter $P_c = \{(c, y) \mid$

$y \in K\}$, kjer je c poljuben element iz K. Če je afina ravnina izomorfna K^2, rečemo, da je definirana nad K.

Razred afinih ravnin, definiranih nad obsegi je definiran geometrijsko. Afina ravnina $\mathbb{A}$ je definirana nad obsegom, če in samo če $\mathbb{A}$ zadošča prvemu in drugemu Desarguesovemu izreku. Oba naslednja izreka in njuna dokaza so iz [7].

Izrek 2.2 (Prvi Desarguesov izrek)**.** *Naj bo $\mathbb{A}$ afina ravnina nad obsegom in p, q in r različne vzporedne premice v njej. Če za točke $P, P' \in p$, $Q, Q' \in q$ in $R, R' \in r$ velja $PQ \parallel P'Q'$ in $QR \parallel Q'R'$, je $PR \parallel P'R'$.*

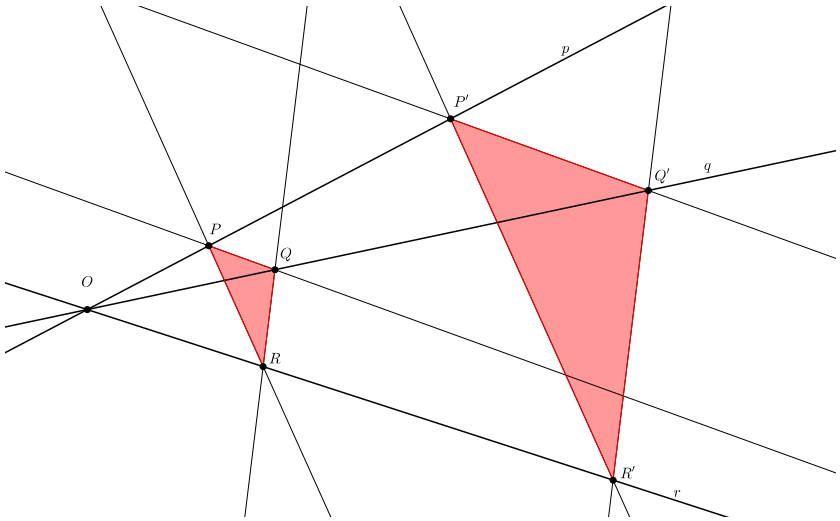


Slika 2.1: Prikaz prvega Desarguesovega izreka

Izrek 2.3 (Drugi Desarguesov izrek)**.** *Naj bo $\mathbb{A}$ afina ravnina ter p, q in r različne premice v njej, ki gredo skozi isto točko O. Če za točke $P, P' \in p$, $Q, Q' \in q$ in $R, R' \in r$ velja $PQ \parallel P'Q'$ in $QR \parallel Q'R'$, je $PR \parallel P'R'$.*

V bistvu pravimo, da je afina ravnina nedesarguesova, če ni definirana nad obsegom. Cilj magistrske naloge je predstaviti nekatere primere nedesarguesovih ravnin.

V razdelku 2.2 bomo v afino ravnino uvedli koordinate. Te koordinate točk vzamemo iz množice s ternarno operacijo imenovane *ternarni kolobar*. Vsak ternarni kolobar definira afino ravnino. Težavo nam povzroča dejstvo, da lahko izomorfne afine ravnine koordinatiziramo (v ravnino vpeljemo koordinatni sistem) s ternarnimi kolobarji, ki niso izomorfni. Ob dodatnih pogojih, o katerih bomo več povedali v razdelku 2.3, pa postanejo izomorfni. V razdelku 2.4 bomo spoznali *izotopizme* ternarnih kolobarjev, ki so povezani z izomorfizmi afinih ravnin. Naprej



Slika 2.2: Prikaz drugega Desarguesovega izreka

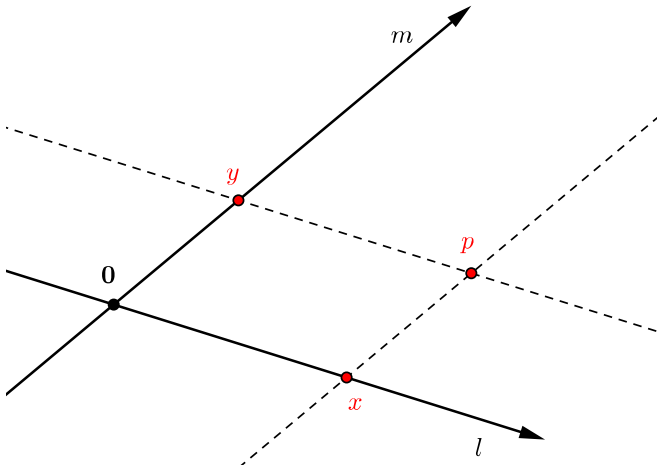
bomo v razdelku 2.5 predstavili najbolj konkretnen razred ternarnih kolobarjev imenovan *Veblen-Wedderburnovi sistemi* ali *kvazi polja*. Podobno kot polja, so kvazi polja množice z binarnima operacijama, vendar ne zadostujejo vsem aksiomom kot polje. V razdelkih 2.6 in 2.7 spoznamo različna načina, s katerima lahko dokažemo, da afina ravnina ni definirana nad obsegom. Naprej v razdelku 2.8 konstruiramo kvazi polja, ki niso izomorfna obsegu. Končno bomo v razdelku 2.9 združili ugotovitve prejšnjih razdelkov, da lahko konstruiramo nedesarguesove ravnine.

2.2 Afine ravnine in ternarni kolobarji

Naj bo $\mathbb{A}$ afina ravnina. Vpeljali bomo kartezične koordinate v $\mathbb{A}$. S pomočjo teh koordinat bomo definirali ternarno operacijo na poljubni premici iz $\mathbb{A}$. Lastnosti te operacije bomo definirali kot aksiome.

Začnimo s tem, da izberemo nevzporedni premici l in m v $\mathbb{A}$. S takšno izbiro premic bomo lahko definirali $\mathbb{A}$ s kartezičnim produktom $l \times m$ podobno kot v Evklidski ravnini. Vsaki točki p iz $\mathbb{A}$ lahko priredimo par $(x, y) \in l \times m$, kjer je x presečišče premice l in premice, ki gre skozi p in je vzporedna m. Podobno je y presečišče premice m s premico, ki je vzporedna l in gre skozi točko p. To nas pripelje do preslikave $\mathbb{A} \to l \times m$. Preslikavo $l \times m \to \mathbb{A}$ pa definiramo tako, da paru (x, y) priredimo presečišče premice, ki vsebuje x in je vzporedna m ter premice, ki vsebuje y in je vzporedna l. Ti dve preslikavi sta med seboj inverzni in ju bomo uporabili za identifikacijo $\mathbb{A}$ z $l \times m$.

Označimo z **0** presečišče premic l in m. To bo izhodišče našega koordinatnega sistema.

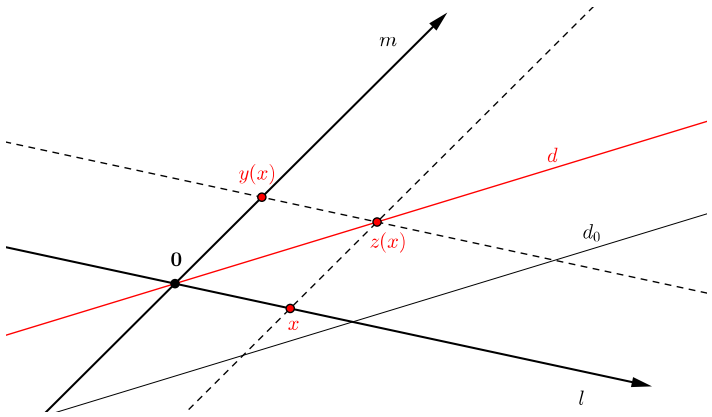


Slika 2.3: Prikaz kordinatnega sistema

Izberimo premico d, ki gre skozi **0** in je različna od l in m. Pri izbiri premice si lahko pomagamo tako, da izberemo poljubno premico d_0, ki seka l in m v točkah različnih od **0** ter za d vzamemo vzporednico tej premici, ki poteka skozi **0**. S takšno izbiro premice d, bomo lahko konstruirali bijekcijo med l in m. Od sedaj naprej predpostavimo, da je d določena. Za poljuben $x \in l$ naj bo $z(x) \in d$ presečišče d in vzporednice premici m, ki gre skozi $x \in l$. Podobno naj bo $y(x) \in m$ presečišče premice m s premico, ki gre skozi $z(x)$ in je vzporedna l. Ta konstrukcija definira bijekcijo $\varphi_d \colon l \to m$.

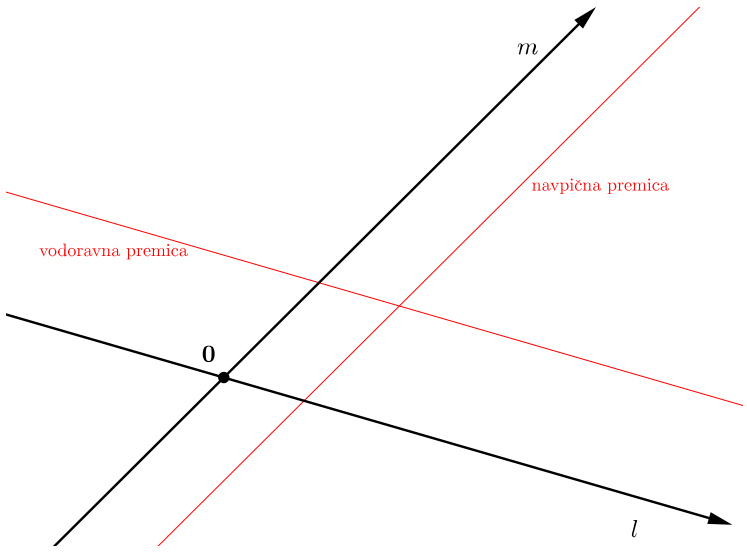
Naj bo sedaj K množica, opremljena z bijekcijo $\psi_l \colon K \to l$. Kompozitum te bijekcije in bijekcije φ_d iz prejšnjega odstavka, nam da bijekcijo $\psi_m \colon K \to m$. Formalno lahko rečemo $K = l$, vendar bomo K in l obravnavali kot različna objekta. Množica K bo imela podobno vlogo kot jo ima $\mathbb{R}$ v Evklidski geometriji.

Z uporabo danih bijekcij lahko enačimo $\mathbb{A} = K^2$. S to identifikacijo smo uvedli kartezične koordinate v $\mathbb{A}$ in premica d postane *diagonala* $\{(x, x) \mid x \in K\}$. Podobno kot pri konstrukciji kartezičnih koordinat v $\mathbb{R}$ bomo element množice K, ki ustreza točki $\mathbf{0} \in l$ označili z 0. Torej $\mathbf{0} = (0, 0)$. Radi pa bi imeli tudi število, ki je analogno 1 v Evklidski ravnini, torej enoto. To naredimo tako, da izberemo poljuben od 0 različen element množice K in ga označimo z 1, saj imamo kot v Evklidski ravnini svobodo določanja enote. Od sedaj naprej predpostavimo, da je element $1 \in K$ določen.



Slika 2.4: Koordinatni sistem s premico d

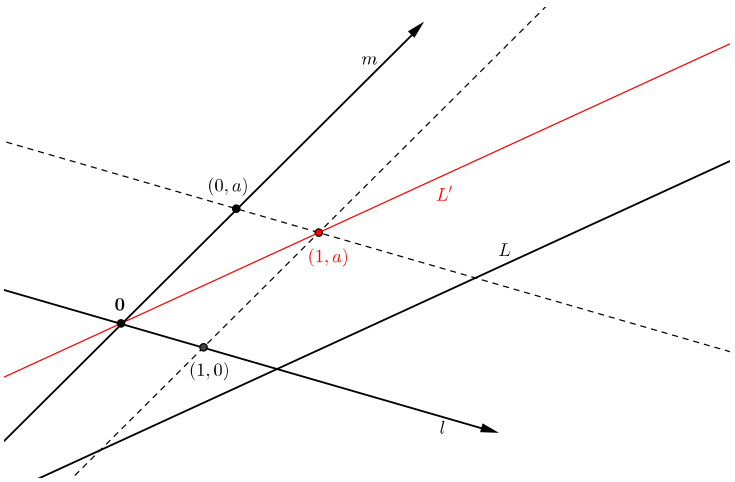
Definirajmo sedaj *naklon* premice L v $\mathbb{A}$. Če je L vzporedna l, bomo rekli, da je njen naklon 0. Takim premicam bomo rekli *vodoravne*. Če je L vzporedna m, bo njen naklon ∞ in za te premice bomo rekli, da so *navpične*.



Slika 2.5: Vodoravnica in navpičnica

Poglejmo, kaj se zgodi v primeru, ko premica L ni ne navpična ne vodoravna. Naj bo L' premica, ki je vzporedna L in gre skozi $(0,0)$. Poglejmo, kje se seka s premico $\{(1,z) \mid z \in K\}$ (to je navpičnica, ki gre skozi točko $(1,0)$). Če je presečišče v točki $(1,a)$, potem rečemo, da je a naklon premice L. Naklon premice, ki ni ne navpična in ne vodoravna, je odvisen od izbire 1. Po definiciji imajo

vzporednice enak naklon. Še več: poljubni premici sta vzporedni natanko tedaj, ko imata enak naklon. Ker d vsebuje točko $(1,1)$, je njen naklon 1.



Slika 2.6: Premica z naklonom a

Če premica L ni navpična, potem seka m v natanko eni točki $(0,b)$. Premica L je definirana z b in naklonom a. Za vsak $x \in K$, premica L seka navpičnico $\{(x,z) \mid z \in K\}$ v enolično določeni točki, recimo (x,y). V tem primeru bomo pisali:

$$y = \langle ax + b \rangle. \tag{2.1}$$

Preslikava $(a,x,b) \mapsto \langle ax+b \rangle$ je ternarna operacija v K.

Seveda je vsaka premica, ki ni navpična, množica točk $(x,y) \in K^2$, ki zadošča (2.1) za neka $a,b \in K$. Navpičnice so podane z enačbo $x = x_0$.

Kot bomo spodaj pojasnili, ternarna operacija $(a,x,b) \mapsto \langle ax+b \rangle$ zadostuje naslednjim lastnostim:

T1. Za vsak $x \in K$ je $\langle 1x+0 \rangle = \langle x1+0 \rangle = x$.

T2. Za vsaka $a,b \in K$ je $\langle a0+b \rangle = \langle 0a+b \rangle = b$.

T3. Če so $a,x,y \in K$, potem obstaja enolično določen $b \in K$, tako da velja $\langle ax+b \rangle = y$.

T4. Če so $a,a',b,b' \in K$ in $a \neq a'$, potem ima enačba $\langle ax+b \rangle = \langle a'x+b' \rangle$ enolično rešitev $x \in K$.

T5. Če so $x, y, x', y' \in K$ in $x \neq x'$, potem obstaja enolično določen par $a, b \in K$, tako da velja $y = \langle ax + b \rangle$ in $y' = \langle ax' + b \rangle$.

Pojasnimo geometrijski pomen teh lastnosti. S tem tudi dokažemo, da veljajo za $(a, x, b) \mapsto \langle ax + b \rangle$.

T1: Enačba $\langle 1x + 0 \rangle = x$ pove, da je $d = \{(x, x) \mid x \in K\}$ premica z naklonom 1. Enačba $\langle x1 + 0 \rangle = x$ pove, da je naklon premice, ki gre skozi $(0, 0)$ in $(1, x)$, enak x (kar sledi iz definicije naklona).

T2: Enačba $\langle a0 + b \rangle = b$ nam pove, da premica definirana z enačbo (2.1) seka m v $(0, b)$ (to je res po definiciji $\langle ax + b \rangle$). Enačba $\langle 0a + b \rangle = b$ pove, da na vodoravnici skozi $(0, b)$ ležijo točke $(a, b), a \in K$.

T3: To pomeni, da za vsak naklon $\neq \infty$ obstaja natanko ena premica s tem naklonom, ki gre skozi (x, y).

T4: To pomeni, da se poljubni premici z različnima naklonoma $\neq \infty$ sekata v enolično določeni točki.

T5: To pomeni, da poljubni točki, ki ne ležita na isti navpičnici (torej nista na isti premici z naklonom ∞), ležita na natanko eni premici, z naklonom $\neq \infty$.

Predpostavimo sedaj, da imamo množico K z različnima elementoma 0 in 1 ter ternarno operacijo $(a, x, b) \mapsto \langle ax + b \rangle$ za katero veljajo lastnosti **T1-T5**. Takšni množici K pravimo *ternarni kolobar*.

Poglejmo množico točk $\mathbb{A} = K^2$, kjer definiramo premice tako: za vsak $x_0 \in K$ obstaja premica $\{(x_0, y) \mid y \in K\}$ (torej navpičnica) in za vsaka $a, b \in K$ obstaja premica $\{(x, \langle ax + b \rangle) \mid x \in K\}$. To definira strukturo afine ravnine na $\mathbb{A} = K^2$.

Preverimo, da aksiomi afine ravnine držijo:

A1. Dokazati moramo, da skozi poljubni točki poteka natanko ena premica. Naj bosta $T_1 = (t, u)$ in $T_2 = (v, z)$ poljubni točki iz afine ravnine. Če je $t = v$, ležita točki na navpičnici $x = t$. V nasprotnem primeru aksiom drži po **T5**.

A2. Pokazati je potrebno, da za vsako premico l in točko P, ki ne leži na premici, obstaja natanko ena vzporednica premici l, ki poteka skozi P. Če je l navpičnica z enačbo $x = x_0$ in ima točka P koordinate (u, z), potem je iskana vzporednica $x = u$. V nasprotnem primeru to sledi iz **T3**: podane imamo koordinate točke in naklon.

A3. Želimo pokazati, da obstajajo 3 nekolinearne točke. Naj bodo te točke kar $A(0,0)$, $B(1,0)$ in $C(0,1)$. Točki A in B ležita na vodoravnici $y = 0$. Točki A in C pa ležita na navpičnici $x = 0$. Torej res obstajajo 3 nekolinearne točke.

Trditev 2.1. *Za končen K pogoj* **T5** *sledi iz* **T3** *in* **T4**.

Dokaz. Naj bosta x in x' različna elementa iz K in naj bo preslikava $f\colon K^2 \to K^2$ definirana kot

$$f(a,b) = (\langle ax + b\rangle, \langle ax' + b\rangle).$$

Predpostavimo, da f ni injektivna. Potem obstaja par $(a,b) \neq (a',b')$, da velja $f(a,b) = f(a',b')$ in je

$$\langle ax + b\rangle = \langle a'x + b'\rangle, \tag{2.2}$$

$$\langle ax' + b\rangle = \langle a'x' + b'\rangle. \tag{2.3}$$

Če je $a = a'$, potem (2.2) nasprotuje **T3**. Če $a \neq a'$, potem (2.3) nasprotuje **T4**, saj dobimo različni rešitvi x in x' za dane a, a', b, b'. Torej iz **T3** in **T4** sledi, da je f injektivna. Ker je f preslikava, ki slika iz končne množice sama vase, iz injektivnost f sledi surjektivnost f. Torej je f bijektivna. Iz tega sledi **T5**. □

2.3 Izomorfizmi ternarnih kolobarjev

Ternarni kolobar K v povezavi z afino ravnino $\mathbb{A}$ lahko konstruiramo na različne načine. Najprej je potrebno izbrati nevzporedni premici l in m. Potem moramo izbrati tretjo premico d, ki poteka skozi presečišče premic l in m (točka **0**) ter element $1 \in K$, da je $1 \neq 0$. Premica d in element 1 iz K definirata točko $z \in \mathbb{A}$: to je presečišče d s premico, ki gre skozi točko na l, ki ustreza 1 in je vzporedna premici m. Ta točka ustreza $(1,1)$ po naši identifikaciji $\mathbb{A} = K^2$. In obratno: če imamo podano točko $z \in \mathbb{A}$, ki ne leži ne na premici m, ne na premici l, lahko definiramo d kot premico, ki povezuje točko **0** s točko z, in 1 kot element K, ki je presečišče l in vzporednice z m, ki vsebuje z. Torej je izbira d in 1 enakovredna izbiri točke z, ki ne leži ne na m in ne na l.

Ternarni kolobar K je do izomorfizma natančno določen z ravnino $\mathbb{A}$ preko izbire l, m, z. Rečemo, da je K *koordinatni kolobar* ravnine $\mathbb{A}$ s trojico (l, m, z), kot zgoraj.

Definicija 2.1. Naj bo $\mathbb{A}'$ neka druga afina ravnina s premicama l' in m' ter točko z' kot zgoraj in naj bo K' njen koordinatni kolobar. Obstaja tak izomorfizem $f\colon \mathbb{A} \to \mathbb{A}'$, da je $f(l) = l'$, $f(m) = m'$ in $f(z) = z'$ natanko tedaj, ko obstaja taka bijekcija $F\colon K \to K'$, da je $F(0) = 0$, $F(1) = 1$ in velja

$$F(\langle ax + b\rangle) = \langle F(a)F(x) + F(b)\rangle$$

za vse $a, x, b \in K$. Takšni bijekciji F rečemo *izomorfizem ternarnih kolobarjev*.

2.4 Izotopizmi ternarnih kolobarjev

Ternarni kolobarji, ki so določeni z isto afino ravnino $\mathbb{A}$, isto izbiro premic l in m ter isto izbiro točke z so izomorfni. V primeru drugačne izbire točke z lahko dobimo ternarne kolobarje, ki niso izomorfni. Lahko pa ta izbira različnih točk z pripelje do ternarnih kolobarjev, ki so *izotopni*.

Trojici (F, G, H) bijekcij $K \to K'$ rečemo *izotopizem*, če je $H(0) = 0$ in velja

$$H(\langle ax + b\rangle) = \langle F(a)G(x) + H(b)\rangle$$

za vse $a, x, b \in K$. Takšna trojica porodi preslikavo $\varphi\colon K^2 \to (K')^2$ s predpisom $\varphi(x, y) = (G(x), H(y))$. Preslikava φ preslika navpičnice z enačbo $x = 0$ v navpičnice z enačbo $x = G(0)$ in φ preslika vse navpičnice v navpičnice. Iz enačbe $y = \langle ax + b\rangle$ sledi $H(y) = \langle F(a)G(x) + H(b)\rangle$, kar pomeni, da $(x', y') = \varphi(x, y)$ ustreza enačbi $y' = \langle F(a)x' + H(b)\rangle$. Sledi, da φ preslika premice z naklonom $a \neq \infty$ v premice z naklonom $F(a) \neq \infty$. Preslikava $\varphi\colon K^2 \to (K')^2$ je izomorfizem afinih ravnin.

Lema 2.1. *Preslikava φ slika vodoravnice v vodoravnice (tj. $F(0) = 0$) in točko $\mathbf{0}$ v točko $\mathbf{0}$.*

Dokaz. Da bomo lahko dokazali prvi del leme, opazimo, da φ preslika premico $\{(x, 0) \mid x \in K\}$ v premico $\{(G(x), H(0)) \mid x \in K\} = \{(x, 0) \mid x \in K'\}$ (ker je $H(0) = 0$ in je G bijekcija). Ker imata obe premici naklon 0, je $F(0) = 0$. Torej φ slika vodoravnice v vodoravnice.
Naj bosta sedaj a, a' različna naklona. Potem se premici z enačbama $y = \langle ax + 0\rangle$ in $y = \langle a'x + 0\rangle$ sekata v točki $\mathbf{0} = (0, 0)$. Njune slike so oblike $y = \langle F(a)x + 0\rangle$ in $y = \langle F(a')x + 0\rangle$ (spomnimo se, da je $H(0) = 0$). Ker je F bijekcija je $F(a) \neq F(a')$ in zato se ti premici sekata le v točki $\mathbf{0}$. Iz tega sledi, da je $\varphi(\mathbf{0}) = \mathbf{0}$. □

Posledica 2.1. *Naj bo (F, G, H) izotopizem. Potem velja poleg $H(0) = 0$ tudi $F(0) = 0$ in $G(0) = 0$.*

Dokaz. Za $F(0) = 0$ smo že dokazali. Da je $G(0) = 0$, sledi iz dejstva, da je $\varphi(\mathbf{0}) = \mathbf{0}$. Potem je $\varphi(0,0) = (G(0), H(0) = (0,0)$. Torej je $G(0) = 0$. □

Posledica 2.2. *Izomorfizem afinih ravnin porojen z izotopizmom ternarnih kolobarjev slika vodoravnico/navpičnico, ki gre skozi točko **0**, v vodoravnico/navpičnico, ki gre skozi točko **0**.*

Velja tudi obratno: Izotopizem ternarnih kolobarjev porojen z izomorfizmom afinih ravnin slika vodoravnice (navpičnice), ki vsebujejo točko **0**, v vodoravnice (navpičnice), ki vsebujejo točko **0**.

Izrek 2.4. *Naj bo K koordinatni kolobar ravnine $\mathbb{A}$ z isto izbiro elementov l, m, z kot zgoraj. Naj bo K' koordinatni kolobar ravnine $\mathbb{A}'$ z izbiro l', m', z'. Obstaja izomorfizem $\mathbb{A} \to \mathbb{A}'$, ki preslika l v l' in m v m' (vendar ne nujno z v z') natanko tedaj, ko obstaja izotopizem $K \to K'$.*

Dokaz. ($\Leftarrow$): V to smer je že dokazano.
($\Rightarrow$): Identificirajmo $\mathbb{A}$ s K^2 in $\mathbb{A}'$ s $(K')^2$. Naj bo $G\colon K \to K'$ preslikava določena s preslikavo $K \times \{0\} \to K' \times \{0\}$ porojeno s φ. Podobno naj bo $H\colon K \to K'$ preslikava določena s preslikavo $\{0\} \times K \to \{0\} \times K'$ porojeno s φ. Ker je vsaka točka presečišče enolično določene navpičnice z enolično določeno vodoravnico in ker φ preslika vodoravnice/navpičnice v vodoravnice/navpičnice vidimo, da je φ določena s preslikavama G, H in je $\varphi(x, y) = (G(x), H(y))$. Velja tudi $G(0) = 0$ in $H(0) = 0$.

Z namenom, da določimo F, definirajmo za vsak $a \in K$ premico v $\mathbb{A}$ z naklonom a, ki poteka skozi točko **0**. Preslikava φ jo slika v premico v $\mathbb{A}'$, ki gre skozi **0** in ima naklon $F(a) \in K'$.

Dokažimo sedaj, da je (F, G, H) izotopizem. Ker φ slika vzporednice v vzporednice, preslika vsako premico z naklonom a v premico z naklonom $F(a)$. Torej slika premice z enačbo $y = \langle ax + b \rangle$ v premice z enačbo $y' = \langle F(a)x' + b' \rangle$. Prva premica vsebuje točko $(0, b)$ (ker je $\langle a0 + b \rangle = b$ po **T2**). Sledi, da je $H(b) = \langle F(a)0 + b' \rangle$. Ampak $\langle F(a)0 + b' \rangle = b'$ po **T2**. Zato je $b' = H(b)$.

Vidimo, da φ preslika premico z enačbo $y = \langle ax + b \rangle$ v premico z enačbo $y' = \langle F(a)x' + H(b) \rangle$. Ker je $\varphi(x, y) = (G(x), H(y))$ iz $y = \langle ax + b \rangle$ sledi $H(y) = \langle F(a)G(x) + H(b) \rangle$. Torej je (F, G, H) izotopizem. □

Opomba 2.1. Če je (F, G, H) izotopizem, sta F in G določena s H in elementoma $G^{-1}(1)$ ter $F^{-1}(1)$.

Dokaz. Res,

$$F(a) = \langle F(a)1 + 0\rangle = \langle F(a)G(G^{-1}(1)) + H(0)\rangle = H(\langle aG^{-1}(1) + 0\rangle) \quad \text{in}$$
$$G(a) = \langle 1G(a) + 0\rangle = \langle F(F^{-1}(1))G(a) + H(0)\rangle = H(\langle F^{-1}(1)a + 0\rangle).$$

□

2.5 Veblen-Wedderburnovi sistemi

Naj bo K množica z binarnima operacijama: seštevanjem $(x, y) \mapsto x + y$ in množenjem $(x, y) \mapsto xy$, ter naj v K obstajata različna elementa 0 in 1. Če naslednje lastnosti držijo za K, potem rečemo, da je K *levi Veblen-Wedderburnov sistem* ali *levo kvazi polje*.

VW1. Množica K je Abelova grupa za seštevanje.

VW2. Za podana $a, b \neq 0$ ima vsaka izmed enačb $ax = b$ in $xa = b$ natanko eno neničelno rešitev x. Opomba: Če $a, b \neq 0$, potem $ab \neq 0$.

VW3. Za vsak $x \in K$ velja: $1x = x1 = x$, $0x = x0 = 0$, $x + 0 = 0 + x = x$.

VW4. Leva distributivnost: $a(x + y) = ax + ay$ za vse $a, x, y \in K$.

VW5. Za $a \neq a'$ ima enačba $ax = a'x + b$ enolično rešitev $x \in K$.

Prva sta to zapisala O. Veblen in J. Wedderburn leta 1907 v svojem delu [8]. Tem sistemom se je v literaturi do leta 1975 reklo Veblen-Wedderburnovi sistemi, sedaj pa se v večini literature uporablja izraz kvazi polja.

Opazimo, da je **VW5** šibka verzija desne distributivnosti. Z upoštevanjem pogojev **VW1** in **VW2** sledi **VW5** iz desne distributivnosti. Ker je K Abelova grupa za seštevanje, lahko $ax = a'x + b$ zapišemo kot $ax - a'x = b$. Če bi veljala desna distributivnost, bi bilo to isto kot $(a - a')x = b$, kjer bi po **VW2** obstajala natanko ena neničelna rešitev x.

Podobno definiramo *desni Veblen-Wedderburnov sistem* oziroma *desno kvazi polje*. Pogoja **VW4** in **VW5** zamenjamo z naslednjima pogojema:

VW4′. Desna distributivnost: $(x + y)a = xa + ya$ za vse $a, x, y \in K$.

VW5′. Za $a \neq a'$, ima enačba $xa = xa' + b$ enolično rešitev $x \in K$.

Opomba 2.2. Množica K je desno kvazi polje natanko tedaj, ko je K z istim seštevanjem, istima elementoma 0 in 1 ter obratnim množenjem $a \cdot b = ba$, levo kvazi polje.

Dokaz. Pokažimo, da to res velja.
($\Rightarrow$) Predpostavimo, da je K desno kvazi polje, v katerem veljajo aksiomi **VW1** $-$ **VW3** in **VW4'** ter **VW5'**. Ker so aksiomi **VW1** $-$ **VW3** isti za leva in desna kvazi polja, moramo pokazati, da K zadošča aksiomoma **VW4** in **VW5**. Ker je

$$(x+y)\cdot a = x\cdot a + y\cdot a = ax + ay,$$
$$(x+y)\cdot a = a(x+y),$$

vidimo, da je $a(x+y) = ax+ay$ ter **VW4** velja. Iz $x\cdot a = x\cdot a' + b$ dobimo $ax = a'x + b$, torej velja tudi **VW5** in je K z obratnim množenjem levo kvazi polje.
($\Leftarrow$) Predpostavimo sedaj, da je K levo kvazi polje z obratnim množenjem. Ker je

$$a\cdot(x+y) = a\cdot x + a\cdot y = xa + ya,$$
$$a\cdot(x+y) = (x+y)a,$$

vidimo, da je $(x+y)a = xa+ya$ in velja **VW4'**. Iz enakosti $a\cdot x = a'\cdot x + b$ dobimo $xa = xa' + b$ in velja tudi pogoj **VW5'**. Torej je K desno kvazi polje za navadno množenje. □

Če K zadošča le pogojem **VW1 - VW4**, pravimo, da je *šibko levo kvazi polje*. Podobno: K je *šibko desno kvazi polje*, če zadostuje pogojem **VW1 - VW3** in **VW4'**.

Če je K levo ali desno kvazi polje, potem lahko definiramo ternarno operacijo $(a,x,b) \mapsto \langle ax+b\rangle$ kot $\langle ax+b\rangle = ax+b$. Trdimo, da je K s to ternarno operacjo ter različnima elementoma 0 in 1, ternarni kolobar. Preverimo to najprej za leva kvazi polja.

T1: Ta pogoj sledi iz **VW3**: Hočemo, da velja $\langle 1x+0\rangle = \langle x1+0\rangle = x$. Iz $\langle 1x+0\rangle$ dobimo $1x+0 = x+0 = x$ in iz $\langle x1+0\rangle$ dobimo $x1+0 = x+0 = x$. Torej ta pogoj drži.

T2: Ta pogoj sledi iz **VW3**: Želimo, da velja $\langle a0+b\rangle = \langle 0a+b\rangle = b$. Podobno kot prej iz $\langle a0+b\rangle$ dobimo $a0+b = 0+b = b$ in iz $\langle 0a+b\rangle$ dobimo $0a+b = 0+b = b$. Tudi ta pogoj drži.

T3: Ta pogoj sledi iz **VW1**: Želimo, da za $a,x,y \in K$ obstaja enolično določen $b \in K$, da velja $\langle ax+b\rangle = y$. Ker je $\langle ax+b\rangle = ax+b$, je $ax+b = y$. To lahko zapišemo kot $y - ax = b$.

T4: Naj bodo $a, a', b, b' \in K$ in $a \neq a'$. Enačba $ax + b = a'x + b'$ za x je ekvivalentna enačbi $ax = a'x + (b' - b)$ po **VW1**. Ta ima enolično rešitev po **VW5**.

T5: Naj bodo $x, y, x', y' \in K$ in $x \neq x'$. Iz enačb $y = ax + b$ in $y' = ax' + b$ za a, b sledi

$$y - y' = ax - ax'$$

po **VW1** in

$$y - y' = a(x - x')$$

po **VW4**. Če je $y \neq y'$, ima ta enačba enolično rešitev a po **VW2**. Če poznamo a, lahko dobimo b iz ene izmed enačb $y = ax + b$ in $y' = ax' + b$. Torej je b natanko določen. Potem **T5** velja v primeru, ko je $y \neq y'$. Če pa je $y = y'$, mora biti $a = 0$ po **VW2** (ker $x - x' \neq 0$). Zato je $b = y = y'$. Torej **T5** velja tudi v primeru ko je $y = y'$.

Za desno kvazi polje K, pogoji **T1-T3** držijo iz istih razlogov kot pri levih kvazi poljih (niso odvisni od distributivnosti). Preverimo še **T4** in **T5**.

T4: Naj bodo $a, a', b, b' \in K$ in $a \neq a'$. Enačba $ax + b = a'x + b'$ za x je ekvivalentna $ax - a'x = b' - b$ po **VW1** in to je $(a - a')x = (b' - b)$ po **VW4'** (desna distributivnost). Po **VW2** ima enolično rešitev.

T5: Naj bodo $x, y, x', y' \in K$ in $x \neq x'$. Iz enačb $y = ax + b$ in $y' = ax' + b$ za a, b dobimo po **VW1**

$$ax = ax' + (y - y').$$

Ker velja $x \neq x'$, ima enačba enolično rešitev po **VW5'**. Podobno kot zgoraj: če poznamo a, lahko dobimo b iz ene izmed enačb $y = ax + b$ in $y' = ax' + b$. Torej je b enolično določen. S tem smo dokazali **T5**.

Opomba 2.3. Ko gremo iz levih kvazi polj na desna, se zamenjata vlogi aksiomov **VW4** in **VW5**.

Levo kvazi polje lahko dobimo iz pripadajočega ternarnega kolobarja: ima ista elementa 0 in 1; seštevanje in množenje sta definirana z $a + b = \langle 1a + b \rangle$ in $ab = \langle ab + 0 \rangle$. Velja tudi $1\langle ax + 0 \rangle + b = ax + 0 + b = ax + b$. Zato lahko kvazi polja smatramo kot poseben razred ternarnih kolobarjev. S kvazi poljem lahko definiramo afino ravnino. Seveda je ta ravnina lahko podana tudi eksplicitno: je množica točk iz K^2 kjer so premice podane z enačbami oblike $x = a$ in $y = ax + b$ za vsak par $(x, y) \in K^2$ ter sta a in b fiksna elementa iz K.

Trditev 2.2. *Naj bo K končno šibko levo kvazi polje. Potem je K levo kvazi polje (to pomeni: za končen K pogoj **VW5** sledi iz **VW1-VW4**).*

Dokaz. Za $a \neq a'$, naj bo preslikava $f\colon K \to K$ definirana s predpisom $f(x) = ax - a'x$. Predpostavimo, da f ni injektivna, torej obstajata različna x in y, da velja $ax - a'x = ay - a'y$. To je po **VW1** isto kot $ax - ay = a'x - a'y$ in je $a(x-y) = a'(x-y)$ po **VW4** (leva distributivnost). Ker je $a \neq a'$, pridemo v protislovje z **VW2**. Torej je f injektivna. Ker je f preslikava, ki slika iz končne množice sama vase, je bijektivna (tukaj uporabimo isti razmislek kot pri dokazu Trditve 2.1). Torej za vsak b obstaja tak enolično določen x, da velja $ax - a'x = b$. Zato **VW5** drži. □

Trditev 2.1 nam pove, da lahko za končen K, opustimo **T5** iz aksiomov ternarnih kolobarjev. Po Trditvi 2.2 lahko v tem primeru opustimo tudi **VW5** iz aksiomov za kvazi polja. Pri preverjanju **T4** za ternarni kolobar povezan s kvazi poljem zgoraj, smo se sklicevali na **VW5**. Če je kvazi polje končno in opustimo aksiom **VW5**, moramo uporabiti Trditev 2.2 in namesto **VW5** uporabimo levo distributivnost. V nekaterih primerih lahko končnost nadomestimo s končno razsežnostjo nad primernim obsegom, kot bomo videli v naslednji trditvi. Še prej pa si poglejmo, kaj je jedro šibkega kvazi polja.

Jedro poljubnega šibkega kvazi polja W je množica vseh elementov $k \in W$, da velja:

i) $(x+y)k = xk + yk$,

ii) $(xy)k = x(yk)$.

Trditev 2.3. *Naj bo K šibko levo kvazi polje in naj vsebuje podmnožico F, ki je obseg z istimi operacijami ter istima elementoma 0 in 1. Naj velja:*

$$(xy)a = x(ya), \tag{2.4}$$

$$(x+y)a = xa + ya \tag{2.5}$$

*za vsak $a \in F$ ter $x, y \in K$ (torej je F vsebovana v jedru K). Potem je K desni vektorski prostor nad F. Če je ta vektorski prostor končno razsežen, je K levo kvazi polje (torej **VW5** drži).*

Dokaz. Pokažimo najprej, da velja prvi del trditve. Po definiciji vektorskega prostora iz uvoda preverimo, če držijo lastnosti za vektorske prostore, vendar želimo, da je K desni vektorski prostor nad F, tj. pri množenju s skalarjem, množimo z desne strani.

Ker je K šibko levo kvazi polje, je grupa $(K, +)$ Abelova.

Preverimo še ostale lastnosti in upoštevajmo, da je množenje s skalarjem množenje z desne.

1. Hočemo, da velja $x(ba) = (xb)a$. Ker je $(xy)a = x(ya)$, mora veljati tudi $(xb)a = x(ba)$, saj je b tudi element K.

2. V K velja leva distributivnost, zato je $x(a + b) = xa + xb$.

3. Po trditvi velja $(x + y)a = xa + ya$, kar smo želeli pokazati.

4. Velja po **VW4**, saj je $1x = x$.

Torej je K res desni vektorski prostor nad F.

Dokažimo še drugi del. Za $a \in K$, naj bo $L_a \colon K \to K$ množenje z leve z a, torej $L_a(x) = ax$. Po **VW4** velja $L_a(x + y) = L_a(x) + L_a(y)$ za vsak $x, y \in K$. Če je $b \in F$, potem je $L_a(xb) = a(xb) = (ax)b = L_a(x)b$. Sledi, da je L_a (desna) linearna preslikava vektorskega prostora K vase.

Preveriti moramo, da ima za $a \neq a'$, enačba $L_a(x) = L_{a'}(x) + b$ enolično rešitev x. Naj bo $L = L_a - L_{a'}$. Potem je dovolj, če pokažemo, da ima enačba $L(x) = b$ enolično rešitev x. Očitno je L linearna preslikava. Če je $L(y) = 0$, potem je $ay - a'y = 0$ in $ay = a'y$. Ker je $a \neq a'$, iz pogoja **VW2** sledi, da je to mogoče le, če je $y = 0$. Vidimo, da je L linearna preslikava, torej homomorfizem, ki slika iz K sama vase in ima trivialno jedro. Ker predpostavimo, da je K končno razsežna, ima L trivialno jedro natanko tedaj, ko je L injektivna in tako izomorfizem. Iz tega sledi, da ima $L(x) = b$ enolično rešitev. S tem smo dokazali drugi del trditve. □

Levim kvazi poljem, v katerih velja tudi desna distributivnost, pravimo *polpolja*. Podobno so polpolja desna kvazi polja v katerih velja leva distributivnost.

Pri preverjanju, če je množica polpolje, je v primerih končne množice ekvivalentno, če pogoj **VW2** zamenjamo s pogojem, da je 0 edini delitelj niča ([5]).

2.6 Skoraj polja, obsegi in izomorfizmi

Če sta afini ravnini K^2 in $(K')^2$ izomorfni, v splošnem ni nujno, da sta tudi ternarna kolobarja K in K' izomorfna. Cilj tega razdelka je dokazati, da sta izomorfna, če je K' obseg.

Levo skoraj polje je levo kvazi polje z asociativnostjo množenja. Neničelni elementi levega skoraj polja tvorijo grupo za množenje. *Desno skoraj polje* definiramo podobno: desno skoraj polje je desno kvazi polje z asociativnostjo množenja. Neničelni elementi desnega skoraj polja tvorijo grupo za množenje. Ekvivalentno je, če je množica obseg ali levo in desno skoraj polje hkrati.

Pokažimo, da neničelni elementi levega skoraj polja K tvorijo grupo za množenje $K^* = K\backslash\{0\}$. Torej hočemo, da je v K^* množenje asociativno ter da za vsak $x \in K^*$ obstaja enota in inverzni element. Asociativnost velja po definiciji, obstoj enote 1 pa po **VW3**. Hočemo še, da obstaja element x^{-1}, da za vsak $x \in K^*$ velja $xx^{-1} = x^{-1}x = 1$. Po **VW2** obstajata enolično določena $x_1, x_2 \in K^*$, da velja $ax_1 = 1$ in $x_2a = 1$. Ker je množenje asociativno, velja

$$\begin{aligned} ax_1 &= x_2a, \qquad / \cdot x_1 \\ (ax_1)x_1 &= (x_2a)x_1, \\ x_1 &= x_2(ax_1), \\ x_1 &= x_2, \end{aligned}$$

zato je $x_1 = x_2 = x^{-1}$.
Pokažimo še, da je ekvivalentno, če je množica obseg ali levo in desno skoraj polje hkrati. Ker je K^* grupa za množenje, moramo preveriti samo še, če veljata v K^* desni in levi distributivnostni zakon. Ampak K^* je desno skoraj polje, zato velja desni distributivnostni zakon in hkrati levo skoraj polje, torej velja tudi levi distributivnostni zakon. Torej je K^* obseg.

Lema 2.2. *Naj bo K' levo skoraj polje. Naj bo $\mathbf{0} = (0,0) \in (K')^2$ in naj bosta l vodoravnica in m navpičnica v $(K')^2$, ki potekata skozi točko $\mathbf{0}$ (torej je $l = K' \times \{0\}$ in $m = \{0\} \times K'$). Za poljubni točki $z, z' \in (K')^2$, ki ne ležita na l in m, obstaja avtomorfizem afine ravnine $(K')^2$, ki ohranja $\mathbf{0}$, l in m, ter preslika z v z'.*

Dokaz. Dovolj je, da premislimo za primer, ko je $z = (1,1)$. Naj bo $z' = (u,v)$. Ker točka (u,v) ne leži ne na l in ne na m, sta u in v neničelna elementa. Naj bo preslikava $f\colon (K')^2 \to (K')^2$ podana z $f(x,y) = (ux, vy)$. Očitno je $f(1,1) = (u,v)$ in f preslika navpičnice $x = a$ v navpičnice $x = au$. Torej f slika tudi m v m, saj preslika navpičnico $x = 0$ v navpičnico $x = 0$. Če je $y = ax + b$, potem je $vy = v(ax) + vb = (vau^{-1})ux + vb$, zaradi leve distributivnosti in asociativnosti množenja (u^{-1} je enolična rešitev enačba $xu = 1$). Sledi, da f preslika premice oblike $y = ax + b$ v premice oblike $y = (vau^{-1})x + vb$. Ker slika premico $y = 0$ v $y = 0$, to pomeni, da ohranja l. Očitno slika tudi $\mathbf{0}$ v $\mathbf{0}$, saj je $f(0,0) = (0,0)$. Torej je f avtomorfizem $(K')^2$, ki smo ga želeli dobiti. □

Posledica 2.3. *Naj bo K ternarni kolobar in K' levo skoraj polje. Predpostavimo, da obstaja izomorfizem ravnin $f\colon K^2 \to (K')^2$, ki preslika $\mathbf{0}$ v $\mathbf{0}$ in slika vzporednico (navpičnico), ki poteka skozi $\mathbf{0} \in K^2$ v vzporednico (navpičnico), ki poteka skozi $\mathbf{0} \in (K')^2$. Potem je K izomorfen K' (v smislu ternarnega kolobarja).*

Dokaz. Če f ne slika točke $(1,1)$ v $(1,1)$, lahko vzamemo primeren avtomorfizem $g\colon (K')^2 \to (K')^2$ (ta obstaja po Lemi 2.2), da za kompozitum $h = g \circ f\colon K^2 \to (K')^2$ velja $h(1,1) = (1,1)$. Preslikava h je izomorfizem, ki slika $\mathbf{0}$ v $\mathbf{0}$, l v l, m v m in $(1,1)$ v $(1,1)$. Sedaj imamo isto situacijo kot v Definiciji 2.1, če vzamemo $\mathbb{A} = K^2$ ter $\mathbb{A}' = (K')^2$ in je K izomorfen K'. □

Lema 2.3. *Naj bo K' obseg. Naj bo $\mathbf{0} = (0,0) \in (K')^2$ in l vodoravnica, ter m navpičnica v $(K')^2$, ki potekata skozi $\mathbf{0}$ (torej $l = K' \times \{0\}$ in $m = \{0\} \times K'$). Naj bosta l' in m' poljubni nevzporedni premici v $(K')^2$. Potem obstaja avtomorfizem afine ravnine $(K')^2$, ki slika l v l' in m v m', točko $\mathbf{0}$ pa v presečišče premic l' in m'.*

Dokaz. Pokažimo najprej, da so nekatere preslikave, ki jih bomo uporabili v dokazu, izomorfizmi.

(i) Naj bo $D(x,y) = (y,x)$. Premice oblike $x = a$ preslika v premice $y = 0x + a$, ter premice oblike $y = 0x + b$ v premice $x = b$. Če je $a \neq 0$ preslika premico $y = ax + b$ (to je premica $x = a^{-1}y - a^{-1}b$, kjer je a^{-1} enolična rešitev enačbe $xa = 1$) v premico $y = a^{-1}x - a^{-1}b$. Torej je preslikava D izomorfizem. Uporabili smo levo distributivnost in asociativnost množenja.

(ii) Za vsaka $c, d \in K'$ naj bo $f(x,y) = (x + c, y + d)$. Ta preslikava premice oblike $x = a$ preslika v $x = a + c$ in premice oblike $y = ax + b$ v $y = ax - ac + b + d$. Torej je f res izomorfizem. Tu smo uporabili levo distributivnost.

(iii) Za vsak $c \in K'$ naj bo $f(x,y) = (x, y - cx)$. Premice oblike $x = a$ preslika same vase in premice oblike $y = ax + b$ v $y = (a - c)x + b$. Tu smo uporabili desno distributivnost.

(iv) Za vsak $c \in K'$ je preslikava $g(x,y) = (x - cy, y)$ izomorfizem, ker je $g = D \circ f \circ D$, kjer je $D(x,y) = (y,x)$ in $f(x,y) = (x, y - cx)$.

Sedaj lahko z uporabo izomorfizma tipa (ii) predpostavimo, da se l' in m' sekata v $\mathbf{0}$. Z uporabo izomorfizma D iz (i), pa lahko predpostavimo, da l' ni enak $m = \{0\} \times K'$, če je to potrebno, oz. če je $l' = m$. Potem je l' oblike $y = cx$. Preslikava $f(x,y) = (x, y - cx)$ tipa (iii) preslika l' v l. Torej lahko predpostavimo, da je $l' = l$ in da m' seka $l' = l$ v $\mathbf{0}$. Potem je m' oblike $x = cy$ in izomorfizem tipa (iv) preslika m' v m. Ker vsak izomorfizem tipa (iv) preslika l v l, je s tem dokaz zaključen. □

Izrek 2.5. *Naj bo K ternarni kolobar in K' obseg. Predpostavimo, da obstaja izomorfizem ravnin $f\colon K^2 \to (K')^2$. Potem je K izomorfen K' (v smislu ternarnega kolobarja).*

Dokaz. Predpostavimo, da obstaja izomorfizem $f\colon K^2 \to (K')^2$. Naj bo l vodoravnica v K skozi $\mathbf{0} \in K$, l' vodoravnica v K' skozi $\mathbf{0} \in K'$, m navpičnica v K skozi $\mathbf{0} \in K$ ter m' navpičnica v K' skozi $\mathbf{0} \in K'$. Po Posledici 2.3 je K izomorfen K', če obstaja izomorfizem $K^2 \to (K')^2$, ki slika $\mathbf{0}$ v $\mathbf{0}$, l v l' in m v m'.
Naj bosta l'' in m'' poljubni nevzporedni premici v $(K')^2$, ki se sekata v točki A. Po Lemi 2.3 obstaja avtomorfizem g afine ravnine $(K')^2$, da je $g(l') = l''$, $g(m') = m''$ in $g(A) = 0$. Kompozitum $h = g \circ f\colon K^2 \to (K')^2$ je izomorfizem, ki slika $\mathbf{0}$ v $\mathbf{0}$, l v l' in m v m'. Torej je K izmorfen K'. □

Iz tega sledi, da je za konstrukcijo afine ravnine, ki ne izhaja iz obsega, dovolj konstruirati kvazi polje, ki ni obseg. Torej je dovolj, če konstruiramo levo kvazi polje, v katerem ne velja desna distributivnost, ali pa desno kvazi polje, v katerem ne velja leva distributivnost. Kot alternativo, lahko konstruiramo (levo ali desno) kvazi polje, v katerem množenje ni asociativno. Konstrukcijo takšnega kvazi polja bomo spoznali v razdelku 2.8.

2.7 Translacije

V prejšnjem razdelku smo spoznali metodo konstrukcije afine ravnine, ki ni izomorfna afini ravnini definirani nad obsegom. V tem razdelku pa bomo spoznali drugo metodo, ki temelji na posebnih avtomorfizmih afinih ravnin, imenovanih *translacije*. Ta nam pokaže, da nekatere ravnine niso izomorfne niti ravninam definiranim z levim kvazi poljem (Izrek 2.6).

Definicija 2.2. [7, stran 31]. Naj bosta $\mathbb{A}$ in $\mathbb{A}'$ afini ravnini. Bijekcijo $\tau\colon \mathbb{A} \to \mathbb{A}'$, ki tri kolinearne točke preslika v kolinearne, imenujemo *afina transformacija*.

Definicija 2.3. [7, stran 32]. Afino transformacijo $\tau\colon \mathbb{A} \to \mathbb{A}$, za katero velja $l \parallel \tau(l)$ za vse premice l v $\mathbb{A}$, imenujemo *dilitacija*. Dilitacija, ki je identiteta $id_{\mathbb{A}}$ ali pa nima negibnih točk, se imenuje *translacija*.

Naslednja definicija translacije je ekvivalentna zgornji definiciji.

Definicija 2.4. Naj bo $\mathbb{A}$ afina ravnina. Avtomorfizmu $f\colon \mathbb{A} \to \mathbb{A}$ pravimo *translacija*, če je $f(l)$ vzporedna l za vsako premico l in če f ohranja vsako premico iz natanko določenega razreda vzporednic. Premici, ki je v tem razredu, pravimo *sled* translacije f. Ko je $\mathbb{A}$ mišljena kot K^2 za ternarni kolobar K, rečemo da je translacija *vodoravna*, če ohranja vse vodoravnice.

Pokažimo, da sta definiciji ekvivalentni. Videti želimo, da netrivialna translacija definirana v Definiciji 2.4 nima negibnih točk. Naj bo f translacija, ki ohranja točko z. Naj bo l sled translacije f. Naj bo m premica, ki vsebuje z in ni vzporedna l. Ker je $f(m)$ vzporedna m in vsebuje z, je $f(m) = m$. Vsaka točka na m je enolično določeno presečišče premice m in premice, ki je vzporedna l. Translacija f ohranja obe premici. Iz tega sledi, da f ohranja vse točke na m. Vidimo, da f ohranja vse točke, razen mogoče točk na premici l_z, ki gre skozi z in je vzporedna l. Z uporabo istega argumenta na vseh točkah, ki ne ležijo na l_z, lahko zaključimo, da f ohranja tudi točke na l_z, torej je je $f = id$.
Predpostavimo sedaj, da imamo translacijo definirano kot v Definiciji 2.3. Želimo pokazati, da ta translacija ohranja natanko določen razred vzporednic. Naj bo f translacija, ki nima negibnih točk in naj bo l premica, ki poteka skozi točki z in $f(z)$. Potem je $f(l) = l$. Naj bo l' vzporedna l in naj poteka skozi točko u. Predpostavimo, da $f(u) \notin l'$. Potem obstaja premica m, ki gre skozi u in $f(u)$ in je $f(m) = m$. Premici m in l se sekata v enolični točki, ki je negibna točka, saj translacija f ohranja m in l. Torej mora biti $f(u) \in l'$ in translacija f ohranja vse premice iz tega razreda vzporednic. Pokažimo še, da je to edini razred vzporednic, ki ga translacija f ohranja. Naj bo sedaj l' premica, ki ni vzporedna premici l. Potem se l in l' sekata v enolični točki x. Ker translacija f ohranja premico l, bo točka $f(x)$ ležala na premici l. Premica $f(l')$ bo premica, ki gre skozi točko $f(x)$ in je vzporedna premici l'. Torej $f(l') \neq l'$ in translacija f res ohranja natanko določen razred vzporednic.

Trditev 2.4. *Za poljubni točki z in z' obstaja največ ena translacija, ki preslika z v z'. Premica skozi z in z' je sled te translacije.*

Dokaz. Če sta f_1 in f_2 različni translaciji, ki preslikata z v z', potem je ${f_1}^{-1} \circ f_2$ netrivialna translacija, ki ohranja z, vendar taka translacija ne obstaja.

Naj bo sedaj f takšna translacija, da je $f(z) = z'$ in naj bo m sled translacije f. Naj bo m_z premica, ki gre skozi z in je vzporedna m. Potem je m_z tudi sled translacije f. Očitno je $z \in m_z$ in $z' = f(z) \in m_z$. Označimo z l premico skozi z in z'. Potem je $l = m_z$ in je l sled translacije f. □

Lema 2.4. *Naj bo K levo kvazi polje. Za poljubni točki (c_1, d_1), (c_2, d_2) ravnine K^2 obstaja translacija ravnine K^2, ki slika (c_1, d_1) v (c_2, d_2).*

Dokaz. V tem primeru so najbolj očitni kandidati za translacije preslikave oblike $f(x, y) = (x + c, y + d)$ za vsak $c, d \in K$. Res, če je $c = c_2 - c_1$, $d = d_2 - d_1$, potem je $f(c_1, d_1) = (c_2, d_2)$. Preverimo, da so te preslikave res translacije.

Preslikava $f(x, y) = (x + c, y + d)$ preslika premice oblike $x = a$ v premice oblike $x = a + c$, ter premice oblike $y = ax + b$ v premice oblike $y = ax - ac + b + d$.

V bistvu preslika navpičnice v navpičnice in premice z naklonom a v premice z naklonom a. (Ta primer smo imeli tudi v (ii) v dokazu Leme 2.3 v prejšnjem razdelku.) Če je $c = 0$, potem f ohranja vse navpičnice in je zato translacija. Če pa je $c \neq 0$, potem po **VW2** obstaja a, da velja $d = ec$. Ker f preslika premico $y = ex + b$ v premico $y = ex - ec + b + d$ in je $ex - ec + b + d = ex - d + b + d = ex + b$, vidimo, da f ohranja vsako premico z naklonom e. Sledi, da je f translacija tudi v tem primeru. □

Lema 2.5. *Naj bo K desno kvazi polje. Predpostavimo, da za vsak neničelen $v \in K$ ravnina K^2 vsebuje translacijo, ki preslika $\mathbf{0}$ v $(v, 0)$. Potem v K velja leva distributivnost.*

Dokaz. Naj bo f taka translacija, da je $f(0,0) = (v,0)$. Ker je premica, ki poteka skozi $(0,0)$ in $(v,0)$ vodoravnica $K \times 0$, je f vodoravna translacija. Pokažimo sedaj, da ima f pričakovano obliko $f(a,b) = (a+v,b)$. To sledi iz spodnjih štirih opazk.

1. Premica $y = x$ z naklonom 1, ki poteka skozi točko $(0,0)$ je preslikana v premico z naklonom 1, ki poteka skozi točko $(v,0)$, tj. v premico $y = x - v$.
2. Za vsak $a \in K$, preslikava f ohranja premice oblike $y = a$. Sledi, da f preslika presečišče premic $y = a$ in $y = x$ v presečišče premic $y = a$ in $y = x - v$. To pomeni, da je $f(a,a) = (a+v,a)$.
3. Navpičnica $x = a$, ki poteka skozi (a,a) se preslika v navpičnico, ki poteka skozi $(a+v,a)$, tj. v premico $x = a + v$.
4. Presečišče premic $y = b$ in $x = a$ se preslika v presečišče premic $y = b$ in $x = a + v$. Torej je $f(a,b) = (a+v,b)$.

Potem f preslika premico $y = ax$, ki poteka skozi točko $(0,0)$ v drugo premico, z naklonom a, tj. v premico oblike $y = ax - c$. Ker vsebuje $(v,0)$, je $c = av$. Torej premico $y = ax$ preslika v premico $y = ax - av$. Za vsak $u \in K$ točka (u, au) leži na premici $y = ax$ in se preslika v točko $(u+v, au)$. Zato $(u+v, au)$ leži na premici $y = ax - av$, tj. $au = a(u+v) - av$ ali $a(u+v) = au + av$.

Ker to velja za vsak $a, u, v \in K$, leva distributivnost drži. □

Izrek 2.6. *Naj bo K desno kvazi polje, v katerem leva distributivnost ne velja, in naj bo K' levo kvazi polje. Potem ravnini K^2 in $(K')^2$ nista izomorfni.*

Dokaz. Po Lemi 2.5, obstaja takšna točka $(c,d) \in K^2$, da nobena translacija ne preslika $(0,0)$ v (c,d). Zato po Lemi 2.4 ravnina K^2 ni izomorfna nobeni ravnini konstruirani iz levega kvazi polja. □

2.8 Andréjeva kvazi polja

Naj bo Γ grupa in $\mathscr{S}$ množica. Preslikavi $\mathscr{S} \times \Gamma \to \mathscr{S}$, kjer je $(s, g) \mapsto s^g$, pravimo desno delovanje grupe Γ na množici $\mathscr{S}$, če velja:

i) $s^1 = s$,

ii) $s^{gh} = (s^g)^h$ za vse $g, h \in \Gamma, s \in \mathscr{S}$.

Orbita elementa $s \in \mathscr{S}$ je množica $\{s^g : g \in \Gamma\}$. To množico večkrat označimo z $s\Gamma$. Množica $\mathscr{S}$ je disjunktna unija orbit. Če je $\mathscr{S}$ edina orbita v Γ, pravimo, da je Γ *tranzitivna* na $\mathscr{S}$.
V tem razdelku bomo konstruirali širok razred kvazi polj z manjšo spremembo množenja v polju.

Naj bo F polje in Γ njegova grupa avtomorfizmov reda n ter K množica vseh elementov, ki jih Γ ohranja. Potem je K podpolje (torej podmnožica množice F, ki je za iste operacije tudi sama polje) in je F n-razsežen vektorski prostor nad K.

Naj bo sedaj kot zgoraj F polje, Γ končna grupa avtomorfizmov $\mathrm{Aut}(F)$ in K podpolje polja F sestavljeno iz vseh elementov, ki jih Γ preslika same vase. Potem je razsežnost polja F nad podpoljem K enaka redu Γ in je zato končna. Naj bo preslikava $v\colon F^* \to F^*$ definirana z grupo Γ, tj:

$$v(x) = \prod_{g \in \Gamma} x^g.$$

Za vsak $x \in K$ je $v(x) \in K$, saj vsak $g \in \Gamma$ ohranja elemente iz K. Preslikava v je v bistvu homomorfizem iz F^* v K^*, ker je

$$v(xy) = \prod_{g \in \Gamma} (xy)^g = \prod_{g \in \Gamma} x^g \cdot \prod_{g \in \Gamma} y^g = v(x) \cdot v(y)$$

za vsaka $x, y \in F^*$ in ker za poljuben $g \in \Gamma$ velja

$$(v(x))^g = \left(\prod_{g \in \Gamma} x^g \right)^g = \prod_{g \in \Gamma} x^g = v(x).$$

Torej poljuben $g \in \Gamma$ ohranja $v(x)$ za vsak $x \in F^*$ in je $v(x) \in K^*$.

Naj bo $N = v(F^*)$. Potem naslednji primer pokaže, da v splošnem velja $N \neq K^*$, torej v ne slika F^* v cel K^* oziroma, da v ni surjektivna. Naj bo F polje kompleksnih števil in $\Gamma = \langle \gamma \rangle$, kjer je $(a + ib)^\gamma = a - ib$. Potem je K polje realnih števil in $v(a + ib) = (a + ib)(a - ib) = a^2 + b^2$. Torej je vsak element N pozitiven in $N \neq K^*$.

Naj bo sedaj ϕ poljubna preslikava iz N v grupo Γ z eno samo zahtevo: preslikava ϕ preslika enoto F^* (ta enota mora biti v N) v enoto Γ. Z združitvijo v in ϕ dobimo preslikavo $\alpha = \phi \circ v$, ki slika iz F^* v Γ. Za vsak $x \in F^*$ bomo pisali α_x namesto $\alpha(x)$, da poudarimo dejstvo, da je $\alpha(x)$ avtomorfizem v Γ.

Definirajmo sedaj sistem F_ϕ: elementi v F_ϕ so elementi iz F, seštevanje v F_ϕ je isto kot v F, množenje pa vpeljemo na sledeč način:

$$x \odot y = xy^{\alpha_x}, \quad 0 \odot y = 0 \quad \text{za vsak} \quad x, y \in F, \quad x \neq 0. \tag{2.6}$$

Dokažimo sedaj, da je F_ϕ kvazi polje. Da bi to dokazali, bomo preverili, če zadošča lastnostim **VW1** $-$ **VW5** iz prejšnjega razdelka.

VW1: Lastnost **VW1** drži, ker je F polje in je zato seštevanje v F komutativno.

VW2: Poglejmo si enačbo $x \odot y = z$, to je $xy^{\alpha_x} = z$. Če sta x in z podana, potem je $y = (x^{-1}z)^{\alpha_x^{-1}}$ enolična rešitev. Če imamo podana y in z določimo α_x tako, da uporabimo dejstvo, da je $v(x^\beta) = v(x)$ za vsak $\beta \in \Gamma$ in za vsak $x \in F$. Če je $x \odot y = z$, potem je $v(x \odot y) = v(z)$. Ampak $v(x \odot y) = v(xy^{\alpha_x}) = v(x)v(y^{\alpha_x}) = v(x)v(y) = v(z)$. Torej je $v(x) = v(zy^{-1})$ in $\alpha_x = \alpha_w$, kjer je $w = zy^{-1}$. Torej mora vsaka rešitev x zadoščati $x = zy^{-\alpha_w}$, kjer je $w = zy^{-1}$. Lahko je tudi videti, da je takšen x rešitev: $x \odot y = xy^{\alpha_x} = xy^{\alpha_w} = zy^{-\alpha_w}y^{\alpha_w} = z$. Torej lastnost **VW2** tudi drži.

VW3: Velja $\alpha_1 = 1^\alpha = \varepsilon$ (kjer je ε enota za Γ). Torej je $x \odot 1 = x1^{\alpha_x} = x$ in $1 \odot x = 1x^{\alpha_1} = x$. Množenje smo vpeljali tako, da je $0 \odot x = 0$, velja pa tudi $x \odot 0 = x \cdot 0^{\alpha_x} = 0$. Zato lastnost **VW3** drži.

VW4: Velja $x \odot (y+z) = x(y+z)^{\alpha_x} = x(y^{\alpha_x} + z^{\alpha_x}) = xy^{\alpha_x} + xz^{\alpha_x} = x \odot y + x \odot z$, zato F_ϕ zadošča levem distributivnostnem zakonu in **VW4** drži.

VW5: Če je k element iz K, potem je $x \odot k = xk^{\alpha_x} = xk$ za vsak $x \in F$ in je K vsebovan v jedru F_ϕ. Potem je F_ϕ šibko kvazi polje, ki je končno razsežno nad svojim jedrom. Po Trditvi 2.3 velja tudi lastnost **VW5**.

Torej je F_ϕ kvazi polje, ki mu pravimo *levo Andréjevo kvazi polje*. *Desna Andréjeva kvazi polja* so konstruirana na podoben način z množenjem definiranim s formulo $x \odot y = yx^{\alpha_y}$. Kot bomo videli v naslednji lemi, ni v levem Andréjevem kvazi polju množenje skoraj nikoli asociativno (Lema 2.6). Seveda odgovarjajoči rezultati, do katerih bomo prišli tekom tega razdelka, veljajo tudi za desna Andréjeva kvazi polja. Andréjevemu kvazi polju pravimo *netrivialno*, če je ϕ netrivialna preslikava.

Naslednji rezultat je iz [2, stran 7]: Naj bo p praštevilo in $q = p^n$. Potem obstaja (do izomorfizma) enolično določeno polje $GF(p)$, imenovano Galoisovo polje. To

polje je reda q in ima q elementov. Vsako končno polje je izomorfno nekemu $GF(q)$. Velja tudi:

i) Polje $GF(q)$ ima karakteristiko p. *Karakteristika* polja je najmanjše pozitivno celo število p, da velja $p \cdot x = 0$ za vsak $x \in GF(q)$.

ii) Grupa za množenje polja $GF(q)$ je ciklična.

iii) Če je $p = 2$, potem je vsak element $GF(q)$ kvadrat. Če je $p \neq 2$, potem je natanko polovica neničelnih elementov polja $GF(q)$ kvadrat.

Predpostavimo sedaj, da je polje F končno. V tem primeru je Γ ciklična grupa reda n in $K = GF(q)$ za neko potenco praštevila q ter $F = GF(q^n)$. V tem primeru je preslikava v podana z $v(x) = x^{1+q+q^2+\cdots+q^{n-1}}$. Preslikavo ϕ lahko izberemo na n^{q-2} načinov, ker ima poljuben izmed $q-2$ elementov iz K različen od 0 ali 1, poljuben element izmed n elementov iz Γ za svojo sliko. To nam pokaže velikost razredov Andéjevih kvazi polj, ki jih lahko konstruiramo z danim poljem F. Struktura F_ϕ je odvisna od izbire ϕ.

Lema 2.6. *Andréjevo kvazi polje F_ϕ je asociativno natanko tedaj, ko je ϕ antihomomorfizem iz (multiplikativne) grupe N v Γ.*

Dokaz. Dokazali bomo računsko in si pomagali z enakostjo $\alpha(xy^{\alpha_x}) = \alpha(x \odot y) = \alpha(xy)$:

$$x \odot (y \odot z) = x \odot (yz^{\alpha_y}) = x(yz^{\alpha_y})^{\alpha_x} = xy^{\alpha_x} z^{\alpha_y \alpha_x},$$
$$(x \odot y) \odot z = (xy^{\alpha_x}) \odot z = xy^{\alpha_x} z^{\alpha_{xy}}.$$

Zaradi asociativnosti F_ϕ je $\alpha_{xy} = \alpha_y \alpha_x$ in je α antihomomorfizem. Ker je v homomorfizem, mora biti ϕ antihomomorfizem. Obrat je očiten: Ker je ϕ antihomomorfizem in v homomorfizem, je α anitihomomorfizem in je $\alpha_{xy} = \alpha_y \alpha_x$. Če pa to velja, je F_ϕ asociativno. □

Posledica 2.4. *Končno Andréjevo kvazi polje je asociativno natanko tedaj, ko je ϕ homomorfizem iz $N = K^*$ v grupo Γ.*

Dokaz. Ker je F končno, je Γ ciklična in je vsak antihomomorfizem tudi homomorfizem. Potem je $N = K^*$, ker je F končen in N slika vse elemente F^* v K^*. □

Lema 2.7. *Naj bo F_ϕ Andréjevo kvazi polje. Potem so naslednje trditve ekvivalentne:*

(i) *Andréjevo kvazi polje F_ϕ je polpolje,*

(ii) *Andréjevo kvazi polje F_ϕ je polje,*

(iii) *Andréjevo kvazi polje F_ϕ je izomorfno polju F,*

(iv) *za vsak $k \in N$ je $\phi(k) = \varepsilon$, kjer je ε enota Γ.*

Dokaz. Predpostavimo, da je F_ϕ polpolje. Potem F_ϕ zadošča desnem distributivnostnem zakonu, tako da imamo za vsak $a, b, x \in F^*$

$$ax^\alpha + bx^\beta = (a+b)x^\lambda, \tag{1}$$

kjer je $\alpha = \alpha_a$, $\beta = \alpha_b$ in $\lambda = \alpha_{a+b}$. Če v (1) zamenjamo x z xy, dobimo

$$a(x^\alpha y^\alpha) + b(x^\beta y^\beta) = (a+b)(x^\lambda y^\lambda) = \left[(a+b)x^\lambda\right] y^\lambda. \tag{2}$$

Z uporabo (1), postane (2) oblike:

$$ax^\alpha y^\alpha + bx^\beta y^\beta = (ax^\alpha + bx^\beta)y^\lambda. \tag{3}$$

Če pomnožimo obe strani (3) z $(a+b)$ in uporabimo (1), kjer zamenjamo x z y, dobimo

$$(a+b)(ax^\alpha y^\alpha + bx^\beta y^\beta) = (ax^\alpha + bx^\beta)(ay^\alpha + by^\beta). \tag{4}$$

Ko zmnožimo obe strani (4) in okrajšamo z $ab \neq 0$, dobimo

$$x^\alpha y^\alpha + x^\beta y^\beta = x^\alpha y^\beta + x^\beta y^\alpha, \tag{5}$$

in to je $(x^\alpha - x^\beta)(y^\alpha - y^\beta) = 0$ za vsak $x, y \in F$. Torej je $x^\alpha = x^\beta$ za vsak $x \in F$. Iz tega sledi, da je $\alpha_a = \alpha_b$ za vsak $a, b \in F^*$. Ampak $\alpha_1 = \varepsilon$, torej je tudi $\alpha_a = \varepsilon$ za vsak $a \in F^*$. Zato iz (i) sledi (ii), (iii) in (iv). Ampak tudi iz vsakega izmed (ii), (iii), (iv) sledi (i). □

Opomba 2.4. Iz zgornje leme vidimo, da v Andréjevem kvazi polju F_ϕ velja desna distributivnost natanko tedaj, ko ϕ slika vse elemente iz N v enoto grupe Γ in je F_ϕ polje.

Opomba 2.5. Ker je v končnih primerih Γ ciklična, lahko zamenjamo ϕ s preslikavo iz K^* v $\mathbb{Z}_n$, tako da je α_x avtomorfizem $z \to \phi\left(z^{q^x}\right)$. Lemo 2.6 potem zamenjamo s trditvijo, da je ϕ homomorfizem v aditivno grupo $\mathbb{Z}_n$.

Izrek 2.7. *Naj bo $F = GF(p^n)$, kjer je p praštevilo. Potem obstaja Andréjevo kvazi polje reda p^n, ki ni polje natanko tedaj, ko je*

a) p lih in $n \geq 2$ ali

b) $p = 2$ *in* $n \geq 2$ *ni praštevilo.*

Dokaz. Naj bo K neko podpolje polja F in $K \neq F$. Naj bo m razsežnost F nad K. Potrebno je pokazati, da lahko najdemo takšno preslikavo ϕ iz K v ostanke modula m, da preslika nek element iz K, različen od 0 in 1, v neničelen element. Če je p lih in $n \geq 2$, potem izberemo $K = GF(p)$ in preslikamo -1 v 1 v $\mathbb{Z}_n$. Če je $p = 2$ in je n praštevilo, potem je $GF(2)$ edino podpolje pod F in je preslikava ϕ določena v $GF(2)$ z $\phi(1) = 0$. Torej mora biti F_ϕ polje. Pa vendar, če n ni praštevilo, obstaja polje $GF(2^s)$, pravilno vsebovano med $GF(2)$ in $GF(2^n)$. Naj bo $K = GF(2^s)$. Potem K^* vsebuje element, ki ni enota, ki ga lahko preslikamo v 1 iz $\mathbb{Z}_{n/s}$. □

Ker je asociativno kvazi polje skoraj polje, bomo asociativnim Andréjevim kvazi poljem rekli *Andréjeva skoraj polja*.

Lema 2.8. *Naj bo q potenca praštevila in $F = GF(q^2)$. Potem vedno obstaja Andréjevo skoraj polje F_ϕ, katerega jedro je $GF(q)$ in elementi iz jedra komutirajo z vsakim elementom iz F_ϕ.*

Dokaz. Naj bo Γ grupa reda 2 generirana z avtomorfizmom $\alpha\colon x \to x^q$. Potem je $K = GF(q)$. Multiplikativna grupa K^* je ciklična grupa reda $q - 1$ in natanko polovica njenih elementov so kvadrati. Za vsak $k \in K^*$ naj bo $\phi(k)$ definiran kot $\phi(k) = 0$, če je k kvadrat in $\phi(k) = 1$ sicer. Potem je ϕ homomorfizem iz K^* v aditivno grupo $\mathbb{Z}_2$ in zato mora biti F_ϕ asociativen in ne sme biti polje. Ker jedro F_ϕ ne more biti cel F_ϕ, ampak mora vsebovati $GF(q)$, mora biti točno $GF(q)$. Če je b poljuben element K^*, potem za vsak x v F velja $x \odot b = xb^{\alpha_x} = xb$. Ker je $v(b) = b^{1+q}$, kar je kvadrat v K^*, je $\phi(v(b)) = 0$ in potem $\alpha_b = 1$ in dobimo $b \odot x = bx = xb = x \odot b$, kot zahtevano. □

Primer 2.1. Poglejmo si primer, ko je $F = GF(9)$. Potem mora biti Γ grupa reda 2, generirana z $\alpha\colon x \to x^3$ in $K = GF(3)$. Andréjevo skoraj polje F_ϕ bo določeno, ko bomo določili ϕ na $GF(3)^*$. Ker je $\phi(1) = 0$, mora biti $\phi(-1) = 1$, saj je v nasprotnem primeru Andréjevo kvazi polje F_ϕ polje. Sedaj imamo isto situacijo, kot v Lemi 2.8, kar pomeni, da so edina Andréjeva kvazi polja reda 9 asociativna.

2.9 Zaključek: Nedesarguesove ravnine

Če je K levo kvazi polje z neasociativnim množenjem (torej levo Andréjevo kvazi polje), potem K ni izomorfen nobenemu obsegu. Po Izreku 2.5 ni K^2 izomorfna nobeni ravnini definirani nad obsegom in je zato nedesarguesova ravnina.

Če je K levo kvazi polje v katerem desna distributivnost ne velja, potem K ponovno ni izomorfen nobenemu obsegu. Po Izreku 2.5 je K^2 nedesarguesova ravnina.

Naj bo K desno kvazi polje v katerem leva distributivnost ne drži. Za primer lahko vzamemo za K poljubno netrivialno desno Andréjevo kvazi polje (za K lahko vzamemo tudi levo Andréjevo kvazi polje z obratnim množenjem). Potem po Izreku 2.6 ni K^2 izomorfna nobeni ravnini definirani nad kvazi poljem. V splošnem K^2 ni izomorfna nobeni ravnini definirani nad obsegom in je zato nedesarguesova ravnina.

3. Primeri nedesarguesovih projektivnih ravnin

To poglavje v glavnem sledi razlagi iz [2], še posebno iz [2, Poglavje IX].

3.1 Uvod

Projektivna ravnina $\mathscr{P}$ je množica točk in premic, ki jim pravimo elementi projektivne ravnine $\mathscr{P}$. Za točke in premice iz $\mathscr{P}$ veljajo naslednji aksiomi:

i) Poljubni različni točki ležita na enolično določeni premici.

ii) Poljubni različni premici se sekata v enolično določeni točki.

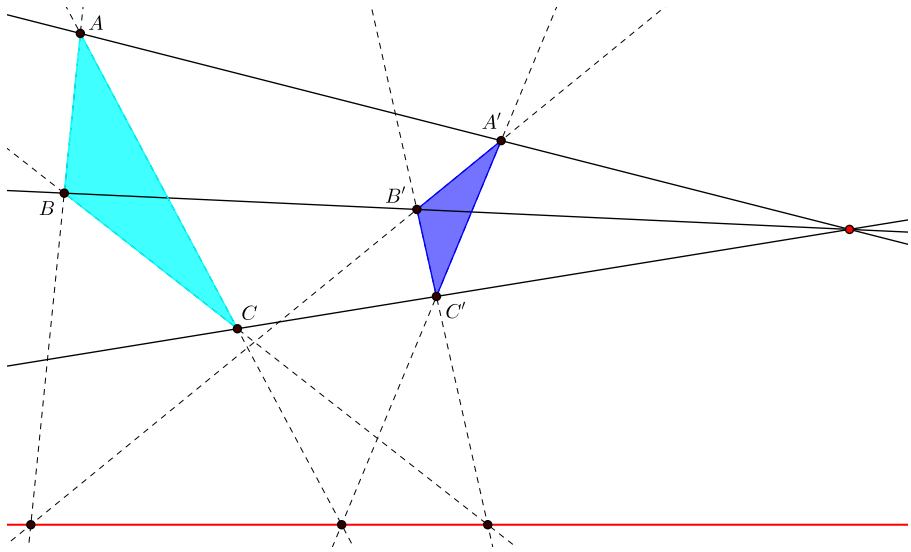
iii) Obstajajo štiri takšne točke, da nobene tri izmed njih ne ležijo na isti premici.

Nedesarguesova projektivna ravnina je taka projektivna ravnina, ki ne zadošča Desarguesovem izreku za projektivno ravnino. Naslednja definicija in izrek sta iz [7], kjer se nahaja tudi dokaz izreka.

Definicija 3.1. Trikotnika ABC in $A'B'C'$ v projektivni geometriji $\mathscr{P}$ sta v *perspektivni legi*, če se projektivne premice AA', BB' in CC' sekajo v isti točki, ki ji pravimo *center perspektivnosti*.

Izrek 3.1 (Desarguesov izrek v projektivni ravnini)**.** *Naj bo V vektorski prostor razsežnosti 3 nad poljem O. Trikotnika ABC in $A'B'C'$ v projektivni ravnini $\mathscr{P}(V)$ (to je v množici vseh vektorskih podprostorov V) sta v perspektivni legi natanko tedaj, ko presečišča nosilk stranic $X = AB \cap A'B'$, $Y = AC \cap A'C'$ in $Z = BC \cap B'C'$ ležijo na isti projektivni premici.*

V tem poglavju si bomo najprej, kot pri afinih ravninah, pogledali metodo za koordinatiziranje projektivne ravnine z ravninskimi ternarnimi kolobarji. Nato bomo podrobneje pogledali primere nekaterih nedesarguesovih projektivnih ravnin. Večina primerov so translacije ravnin, za katere bomo s pomočjo kvazi polj,



Slika 3.1: Desarguesov izrek v projektivni geometriji

ki niso obsegi, pokazali, da obstajajo. Vsako izmed podanih kvazi polj je končno razsežno nad jedrom, kar pomeni, da je potrebno dokazati le, da je šibko kvazi polje (glej Trditev 2.3). Čeprav nas v glavnem zanimajo končni primeri, večina podanih trditev velja tudi za neskončne primere.

Ob koncu poglavja bomo predstavili razred ravnin (Hughesove ravnine), ki se jih ne da koordinatizirati s ternarnimi kolobarji. Obstoj teh ravnin je zagotovljen z dejansko konstrukcijo ravnine, ne pa z vpeljavo koordinatnega sistema na ternarne kolobarje.

Izrek 3.2. *(Dokaz izreka je v [2, stran 79].) Če je $\mathscr{P}$ končna projektivna ravnina reda n, potem velja:*

i) vsaka premica vsebuje natanko $n+1$ točk,

ii) vsaka točka leži na natanko $n+1$ premicah,

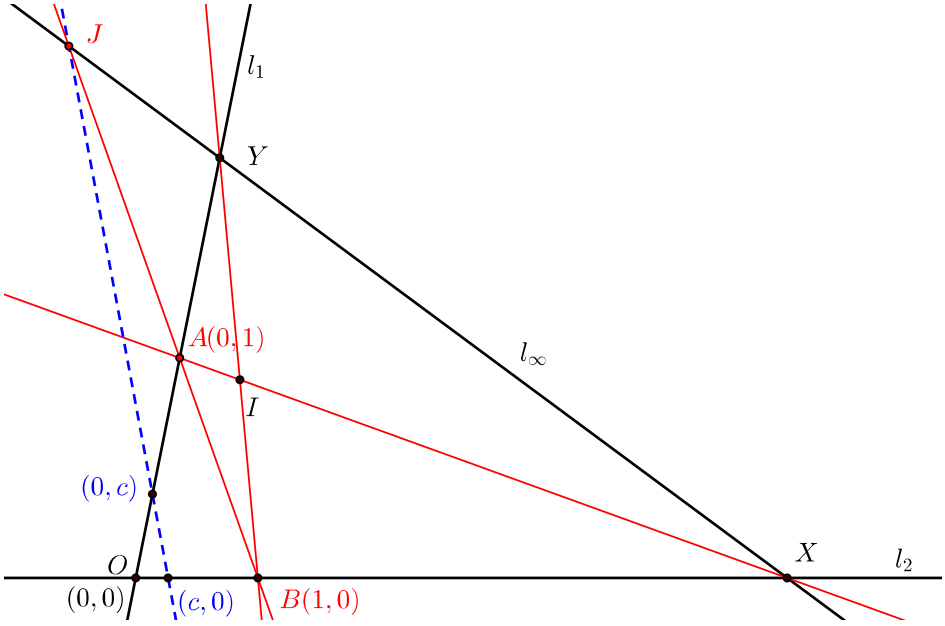
iii) ravnina $\mathscr{P}$ vsebuje n^2+n+1 točk in n^2+n+1 premic.

Kolineacija ali *avtomorfizem* projektivne ravnine je izomorfizem ravnine same vase. Množica vseh kolineacij dane ravnine $\mathscr{B}$ je grupa. To grupo označimo z $\mathrm{Aut}\,\mathscr{B}$ in ji rečemo *polna kolineacijska grupa ravnine*. $\mathscr{B}$ Ko govorimo o kolineacijski grupi ravnine $\mathscr{B}$, se nanašamo na podgrupo grupe $\mathrm{Aut}\,\mathscr{B}$.

3.2 Projektivne ravnine in ravninski ternarni kolobarji

Razdelek je povzet po [2, Poglavje V].

V tem razdelku bomo spoznali eno izmed metod za koordinatizacijo projektivne ravnine z ravninskim ternarnim kolobarjem. Naj bo $\mathscr{P}$ projektivna ravnina reda n in R takšna množica z močjo n, ki vsebuje različna elementa 0 in 1, da simbol ∞ ni v R. Izberimo poljubno premico iz $\mathscr{P}$ in jo označimo z l_∞. Izberimo še takšni premici l_1 in l_2, da l_1, l_2 in l_∞ tvorijo nosilke stranic neizrojenega trikotnika. To pomeni, da točke $X = l_2 \cap l_\infty$, $Y = l_\infty \cap l_1$ in $O = l_1 \cap l_2$ niso kolinearne. Izberimo še točko I, ki ne leži na nobeni izmed nosilk stranic trikotnika. Z uporabo elementov iz R in simbolom ∞ bomo koordinatizirali $\mathscr{P}$ s pomočjo štirikotnika $OXYI$. Definirajmo še točke $A = XI \cap l_1$, $B = YI \cap l_2$ in $J = AB \cap l_\infty$.



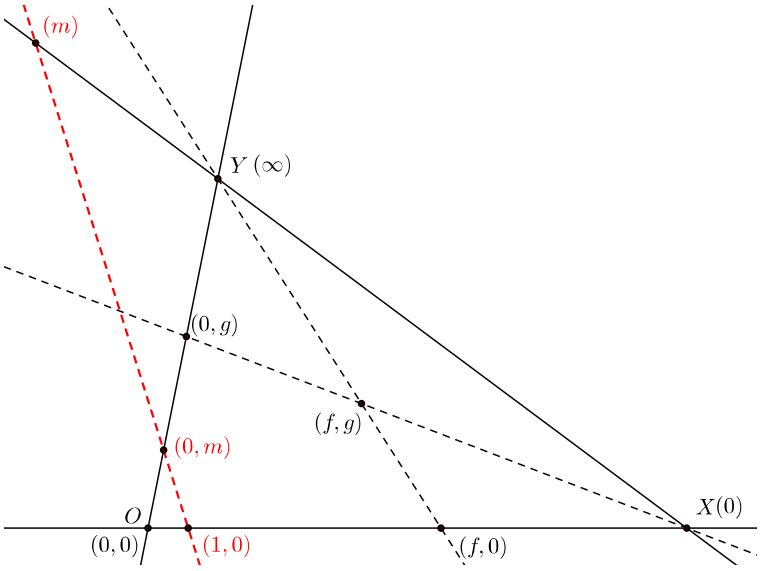
Slika 3.2: Vpeljava koordinat

Da lahko koordiniziramo $\mathscr{P}$, priredimo elementom iz R točke iz $l_1 \setminus Y$ tako, da je 0 točka O in 1 točka A. Če elementu $c \in R$ priredimo $C \in l_1$, potem pišemo $(0, c)$ za C. Za vsako od 0 različno točko D na l_2 naj bo $D' = JD \cap l_1$. Če je D' točka $(0, d)$, pišemo $(d, 0)$ za D. Za 0 pišemo O, ki ima koordinate $(0, 0)$.

Vsaki točki E, ki ne leži na l_∞, lahko določimo koordinate: če je $XE \cap l_1$ točka $(0, g)$ in $YE \cap l_2$ točka $(f, 0)$, potem ima E koordinate (f, g). Tako lahko vsaki točki, ki ne leži na l_∞, določimo enolične koordinate (x, y), kjer $x, y \in R$.

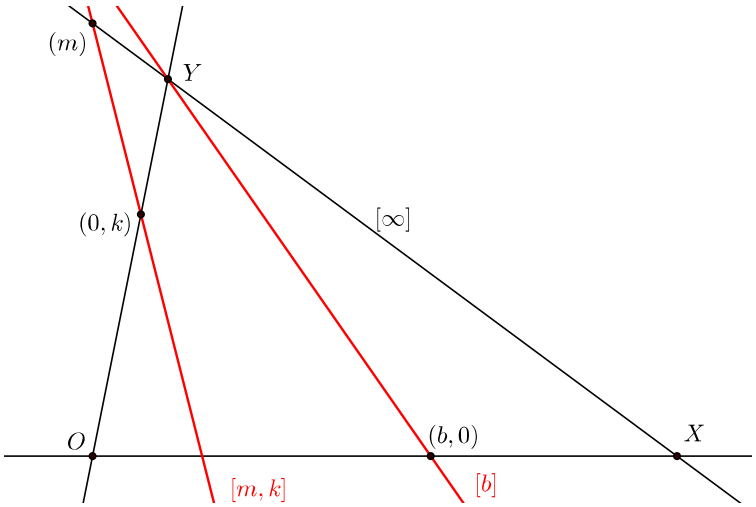
Naj bo M poljubna od Y različna točka na l_∞ in naj premica, ki povezuje M in točko $(1, 0)$ seka l_1 v točki $(0, m)$. V tem primeru bo imela točka M koordinato

(m). Koordinatizirajmo sedaj Y z (∞). Tako je vsaka točka iz $\mathscr{P}$ koordinatizirana in koordinatizacija je odvisna le od začetne izbire O, X, Y, I ter od načina, kako elemente iz R priredimo točkam na $l_1 \setminus Y$.



Slika 3.3: Grafični prikaz nekaterih točk

Koordinatizirajmo še premice z uporabo koordinatizacije točk. Naj bo l poljubna premica, ki ne vsebuje točke Y. Če l seka l_∞ v točki (m) in l_1 v točki $(0, k)$, ima l koordinate $[m, k]$. Če l vsebuje Y (torej če Y leži na l) in je različna od l_∞, potem je l premica $[k]$, kjer je k določen kot $l \cap l_2 = (k, 0)$. Namesto l_∞ bomo pisali $[\infty]$.



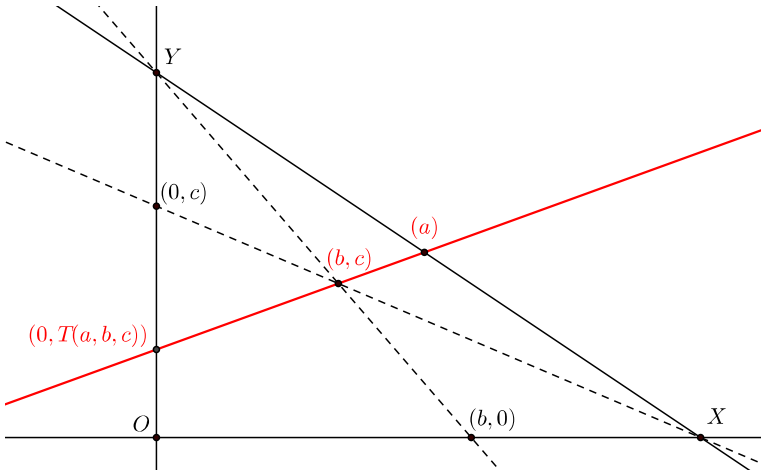
Slika 3.4: Grafični prikaz premic

S tem smo zaključili s koordinatizacijo točk in premic iz $\mathscr{P}$. Sedaj moramo v naš koordinatni sistem vgraditi še metodo za določanje razmerij med elementi.

Naj bo $\mathscr{S}$ poljubna množica. Potem je ternarna operacija T na $\mathscr{S}$ pravilo, ki trem urejenim elementom $a, b, c \in \mathscr{S}$ določi enoličen element $T(a, b, c) \in \mathscr{S}$. Neprazni množici $\mathscr{S}$ s ternarno operacijo T bomo rekli ternarni kolobar, kar bomo označili z $(\mathscr{S}, T)$.

Opomba 3.1. Algebraična struktura $(\mathscr{S}, T)$ ni enaka tisti, ki smo jo definirali v Poglavju 2, vendar jo bomo vseeno poimenovali enako.

Če je projektivna ravnina $\mathscr{P}$ koordinatizirana z elementi iz množice R kot smo opisali zgoraj, potem definiramo ternarno operacijo T na R tako: za $a, b, c \in R$ je $T(a, b, c) = k$ natanko tedaj, ko (b, c) leži na $[a, k]$. Točka $(0, k)$ je presečišče premice l_1 s premico, ki povezuje točki (a) in (b, c). Tako je vrednost k s podanimi a, b, c enolično določena (glej sliko 3.5).



Slika 3.5: Prikaz koordinatizacije s ternarnim kolobarjem T

Izrek 3.3. *Naj bo $\mathscr{P}$ projektivna ravnina koordinatizirana z množico R. Naj bo T definiran kot: $T(a, b, c) = k$ natanko tedaj, ko leži (b, c) na $[a, k]$. Potem držijo spodnje lastnosti.*

(A) Za vse $a, b, c \in R$ je $T(a, 0, c) = T(0, b, c) = c$.

(B) Za vsak $a \in R$ je $T(a, 1, 0) = T(1, a, 0) = a$.

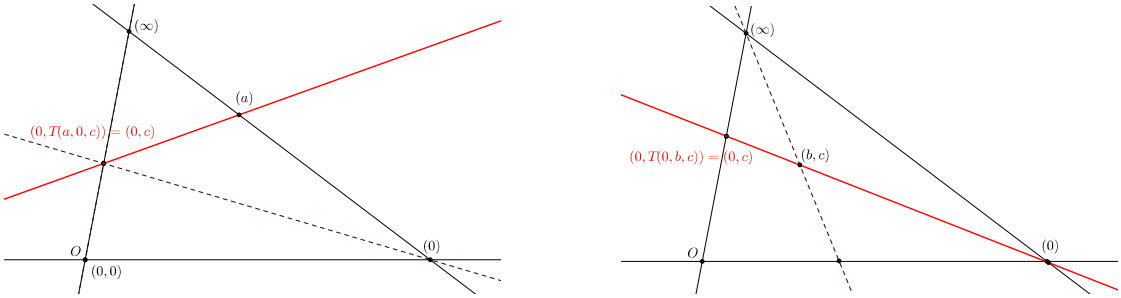
(C) Naj bodo $a, b, c, d \in R$ in $a \neq c$. Potem obstaja enolično določen $x \in R$, da je $T(x, a, b) = T(x, c, d)$.

(D) *Naj bodo $a, b, c, \in R$. Potem obstaja enolično določen $x \in R$, da je $T(a, b, x) = c$.*

(E) *Naj bodo $a, b, c, d \in R$ in $a \neq c$. Potem obstaja enolično določen par $x, y, \in R$, da je $T(a, x, y) = b$ in $T(c, x, y) = d$.*

Dokaz. (A) Iz $T(a, 0, c) = k$ sledi, da leži točka $(0, c)$ na premici $[a, k]$ (torej na premici skozi točki (a) in $(0, k)$). Ker vsaka premica seka l_1 v enolični točki, je $(0, c) = (0, k)$. Torej je $c = k$ in je $T(a, 0, c) = c$.

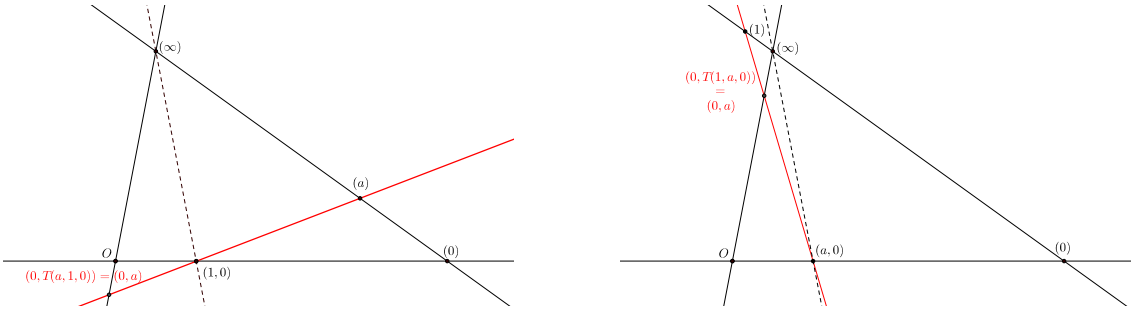
Iz $T(0, b, c) = k$ sledi, da točka (b, c) leži na premici skozi točki (0) in $(0, k)$. Ampak (b, c) je presečišče premice skozi točki (0) in $(0, c)$ ter premice skozi točki (∞) in (b, c). Ker ima premica skozi (b, c) in (0) enolično presečišče s premico l_1, je $c = k$ in $T(0, b, c) = c$.



Slika 3.6: Grafičen prikaz dokaza (A)

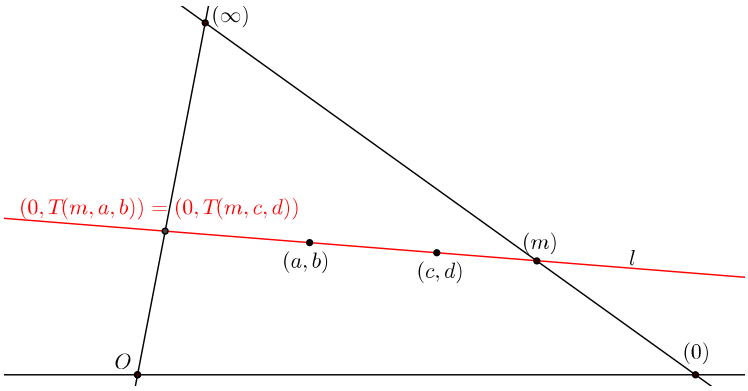
(B) Iz $T(a, 1, 0) = k$ sledi, da leži točka $(1, 0)$ na $[a, k]$. Ampak (a) je točka, kjer premica skozi točki $(1, 0)$ in $(0, a)$ seka premico l_∞. Ker premica skozi $(1, 0)$ in (a) seka premico l_1 v enolični točki, je $(0, k) = (0, a)$ in $k = a$. Torej je $T(a, 1, 0) = a$.

Iz $T(1, a, 0) = k$ sledi, da je točka $(a, 0)$ na premici skozi (1) in $(0, k)$. Ampak $(a, 0)$ je presečišče l_2 s premico skozi točki (1) in $(0, a)$. Torej je $(0, a) = (0, k)$ in $T(1, a, 0) = a$.



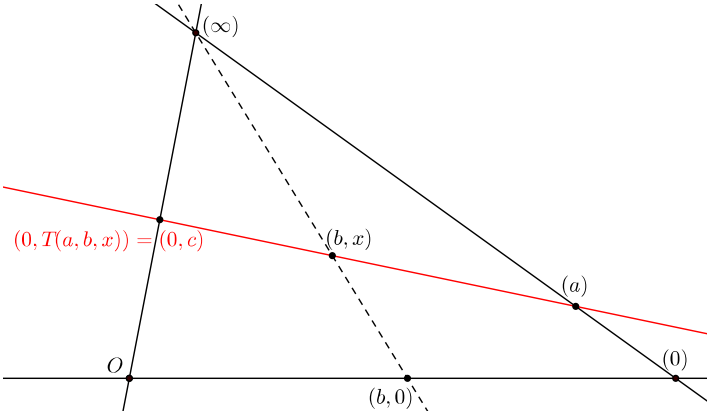
Slika 3.7: Grafičen prikaz dokaza (B)

(C) Naj velja $a, b, c, d \in R$ in $a \neq c$. Potem obstaja enolično določena premica l skozi (a, b) in (c, d). Ker je $a \neq c$, premica l ne poteka skozi (∞) in seka l_∞ v enolični točki (m), kjer je $m \in R$. Če l seka l_1 v točki $(0, k)$, je $T(m, a, b) = T(m, c, d) = k$. Ker je (m) enolično določena točka, obstaja enoličen $x \in R$, da je $T(x, a, b) = T(x, c, d)$.



Slika 3.8: Grafičen prikaz dokaza (C)

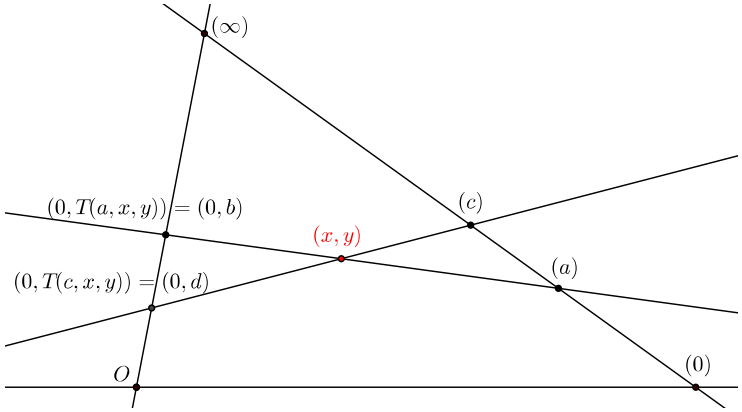
(D) Točka (b, x) leži na premici skozi (a) in $(c, 0)$ natanko tedaj, ko je $T(a, b, x) = c$. Ampak za vsak x leži točka (b, x) na premici skozi točki (∞) in $(b, 0)$. Ti premici se sekata v enolični točki in obstaja enoličen x, da je $T(a, b, x) = c$.



Slika 3.9: Grafičen prikaz dokaza (D)

(E) Točka (x, y) leži na premici $[a, b]$ natanko tedaj, ko je $T(a, x, y) = b$. Podobno leži točka (x, y) na premici $[c, d]$ natanko tedaj, ko je $T(c, x, y) = d$. Premici $[a, b]$ in $[c, d]$ se sekata v enolični točki, ki ne leži na l_∞, ker je $a \neq c$. Torej obstaja tak enolično določen par $x, y \in R$, da je $T(a, x, y) = b$ in $T(c, x, y) = d$.

□



Slika 3.10: Grafičen prikaz dokaza (E)

Poljubnemu ternarnemu kolobarju z različnima elementoma 0 in 1, ki zadošča lastnostim $(A) - (E)$ iz Izreka 3.3, pravimo *ravninski ternarni kolobar*.

Izrek 3.4. *Če je (R, T) ravninski ternarni kolobar, lahko definiramo projektivno ravnino $\mathscr{P}$ na sledeč način: Naj bodo elementi x, y, m, k iz R. Točke v $\mathscr{P}$ so urejeni pari (x, y) skupaj z elementi oblike (x) ter elementom (∞), kjer je ∞ simbol, ki ni v R. Premice so predstavljene z urejenimi pari $[m, k]$ skupaj z elementi oblike $[m]$ in elementom $[\infty]$. Incidenčna relacija je podana v spodnjih točkah.*

i) Točka (x, y) leži na premici $[m, k] \Leftrightarrow T(m, x, y) = k$.

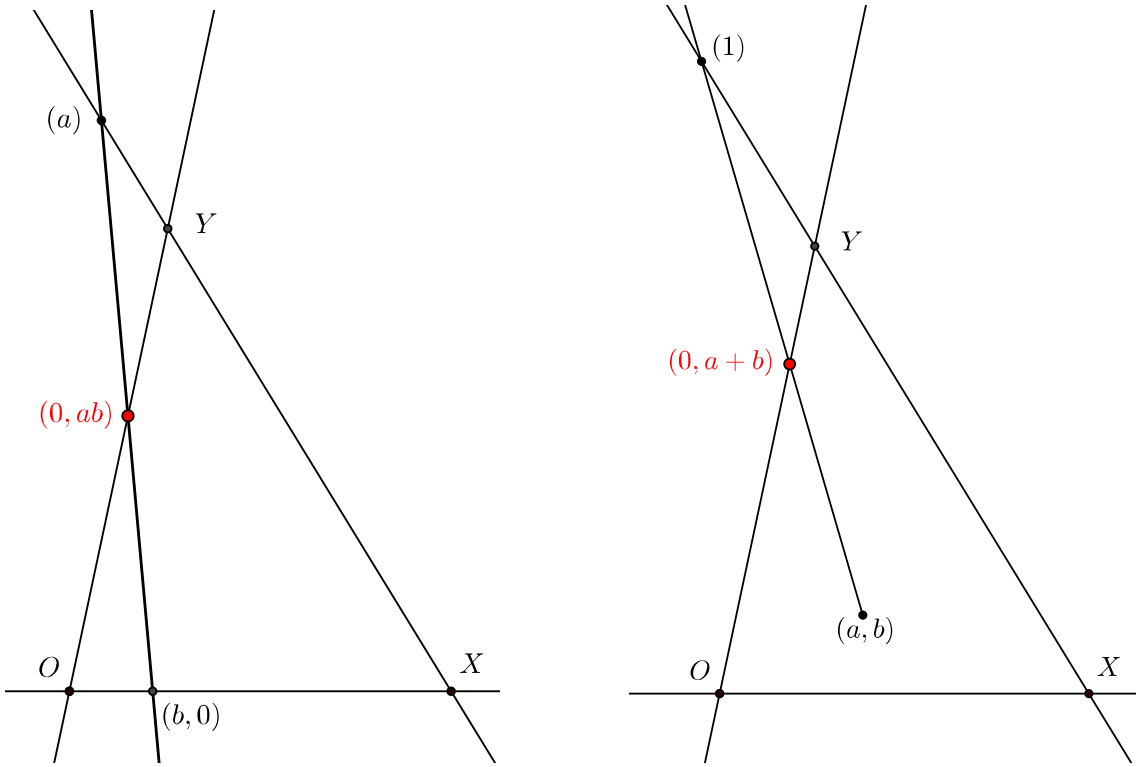
ii) Točka (x, y) leži na premici $[k] \Leftrightarrow x = k$.

iii) Točka (x) leži na premici $[m, k] \Leftrightarrow x = m$.

iv) Točka (x) leži na premici $[\infty]$ za vsak $x \in R$ in točka (∞) leži na premici $[k]$ za vsak $k \in R$. Točka (∞) leži na premici $[\infty]$.

Dokaz je v knjigi [2, Poglavje V].

Vpeljimo sedaj binarni operaciji seštevanja in množenja v ravninski ternarni kolobar (R, T) tako, da bosta $(R, +)$ in $(R^*, \cdot)$ zanki. Za vsaka $a, b \in R$ bo $a \cdot b = ab = T(a, b, 0)$ in $a + b = T(1, a, b)$. Ker je T ternarna operacija, sta ab in $a + b$ enolično določena z a in b.



Slika 3.11: Seštevanje in množenje v ravninskem ternarnem kolobarju

Vaja 3.1. Za vajo poiščimo ravninski ternarni kolobar, ki koordinatizira ravnino $\mathscr{P}(V)$, kjer je V vektorski prostor nad poljubnim obsegom K. Točke v $\mathscr{P}(V)$ so urejene trojice $(x, y, z) \neq (0, 0, 0)$, kjer so $x, y, z \in K$ in je $(x, y, z) = (kx, ky, kz)$ za $k \neq 0$. Premice so urejene trojice $[l, m, n] \neq [0, 0, 0]$, kjer so $l, m, n \in K$ in je $[l, m, n,] = [kl, km, kn]$ za $k \neq 0$. Točka (x, y, z) leži na $[l, m, n]$ natanko tedaj, ko je $lx + my + nz = 0$.

Naj bo $[\infty]$ premica $[0, 0, 1]$. Točka $(0, 1, 0)$ naj bo (∞), točka $(1, 0, 0)$ naj bo (0), točka $(0, 0, 1)$ naj bo $(0, 0)$ in točka $(1, 1, 1)$ naj bo $(1, 1)$. Elemente iz obsega K vzamemo kot elemente ravninskega ternarnega kolobarja in za poljubna $x, y \in K$ točki (x, y) priredimo točko $(x, y, 1)$.

Točka $(1, 0)$ je presečišče premice skozi $(0, 0)$ in (0) in premice skozi (∞) in $(1, 1)$. Torej je presečišče $[0, 1, 0]$ z $[-1, 0, 1]$, kar je točka $(1, 0, 1)$. Točka (1) je presečišče $[\infty]$ s premico skozi točki $(1, 0)$ in $(0, 1)$. Torej je presečišče $[0, 0, 1]$ in $[-1, -1, 1]$, kar je točka $(1, -1, 0)$. Ker je $(a, 0)$ kolinearna s točkama $(0, a)$ in (1), s podobnim razmislekom vidimo, da je $(a, 0)$ točka $(a, 0, 1)$, če predpostavimo, da je $(0, a)$ točka $(0, a, 1)$. Iz tega pa sledi, da je (a, b) točka $(a, b, 1)$. Točka (m) ima koordinate $(1, -m, 0)$.

S podobnimi argumenti vidimo, da je premica $[m, k]$ premica $[m, 1, -k]$ in $[k]$ pre-

mica $[1, 0, -k]$.

Določimo sedaj ternarno operacijo T. Naj $\oplus$ označuje seštevanje in $\odot$ množenje v (K, T). Za poljubna $a, b \in K$ je $a \oplus b = T(1, a, b)$. Ampak $T(1, a, b) = k$ natanko tedaj, ko je točka (a, b) na $[1, k]$. To pomeni da je $T(1, a, b) = k$ natanko tedaj, ko leži točka $(a, b, 1)$ na premici $[1, 1, -k]$. Iz tega sledi, da je $a + b - k = 0$, torej je $a + b = k$. Torej je seštevanje v ternarnem kolobarju (K, T) enako kot seštevanje v obsegu K.

Za poljubna $a, b \in K$ je $a \odot b = T(a, b, 0)$. Ampak $T(a, b, 0) = k$ natanko tedaj, ko je $(b, 0)$ na $[a, k]$. Torej je $T(a, b, 0) = k$ natanko tedaj, ko je točka $(b, 0, 1)$ na premici $[a, 1, -k]$. Ker iz tega sledi, da je $ab + 01 - k = 0$, je $ab = k$. Množenje v ternarnem kolobarju (K, T) je torej tudi množenje v obsegu K.

Sedaj lahko določimo $T(m, x, y)$. Točka (x, y) je na premici $[m, k]$ natanko tedaj, ko je $T(m, x, y) = k$. Torej je $T(m, x, y) = k$ natanko tedaj, ko točka $(x, y, 1)$ leži na premici $[m, -1, k]$. Iz tega sledi $mx + y - k = 0$ in je $T(m, x, y,) = k$. Torej je $T(m, x, y) = m \odot x \oplus y$.

Če je (R, T) poljuben ravninski ternarni kolobar in je $T(a, b, c) = ab + c$ za vse $a, b, c \in R$, potem pravimo, da je (R, T) *linearen ravninski ternarni kolobar*.

Definicija 3.2. (Iz [2, stran 94].) Naj bo $\mathscr{P}$ projektivna ravnina in naj bo $\alpha \neq 1$ kolineacija, ki ohranja neko premico $l \in \mathscr{P}$ glede na točke, ki ležijo na njej. Potem obstaja točka $V \in \mathscr{P}$, za katero velja, da α ohranja vse premice, ki potekajo skozi V. Kolineacija α ne ohranja nobene druge točke ali premice iz $\mathscr{P}$. Če je α takšna kolineacija, bomo rekli, da je $(V, l) -$ *perspektivnost*.

Točki V pravimo *center* perspektivnosti α, premici l pa *os* perspektivnosti.

Definicija 3.3. Ravnina je $(V, l) -$ *tranzitivna*, če za takšni točki A in B, da je $VA = VB$, $A \neq V \neq B$ in $A \notin l$ ter $B \notin l$, obstaja $(V, l) -$ perspektivnost α, da je $\alpha(A) = B$. Če je ravnina $(V, l) -$ tranzitivna za vse točke V na neki premici m, je ravnina $(m, l) -$ tranzitivna.

Naj bo l takšna premica, da je ravnina $(l, l) -$ tranzitivna. Potem rečemo premici l *translacijska premica*, projektivni ravnini pa *translacijska ravnina* glede na premico l.

Opomba 3.2. (Iz [2, Corollary 1, stran 131].) Projektivna ravnina $\mathscr{P}$ je koordinatizirana s kvazi poljem, s premico k kot $[\infty]$ natanko tedaj, ko je k translacijska premica.

3.3 Hallova kvazi polja

Naj bo F polje in $f(s) = s^2 - as - b$ nerazcepna kvadratna forma nad F. Naj bo H dvorazsežen desni vektorski prostor nad F z bazo $\{1, \lambda\}$, tako da je H sestavljen iz elementov oblike $x + \lambda y$, kjer sta x in y iz F. Definirati želimo množenje na H na tak način, da bo H kvazi polje. Predpostavimo, da:

(i) vsak element α iz H, ki ni v F (tj. ni oblike $x + \lambda 0$), je rešitev kvadratne enačbe $f(\alpha) = 0$;

(ii) polje F je v jedru kvazi polja H;

(iii) vsak element iz F komutira z vsemi elementi iz kvazi polja H.

Seštevanje v H je komutativno, tako da se vse predpostavke podobne (iii) nanašajo na množenje.

Za konstrukcijo kvazi polja H predpostavimo, da imamo kvazi polje Q, ki je takšen dvorazsežen vektorski prostor nad F, da njegovo množenje zadostuje predpostavkam (i), (ii), (iii). Potem uporabimo to pravilo, da definiramo množenje v H in pokažemo, da s tem dobimo kvazi polje z želenimi lastnostmi.

Naj bo $\{1, \lambda\}$ baza za Q kot vektorski prostor nad F. Če je $y \neq 0$, potem lahko zapišemo $(z + \lambda t)$ kot $(z + \lambda t) = (x + \lambda y)y^{-1}t + z - xy^{-1}t$ in $(x + \lambda y)(z + \lambda t) = (x + \lambda y)[(x + \lambda y)y^{-1}t + z - xy^{-1}t] = (x + \lambda y)^2 y^{-1}t + (x + \lambda y)(z - xy^{-1}t)$. Distributivnost in asociativnost veljata, ker je F vsebovan v jedru Q. Ker po predpostavki (i) velja $f(x + \lambda y) = 0$, je $(x + \lambda y)^2 = a(x + \lambda y) + b$. Torej je $(x + \lambda y)(z + \lambda t) = [b + (x + \lambda y)a]y^{-1}t + (x + \lambda y)(z - xy^{-1}t)$ ali

$$(x + \lambda y)(z + \lambda t) = xz - y^{-1}tf(x) + \lambda(yz - xt + at). \tag{3.1}$$

Z uporabo (3.1) definiramo množenje v H na sledeč način:

$$\text{Če je} \quad y \neq 0, \qquad (x + \lambda y)(z + \lambda t) = xz - y^{-1}tf(x) + \lambda(yz - xt + at). \tag{3.2}$$

$$\text{Če je} \quad y = 0, \qquad x(z + \lambda t) = xz + \lambda(xt). \tag{3.3}$$

Enačbi (3.2) in (3.3) definirata množenje za H in moramo dokazati še, da aksiomi za kvazi polje držijo.

VW1: Ker je seštevanje isto kot v F, ki je polje, je $(H, +)$ Abelova grupa.

VW2: Če želimo rešiti $(x+\lambda y)(z+\lambda t) = p+\lambda q$, kjer $(x+\lambda y) \neq 0$ za $z+\lambda t$, moramo rešiti linearni enačbi

$$\begin{aligned} xz - y^{-1}tf(x) &= p, \\ yz - xt + at &= q, \end{aligned} \tag{3.4}$$

če je $y \neq 0$ in

$$xz = p, \qquad xt = q, \qquad \text{če je} \qquad y = 0. \tag{3.5}$$

Če je $y = 0$, potem je $x \neq 0$ (ker je $x + \lambda y \neq 0$) in sta $z = x^{-1}p$ in $t = x^{-1}q$ enolično določeni rešitvi. V nasprotnem primeru, ko je $y \neq 0$, ima (3.4) enolično rešitev za z in t natanko tedaj, ko je determinanta $x(a-x) + y \cdot y^{-1}f(x)$ neničelna (Cramerjevo pravilo); ta enačba se poenostavi v $-b$, ki ne more biti 0, saj bi bila v tem primeru $f(s) = s^2 - as$ razcepna.

Potrebno je samo še rešiti $(x+\lambda y)(z+\lambda t) = p+\lambda q$ za x in y, kjer je $z+\lambda t \neq 0$. Če je $t = 0$, potem je $z \neq 0$, ker je $z + \lambda t \neq 0$, in obstaja rešitev pri $y = 0$ natanko tedaj, ko je $q = 0$. V tem primeru je rešitev $y = 0$, $x = z^{-1}p$. Podobno za $z = 0$ obstaja rešitev pri $y = 0$ natanko tedaj, ko je $p = 0$ z rešitvijo $y = 0$, $x = t^{-1}q$. Če je $t \neq 0 \neq z$, je rešitev $y = 0$, $x = pz^{-1}$ natanko tedaj, ko je $pz^{-1} = qt^{-1}$. Sedaj moramo pokazati, da ni v primerih, ko velja ali $z = 0$ in $p = 0$ ali $t = 0$ in $q = 0$ ali $pz^{-1} = qt^{-1}$, nobene rešitve pri $y \neq 0$. V kateremkoli nasprotnem primeru pa obstaja enolično določena rešitev pri $y \neq 0$.

Pomnožimo prvo enačbo iz (3.4) z y in drugo enačbo z x ter dobljeni enačbi odštejemo, da dobimo

$$bt = py - qx. \tag{3.6}$$

Če vzamemo (3.6) in drugo enačbo iz (3.4), dobimo spodnji enačbi, ki imata enaki rešitvi za x in y kot (3.4):

$$\begin{aligned} py - qx &= bt, \\ zy - tx &= q - at. \end{aligned} \tag{3.7}$$

Če je $t = 0$, potem ima (3.7) enolično rešitev $y = qz^{-1}$, $x = pz^{-1}$, kjer je $y = 0$ natanko tedaj, ko je $q = 0$. Če je $t \neq 0$, potem lahko drugo enačbo iz (3.7) pomnožimo s qt^{-1} in jo odštejemo od prve. Dobimo $y(p - qt^{-1}z) = bt - q^2t^{-1} + aq$ ali

$$y(pt - qz) = -t^2 f(qt^{-1}). \tag{3.8}$$

Ker je $t \neq 0$ in je $f(s)$ nerazcepna nad F, je desna stran enačbe (3.8) vedno neničelna. Če je $pt - qz = 0$ (tj. bodisi, ko velja $p = 0$ in $z = 0$ ali pa, ko velja $z \neq 0$ in $pz^{-1} = qt^{-1}$), potem enačba (3.4) nima rešitve pri $y \neq 0$. Sedaj vidimo, da pri pogoju $pt - qz \neq 0$ velja $y = -(t^2 f(qt^{-1}))/(pt - qz) \neq 0$, kot smo zahtevali.

VW3: Velja $(0 + \lambda 0) + (x + \lambda y) = (x + \lambda y) + (0 + \lambda 0) = (x + \lambda y)$, kjer je $0 + \lambda 0 = 0$. Vidimo, da je tudi $0(x + \lambda y) = 0$ ter $(x + \lambda y)0 = 0$. Potrebujemo še enoto za množenje: $1 = 1 + \lambda 0$. Potem velja $1(x + \lambda y) = x + \lambda y$ in $(x + \lambda y)1 = x + \lambda y$.

VW4: Hočemo, da velja leva distributivnost. Če je $y \neq 0$, je

$$\begin{aligned}
&(x + \lambda y)((z + \lambda t) + (u + \lambda v)) = (x + \lambda y)((z + u) + \lambda(t + v)) = \\
&= xz + xu - y^{-1}tf(x) - y^{-1}vf(x) + \lambda(yz + yu - xt - xv + at + av) = \\
&= xz - y^{-1}f(x)t + \lambda(yz - xt + at) + xu - y^{-1}vf(x) + \lambda(yu - xv + av) = \\
&= (x + \lambda y)(z + \lambda t) + (x + \lambda y)(u + \lambda v).
\end{aligned}$$

Če je $y = 0$, pa velja

$$\begin{aligned}
&x((z + \lambda t) + (u + \lambda v)) = x((z + u) + \lambda(t + v)) = xz + xu\lambda(xt + xv) = \\
&xz + \lambda xt + xu + \lambda xv = x(z + \lambda t) + x(u + \lambda v).
\end{aligned}$$

Torej aksiom **VW4** drži.

VW5: Do sedaj smo dokazali, da je H šibko kvazi polje. Iz definicije množenja je vidno, da je F vsebovan v jedru H. Ker je H dvorazsežen vektorski prostor nad F, iz Trditve 2.3 sledi, da je H kvazi polje.

Sistemom, ki smo jih pravkar definirali, bomo rekli *Hallova kvazi polja*. Pokažimo, da v splošnem niso polja. Če bi bil H polje, potem bi vsi njegovi elementi, ki so izven podpolja F, zadostovali isti kvadratni enačbi. Ker ima kvadratna enačba v vsakem polju največ dve ničli, bi bila kvečjemu dva elementa iz H izven F in tako bi F bil enak $GF(2)$. V primeru, ko je $F = GF(2)$, je H reda 4, vendar so vse projektivne ravnine reda 4 Desarguesove. Vsi ravninski ternarni kolobarji reda 4 so polja, zato je tudi H polje. S tem pokažemo, da je H polje natanko tedaj, ko je F enak $GF(2)$.

Lema 3.1. *Hallovo kvazi polje H je asociativno (tj. je skoraj polje) natanko tedaj, ko je bodisi $F = GF(2)$ bodisi $F = GF(3)$ in $f(s) = s^2 + 1$.*

Dokaz. ($\Rightarrow$) : Predpostavimo, da je H asociativnen. Za $x_1, x_2, y_1, y_2 \in F, y_1 \neq 0 \neq y_2$, definirajmo elementa $h_1 = x_1 + \lambda y_1$ in $h_2 = x_2 + \lambda y_2$ iz H. Izračunajmo $h_1(xh_2)$ in $(h_1x)h_2$, ter poiščimo pogoje, da bosta izraza enaka. Dobimo

$$\begin{aligned} h_1(xh_2) &= (x_1 + \lambda y_1)(xx_2 + \lambda xy_2) = \\ &= x_1xx_2 - y_1^{-1}xy_2f(x_1) + \lambda(y_1xx_2 - x_1xy_2 + axy_2) = \\ &= x_1xx_2 - y_1^{-1}y_2x(x_1^2 - ax_1 - b) + \lambda(y_1xx_2 - x_1xy_2 + axy_2) \end{aligned}$$

in

$$\begin{aligned} (h_1x)h_2 &= (x_1x + \lambda y_1x)(x_2 + \lambda y_2) = \\ &= x_1xx_2 - y_1^{-1}x^{-1}y_2f(x_1x) + \lambda(y_1xx_2 - x_1xy_2 + ay_2) = \\ &= x_1xx_2 - y_1^{-1}y_2x^{-1}(x_1^2x^2 - ax_1x - b) + \lambda(y_1xx_2 - x_1xy_2 + ay_2). \end{aligned}$$

Ker je H asociativen, je $h_1(xh_2) = (h_1x)h_2$ za vsak $x \in F$ in po zgornjih izrazih velja

$$bx = bx^{-1} \qquad \text{za vsak } x \in F,\ x \neq 0, \tag{3.9}$$

$$ax = a \qquad \text{za vsak } x \in F,\ x \neq 0. \tag{3.10}$$

Če je $x \neq 1$, potem iz (3.10) sledi $a = 0$. Ker b ne more biti 0 (v tem primeru bi bila $f(s)$ razcepna), mora za vsak $x \in F$, $x \neq 0$, veljati $x^2 = 1$. V $GF(2)$ ne obstaja element $x \neq 0, 1$, zato iz tega ne moremo ugotoviti nič drugega razen tega, da je $F = GF(2)$ možnost (zgoraj smo tudi videli, da dejansko deluje). Vendar, če v F obstaja element x, različen od 0 in 1, potem je $a = 0$ in morajo vsi elementi $x \in F$, $x \neq 0$, zadostovati $x^2 = 1$. Edino polje s temi lastnostmi je $GF(3)$ in edina nerazcepna kvadratna enačba nad $GF(3)$ pri $a = 0$ je $s^2 + 1$.

($\Leftarrow$) : Videli smo, da je H polje, ko je $F = GF(2)$. Če je $F = GF(3)$ in $f(s) = s^2 + 1$, lahko (3.1) poenostavimo do

$$(x + \lambda y)(z + \lambda t) = xz - yt(x^2 + 1) + \lambda(yz - xt), \tag{3.11}$$

ker je $x^{-1} = x$ za vsak $x \neq 0$. Hočemo pokazati še, da je množenje v H asociativno, torej da velja

$$\begin{aligned} bx &= bx^{-1} && \text{za vsak} && x \in F, && x \neq 0, \\ ax &= a && \text{za vsak} && x \in F, && x \neq 0. \end{aligned}$$

Ker je $f(s) = s^2 + 1$, je $a = 0$. Zato je $ax = x$, saj je $0 = 0$. Ker je $x^{-1} = x$, prav tako velja $bx = bx^{-1}$. Torej je H asociativnen.

□

Ko smo definirali Hallovo kvazi polje H nad poljem F, smo iz H naredili dvorazsežen vektorski prostor nad F na tak način, da je bil F vsebovan v jedru K. Vendar je hkrati H vektorski prostor nad K, zato velja ali $H = K$ ali $K = F$. Ker je $H = K$ natanko tedaj, ko je H polje (tj. H je reda 4) ima Hallovo kvazi polje z redom večjim od 4 nad svojim jedrom razsežnost 2. Ko smo definirali Hallovo kvazi polje, smo zahtevali, da vsak element F komutira z vsemi elementi H. Z naslednjim izrekom, bomo pokazali, da je ta pogoj odvečen.

Izrek 3.5. *Naj bo Q kvazi polje razsežnosti 2 nad svojim jedrom K. Če je grupa avtomorfizmov Q, ki preslika vsak element iz K samega vase, tranzitivna na elementih, ki niso v K, potem vsak element jedra K komutira z vsemi elementi iz Q.*

Dokaz. Naj bo λ izbran element iz Q, ki ni v K. Potem je $\{1, \lambda\}$ baza za Q nad K, tako da je vsak element oblike $a + \lambda b$ za neka $a, b \in K$. Naj bo $k \in K$. Potem je $k\lambda = a_1 + \lambda b_1$ za neka $a_1, b_1 \in K$. Ampak za $c, d \in K$, $d \neq 0$, obstaja element α iz $\mathrm{Aut}_K Q$ (to je grupa avtomorfizmov Q, ki ohranja vsak element iz K), da je $\lambda^\alpha = c + \lambda d$. Ker α ohranja vsak element iz K, je $(k\lambda)^\alpha = k^\alpha \lambda^\alpha = k\lambda^\alpha$. Potem je

$$\begin{aligned}(a_1 + \lambda b_1)^\alpha &= k(c + \lambda d),\\ a_1 + (c + \lambda d)b_1 &= kc + k \cdot \lambda d,\\ a_1 + cb_1 + \lambda \cdot db_1 &= kc + k\lambda \cdot d\\ &= kc + a_1 d + \lambda \cdot b_1 d.\end{aligned}$$

Za vsak $c, d \in K$, $d \neq 0$, je $a_1 + cb_1 = a_1 d + kc$ in $db_1 = b_1 d$. Če je $c = 0$, je $a_1 = a_1 d$ in je bodisi $a_1 = 0$ bodisi $d = 1$. Ampak, če je $d = 1$ edini element v K^*, je $K = GF(2)$ in mora Q imeti 4 elemente in biti enak $GF(4)$, vendar pridemo do protislovja, ker je v tem primeru Q svoje lastno jedro. Torej mora biti $a_1 = 0$. Potem je $cb_1 = kc$ za vsak $c \in K$ in $db_1 = b_1 d$ za vsak $d \in K^*$. Če je $c = 1$, potem pri $b_1 = k$ vidimo, da k komutira z vsemi elementi iz K, torej je K polje. Ker imamo $a_1 = 0$ in $b_1 = k$, $k\lambda = a_1 + \lambda b_1 = \lambda k$. □

Posledica 3.1. *Naj bo Q dvorazsežno kvazi polje nad svojim jedrom K. Potem je Q Hallovo kvazi polje natanko tedaj, ko je $\mathrm{Aut}_K Q$ tranzitivna na elementih iz Q, ki niso v K.*

Projektivnim ravninam koordinatiziranim s Hallovimi kvazi polji bomo rekli *Hallove ravnine*. Te so (kot smo pravkar pokazali) nedesarguesove, če imajo red večji od 4. Prvi primer takšne ravnine sta podala Veblen in Wedderburn z ravnino koordinatizirano s skoraj poljem reda 9.

3.4 Razredi polpolj

Med vsemi poznanimi razredi polpolj bomo podrobneje spoznali enega, ki vključuje veliko zanimivih posebnosti.

Center obsega M je množica elementov, ki komutirajo z vsakim drugim elementom: $Z(M) = \{c \in M \mid cx = xc \text{ za vsak } x \in M\}$. Naj bo obseg F končno razsežen vektorski prostor nad svojim centrom Z (torej je Z polje). Naj bo θ antiavtomorfizem obsega F s končnim redom m, da je xx^θ v Z za vsak $x \in F$. Denimo, da obstajata takšna elementa a, b iz F, da

$$a = x^{1+\theta} + xb \tag{1}$$

nima rešitve za $x \in F$.

Opomba 3.3. Če je $xx^\theta = y$, potem je (ker je $y \in Z$) $x^\theta = x^{-1}y = yx^{-1}$, tako da je $xx^\theta = y = x^\theta x$. Zato lahko pišemo $x^{1+\theta}$ ali $x^{\theta+1}$ namesto xx^θ.

Opomba 3.4. Opazimo, da je a neničelen, saj bi bil v nasprotnem primeru $x = 0$ rešitev enačbe (1).

Naj bo sedaj D dvorazsežen vektorski prostor nad obsegom F z bazo $\{1, \lambda\}$. Množenje na D bomo definirali tako, da bo D postal polpolje. Pravilo za množenje je

$$(x + \lambda y)(z + \lambda t) = (xz + aty^\theta) + \lambda(zy + x^\theta t + y^\theta bt). \tag{2}$$

Izrek 3.6. *Vektorski prostor D je polpolje.*

Dokaz. Potrebno je preveriti, da je D kvazi polje, kjer velja tudi desna distributivnost. Za kvazi polje je treba preveriti, če zadošča lastnostim **VW1**$-$**VW5**. Vendar pogoj **VW5** sledi iz pogojev **VW1** in **VW2**, če velja desna distributivnost (v razdelku 2.5 smo pokazali, da to velja), zato nam ne bo potrebno preverjati lastnosti **VW5**, če bomo pokazali, da velja desna distributivnost.

Poglejmo najprej obe distributivnosti. S tem bomo pokazali tudi, da lastnost **VW4** drži (leva distributivnost). Ker je

$$\begin{aligned}
&(x + \lambda y)((z_1 + \lambda t_1) + (z_2 + \lambda t_2)) = (x + \lambda y)(z_1 + z_2 + \lambda(t_1 + t_2)) = \\
&\quad = x(z_1 + z_2) + a(t_1 + t_2)y^\theta + \lambda((z_1 + z_2)y + x^\theta(t_1 + t_2) + y^\theta b(t_1 + t_2)) = \\
&\quad = xz_1 + xz_2 + at_1y^\theta + at_2y^\theta + \lambda(z_1y + x^\theta t_1 + y^\theta bt_1) + \lambda(z_2y + x^\theta t_2 + y^\theta bt_2) = \\
&\quad = (x + \lambda y)(z_1 + \lambda t_1) + (x + \lambda y)(z_2 + \lambda t_2)
\end{aligned}$$

vidimo, da velja desna distributivnost. Iz

$$\begin{aligned}((z_1+\lambda t_1)+(z_2+\lambda t_2))(x+\lambda y) &= (z_1+z_2+\lambda(t_1+t_2))(x+\lambda y) = \\ &= (z_1+z_2)x + ay(t_1+t_2)^\theta + \lambda(x(t_1+t_2)+(z_1+z_2)^\theta y + (t_1+t_2)^\theta by = \\ &= z_1x + z_2x + ayt_2^\theta + ayt_1^\theta + \lambda(xt_1+xt_2+z_2^\theta y + z_1^\theta y + t_2^\theta by + t_1^\theta by) = \\ &= (z_1+\lambda t_1)(x+\lambda y) + (z_2+\lambda t_2)(x+\lambda y)\end{aligned}$$

vidimo, da velja leva distributivnost. Torej D zadošča obema distributivnostnima zakonoma.

Ker ima θ red m kot antiavtomorfizem F in ker mora θ ohranjati Z, mora njen red, kot avtomorfizem Z, deliti m. Če je K podpolje polja Z, sestavljeno iz elementov, ki jih θ ohranja, je Z končno razsežen nad K. Zato je F prav tako končno razsežen nad K. Naj bo ta razsežnost k. Potem je vektorski prostor D razsežnosti $2k$ nad K in je K vsebovan v centru polpolja D. Ker je D končno razsežen nad poljem K, je za dokaz, da ima $(x+\lambda y)(z+\lambda t) = p+\lambda q$ enolično rešitev za enega izmed faktorjev na levi, če sta drugi faktor in $p+\lambda q$ podana, potrebno pokazati, da sta edini rešitvi za $(x+\lambda y)(z+\lambda t) = 0 (= 0+\lambda 0)$ le $x+\lambda y = 0$ ali $z+\lambda t = 0$. Poglejmo zakaj: Če je D končno razsežen vektorski prostor nad poljem K trdimo, da sta naslednji trditvi ekvivalentni za vsak $u \in D$.

1. Element $u \in D$ ni levi delitelj niča (torej ne obstaja $v \in D \setminus \{0\}$, da je $uv = 0$).
2. Za vsak $y \in D$ obstaja enoličen $x \in D$, da je $xu = y$.

Naj bo $\mu_u \colon D \to D$, $x \mapsto ux$. Pokažimo, da je to linearni endomorfizem vektorskega prostora D. Zaradi distributivnosti množenja velja $\mu_u(x+y) = u(x+y) = ux+uy = \mu_u(x)+\mu_u(y)$. Poglejmo še, če velja $\alpha\mu_u(x) = \mu_u(\alpha x)$ za vsak $\alpha \in K$, kjer je $u = (u_1+\lambda u_2)$ in $x = (x_1+\lambda x_2)$ ter θ ohranja vsak element iz K:

$$\alpha\mu_u(x) = \alpha(ux) = \alpha((u_1+\lambda u_2)(x_1+\lambda x_2)) = \alpha(u_1x_1 + ax_2u_2^\theta + \lambda(x_1u_2 + u_1^\theta x_2 + \\ + u_2^\theta bx_2)) = \alpha u_1x_1 + \alpha ax_2u_2^\theta + \lambda(\alpha x_1u_2 + \alpha u_1^\theta x_2 + \alpha u_2^\theta bx_2),$$

$$\mu_u(\alpha x) = u(\alpha x) = u(\alpha(x_1+\lambda x_2)) = (u_1+\lambda u_2)(\alpha x_1 + \lambda\alpha x_2) = u_1\alpha x_1 + a\alpha x_2u_2^\theta + \\ + \lambda(\alpha x_1u_2 + u_1^\theta \alpha x_2 + u_2^\theta b\alpha x_2).$$

Vidimo, da sta izraza enaka in je μ_u res linearni endomorfizem vektorskega prostora D. Ker je D končno dimenzionalen nad poljem K, je μ_u injektivna natanko tedaj, ko je surjektivna. Prva trditev drži natako tedaj, ko je μ_u injektivna, druga pa natanko tedaj, ko je μ_u surjektivna. Torej sta trditvi res ekvivalentni in lahko v dokazu preverimo le, da sta levi in desni delitelj niča enaka 0.

Če postavimo desno stran (2) na 0, dobimo:

$$\begin{aligned} xz + aty^\theta &= 0, \\ zy + x^\theta t + y^\theta bt &= 0. \end{aligned} \tag{3}$$

Če pomnožimo prvo izmed enačb v (3) z desne z y in drugo enačbo z leve z x in odštejemo, dobimo

$$aty^{1+\theta} - x^{1+\theta}t - xy^\theta bt = 0. \tag{4}$$

Če je $t = 0$, iz enačb iz (3) dobimo $xz = zy = 0$, kar pomeni, da je bodisi $x = y = 0$ bodisi $z = 0$. Torej lahko predpostavimo, da je $t \neq 0$ in potem, ker je $y^{1+\theta} \in Z$, iz (4) dobimo

$$ay^{1+\theta} - x^{1+\theta} - xy^\theta b = 0. \tag{5}$$

Če je $y = 0$, potem iz (5) sledi, da je $x = 0$. Predpostavimo torej, da je $y \neq 0$. Naj bo $x = x_1 y$, tako da je $x^\theta = y^\theta x_1^\theta$. Potem je $x^{1+\theta} = x_1 y^{1+\theta} x_1^\theta = x_1^{1+\theta} y^{1+\theta}$, ker je $y^{1+\theta} \in Z$. Potem iz (5) dobimo $ay^{1+\theta} - x_1^{1+\theta} y^{1+\theta} - x_1 y^{1+\theta} b = 0$ ali

$$(a - x_1^{1+\theta} - x_1 b) y^{1+\theta} = 0. \tag{6}$$

Prvi faktor v (6) mora biti neničelen po pogoju (1) in je zato $y^{1+\theta} = 0$ edina rešitev. Ampak iz tega sledi $y = 0$ in potem še $x = 0$ iz (5). Torej pogoj **VW2** velja.

Pokažimo še, da velja tudi lastnost **VW3**. Enota za D je $1 = 1 + \lambda 0$, saj je $(1 + \lambda 0)(z + \lambda t) = 1z + \lambda 1^\theta t = z + \lambda t$ in $(z + \lambda t)(1 + \lambda 0) = z1 + \lambda 1t = z + \lambda t$.

Velja tudi $(0 + \lambda 0) + (x + \lambda y) = x + \lambda y = (x + \lambda y) + (0 + \lambda 0)$. S tem smo dokazali, da je D polpolje. □

Poglejmo si nekaj posebnih primerov in pokažimo, da držijo.

a) Naj bo F polje realnih števil. Določimo $\theta = 1$, $a = -1$, $b = 0$. V tem primeru je D izomorfen množici kompleksnih števil.

   Pokažimo, da je to res. Naj bodo $x, y, z, t \in F$. Potem je $(x + iy)(z + it) = (xz - yt) + i(xt + yz)$. Ker je $(x + \lambda y)(z + \lambda t) = (xz - ty^\theta) + \lambda(zy + xt) = (xz - ty) + \lambda(zy + xt)$, vidimo, da je D izomorfen množici kompleksnih števil, saj je F komutativen.

b) Naj bo F polje kompleksnih števil in izberimo $a = -1$, $b = 0$ in tako preslikavo θ, da je $(x + iy)^\theta = x - iy$. Potem je D obseg kvaternionov, ki ni polje.

   Poglejmo, da to velja. Če sta h_1 in h_2 kvaterniona, naj bo $h_1 = a + bi + cj + dk$ in $h_2 = e + fi + gj + hk$. Hočemo, da je produkt $(z_1 + \lambda z_2)(z_3 +$

$\lambda z_4) = (z_1 z_3 - z_4 z_2^\theta) + \lambda(z_3 z_2 + z_1^\theta z_4)$, kjer so $z_1, z_2, z_3, z_4 \in F$ enak produktu kvaternionov $h_1 h_2$. Torej $h_1 = z_1 + \lambda z_2$ in $h_2 = z_3 + \lambda z_4$.

Iz $z_1 + \lambda z_2 = a + bi + cj + dk = a + bi + j(c - di)$ vidimo, da lahko vzamemo $z_1 = a + bi$ in $z_2 = c - di$. Podobno iz $z_3 + \lambda z_4 = e + fi + gj + hk = e + fi + j(g - hi)$ sledi, da je $z_3 = e + fi$ in $z_4 = g - hi$. Preverimo, če to ustreza:

$$\begin{aligned}
&h_1 h_2 = (a + ib + jc + kd)(e + if + jg + kh) = \\
&= ae + iaf + jag + kah + ibe - bf + kbg - jbh + jce - kcf - cg + ich + \\
&+ kde + jdf - idg - dh = \\
&= ae - bf - cg - dh + i(af + be + ch - dg) + j(ag - bh + ce + df) + \\
&+ k(ah + bg - cf + de) = \\
&= ae - bf - cg - dh + i(af + be + ch - dg) + j(ag - bh + ce + df + \\
&+ i(-ah - bg + cf - de)).
\end{aligned}$$

Poglejmo še produkt $(z_1 + \lambda z_2)(z_3 + \lambda z_4)$:

$$\begin{aligned}
&(a + bi + j(c - di))(e + fi + j(g - hi)) = \\
&= ((a + bi)(e + fi) - (g - hi)(c - di)^\theta) + j((e + fi)(c - di) + \\
&+ (a + bi)^\theta (g - hi) = (ae - bf + i(af + be) - (g - hi)(c + di)) + \\
&+ j((e + fi)(c - di) + (a - bi)(g - hi)) = ae - bf - gc - dh + \\
&+ i(af + be - gd + hc) + j(ag - bh + ec + fd + i(fc - ed - ah - bg).
\end{aligned}$$

Torej je D res obseg kvaternionov.

c) Naj bo F obseg kvaternionov. Naj bo $a = -1$, $b = 0$, preslikava θ pa naj bo kot zgoraj antiavtomorfizem definiran na kvaternionih kot $(x + iy + jz + kt)^\theta = x - ij - jz - kt$. Potem je D neasociativno polpolje, ki mu pravimo *Cayley-Dicsonova algebra*.

Pokažimo, da je ta preslikava antiavtomorfizem (tj. velja $(h_1 h_2)^\theta = h_2^\theta h_1^\theta$ za vsaka $h_1, h_2 \in \mathbb{H}$) in da je $(x + iy + jz + kt)^{1+\theta}$ realno število.

Če je $h_1 = a + ib + jc + kd$ in $h_2 = e + if + jg + kh$, je

$$\begin{aligned}
&(h_1 h_2)^\theta = ((a + ib + jc + kd)(e + if + jg + kh))^\theta = \\
&= (ae + iaf + jag + kah + ibe - bf + kbg - jbh + jce - kcf - cg + ich + \\
&+ kde + jdf - idg - dh)^\theta = \\
&= ((ae - bf - cg - dh + i(af + be + ch - dg) + j(ag - bh + ce + df) + \\
&+ k(ah + bg - cf + de))^\theta = \\
&= ae - bf - cg - dh - i(af + be + ch - dg) - j(ag - bh + ce + df) - \\
&- k(ah + bg - cf + de).
\end{aligned}$$

Poglejmo si še produkt $h_2^\theta h_1^\theta$:

$$\begin{aligned}
&(e+if+jg+kh)^\theta(a+ib+jc+kd)^\theta = \\
&= (e-if-jg-kh)(a-ib-jc-kd) = \\
&= ea-ieb-jec-ked-ifa-fb+kfc-jfd-jag-kgb-gc+igd- \\
&-kha+jhb-ihc-hd = \\
&= ea-fb-gc-hd+i(-eb-fa+gd-hc)+j(-ec-fd-ag+hb)+ \\
&+k(-ed+fc-gb-ha) = \\
&= ea-fb-gc-hd-i(eb+fa-gd+hc)-j(ec+fd+ag-hb)- \\
&-k(de-fc+gb+ha).
\end{aligned}$$

Torej je preslikava θ res antiavtomorfizem. Pokažimo še, da je $(x+iy+jz+kt)^{1+\theta} \in \mathbb{R}$:

$$\begin{aligned}
&(x+iy+jz+kt)^{1+\theta} = (x+iy+jz+kt)(x+iy+jz+kt)^\theta = \\
&= (x+iy+jz+kt)(x-iy-jz-kt) = \\
&= x^2-ixy-jxz-kxt+iyx+y^2-kyz+jyt+jzx+kzy+z^2-izt+ \\
&+ktx-jty+itz+t^2 = x^2+y^2+z^2+t^2.
\end{aligned}$$

Ker so x, y, z, t realna števila, je tudi $(x+iy+jz+kt)^{1+\theta}$ realno število.

Sedaj pridemo do primerov, ki so najbolj zanimivi za študijo končnih projektivnih ravnin. Če je F končen, potem je polje in posledično je θ avtomorfizem. S tem dobi obseg D nekaj dodatnih lastnosti, ki jih bomo sedaj preučili.

V poljubnem kvazi polju Q je *asociator* $[r,s,t]$ treh elementov r,s,t iz Q definiran kot $[r,s,t] = (rs)t - r(st)$. Če je F polje in izračunamo asociator v D, z nekaj računanja dobimo

$$\begin{aligned}
[x+\lambda y, z+\lambda t, h+\lambda k] = at^\theta k((x^{\theta^2}-x)+(b^\theta y^{\theta^2}-by^\theta)) \\
+\lambda t^\theta k((a^\theta y^{\theta^2}-ay)+b(x^{\theta^2}-x^\theta)+b(b^\theta y^{\theta^2}-by^\theta)).
\end{aligned} \tag{7}$$

Desno asociativnostno jedro N_r polpolja D je množica vseh elementov $d \in D$, da velja $(xy)d = x(yd)$ za vsak $x, y \in D$. *Levo asociativnostno jedro* N_l je podobno množica vseh elementov $d \in D$, da velja $d(xy) = (dx)y$ za vsak $x, y \in D$. *Srednje asociativnostno jedro* N_m je množica vseh elementov $d \in D$, da velja $(xd)y = x(dy)$ za vsak $x, y \in D$. Presečišču vseh treh semi asociativnostnih jeder polpolja pravimo *asociativnostno jedro* N.

Opomba 3.5. Ker je F polje in sam svoj center, ni potrebno, da θ zadošča $x^{1+\theta} \in Z$ za vsak $x \in F$. Vsa tri semi asociativnostna jedra iz D lahko izračunamo iz (7).

Lema 3.2. *Naj bo polje F končno in $\theta \neq 1$. Potem je F desno in srednje asociativnostno jedro polpolja D.*

Dokaz. Če v (7) vstavimo $t = 0$ ali $k = 0$, je desna stran enačbe enaka 0 za vsak x, y, z, h. Torej je F vsebovana v vsakem desnem in srednjem asociativnostnem jedru. Ker je vsako semi asociativnostno jedro obseg in je D končen, je vsak asociativnostno jedro tudi polje. Če bi bila desno ali srednje asociativnostno jedro večja od F, bi bil D polje in bi bila desna stran (7) vedno ničelna, ne glede na vrednosti spremenljivk. Predpostavimo, da je D polje in pokažimo, da pridemo do protislovja. Ker je D asociativen, je vsak asociator ničelen. Če vstavimo $t = k = 1$ in $y = 0$, iz (7) vidimo, da je $x^{\theta^2} = x$ in $b(x^{\theta^2} - x^{\theta}) = 0$ za vsak x. Ker je $\theta \neq 1$, je $\theta^2 = 1$ in $b = 0$. Če vstavimo $b = 0$ v (7), dobimo $t^{\theta}k(a^{\theta} - a)y = 0$ za vsak t, k, y. Ampak to velja natanko tedaj, ko je $a^{\theta} = a$ (to pomeni natanko tedaj, ko elementi a tvorijo podpolje K sestavljeno iz elementov, ki jih θ ohranja). Ker je $\theta^2 = 1$, mora biti $K = GF(q)$, kjer je $F = GF(q^2)$ in je θ podana z $x^{\theta} = x^q$ za vsak $x \in F$. Ampak, ko x teče po F, teče $x^{1+\theta} = x^{1+q}$ po vseh elementih iz K, tako da obstaja vrednost $x \in F$, da velja $x^{1+\theta} = a$. To pa je v nasprotju z (1) (spomnimo se, da je $b = 0$) in s tem smo dokazali lemo. □

V bistvu smo dokazali še več:

Lema 3.3. *Naj bo polje F končno. Potem je polpolje D asociativno natanko tedaj, ko je $\theta = 1$.*

Da bi lahko konstruirali D, moramo predpostaviti obstoj elementov $a, b \in F$ in antiavtomorfizma θ, ki zadošča nekateri pogojem. Ker je $\theta \neq 1$, mora biti v primeru, ko je F končen, F enak $GF(p^n)$, kjer je p praštevilo in $n \neq 1$.

Izrek 3.7. *Naj bo $F = GF(p^n)$, kjer je p praštevilo in $n > 1$. Potem lahko izberemo takšne a, b in θ, da polpolje D ni asociativno.*

Dokaz. Če je p lih, izberimo $x^{\theta} = x^p$, $b = 0$ in takšen a, da ni kvadrat v F. Ker je x^{1+p} vedno kvadrat, je pogoj (1) vedno zadoščen. Če je $p = 2$, izberimo $x^{\theta} = x^2$ in poljuben $b \neq 0$. V primeru, ko predpostavimo, da ni mogoča nobena izbira za a, ima $x^3 + bx = a$ rešitev za vsak $a \in F$. Ampak potem je preslikava $x \mapsto x^3 + bx$ injektivna in surjektivna, kar ni mogoče, ker ima $x^3 + bx = 0$ dve rešitvi: eno $x = 0$ in drugo $x = d$, kjer je d (natanko eden) element iz F, ki zadošča $d^2 = b$ (tu uporabimo dejstvo, da je vsak element končnega polja s karakteristiko 2 kvadrat). Torej obstaja izbira za a in je s tem izrek dokazan. □

3.5 Dicksonova komutativna polpolja

Naš zadnji primer polpolj bo komutativen, vendar neasociativen. Konstrukcija je podobna kot v prejšnjih razdelkih: F naj bo končno polje, D dvorazsežen vektorski prostor nad F z bazo $\{1, \lambda\}$ in na D definiramo množenje.

Naj bo $F = GF(p^n)$, kjer je p liho praštevilo in $n > 1$. Naj bo a poljubnen element, ki ni kvadrat v F. Če je θ avtomorfizem polja F podan z $x^\theta = x^{p^r}$, $1 \leq r < n$, potem definiramo množenje v D kot:

$$(x + \lambda y)(z + \lambda t) = (xz + ay^\theta t^\theta) + \lambda(yz + xt). \tag{1}$$

Izrek 3.8. *Vektorski prostor D je komutativno polpolje, ki ni nikoli asociativno.*

Preden dokažemo izrek, bomo pogledali in dokazali spodnjo lemo, saj jo bomo potrebovali pri dokazu izreka.

Lema 3.4. *Naj bo F srednje asociativnostno jedro D. Če je K podpolje polja F sestavljeno iz elementov, ki jih θ ohranja, je K desno in levo asociativnostno jedro. Od tod pa sledi, da je K asociativnostno jedro in center polpolja D.*

Dokaz. Če izračunamo asociator, dobimo

$$[x + \lambda y, z + \lambda t, h + \lambda k] = at^\theta(y^\theta(h - h^\theta) + k^\theta(x^\theta - x)) + \lambda at^\theta(y^\theta k - yk^\theta).$$

Če nastavimo t na 0, bo očitno desna stran ničelna. Pokažimo sedaj, da je K desno in levo asociativnostno jedro:

i) Nastavimo $k = 0$ in upoštevamo, da je $h^\theta = h$. Dobimo $[x + \lambda y, z + \lambda t, h] = at^\theta y^\theta(h - h^\theta) = 0$.

ii) Nastavimo sedaj $y = 0$ ter upoštevajmo, da je $x^\theta = x$. Dobimo $[x, z + \lambda t, h + \lambda k] = at^\theta k^\theta(x^\theta - x) = 0$.

Ker je $D \neq K$, je K hkrati N_l, N_m in N_r in je zato tudi asociativnostno jedro. Ker je D komutativen, je K tudi center. □

Sedaj pa si lahko pogledamo dokaz Izreka 3.8.

Dokaz. Množenje v D je po definiciji komutativno, saj je F polje. Komutativno je tudi seštevanje in pogoj **VW1** velja. Ker je F končna množica, moramo namesto pogoja **VW2** pokazati, da sta edini rešitvi $x + \lambda y$ in $z + \lambda t$ enačbe $(x + \lambda y)(z + \lambda t) = 0$ ničelni.

Če enačimo desno stran enačbe (1) z 0, dobimo:

$$\begin{aligned} xz + ay^\theta t^\theta &= 0, \\ yz + xt &= 0. \end{aligned} \tag{2}$$

Če je $z = 0$, potem je ali $t = 0$ ali $x = y = 0$, torej lahko predpostavimo, da je $z \neq 0$. Če prvo enačbi iz (2) rešimo po x in to vstavimo v drugo, dobimo $yz - ay^\theta t^{1+\theta} z^{-1} = 0$, od kod sledi

$$z^2 = ay^{\theta-1}t^{\theta+1} = ay^{p^r-1}t^{p^r+1}, \quad \text{če je} \quad y \neq 0. \tag{3}$$

Ampak vsak faktor iz (3), razen a, je kvadrat, zato mora biti $z = 0$. To pa vodi do protislovja, zato je $y = 0$. Sedaj lahko vidimo, da mora biti tudi $x = 0$. Pogoj **VW3** je trivialen, za pogoj **VW4** pa moramo pokazati distributivnost samo z ene strani, ker je množenje komutativno:

$$\begin{aligned} &(x + \lambda y)((z_1 + \lambda t_1) + (z_2 + \lambda t_2)) = (x + \lambda y)((z_1 + z_2 + \lambda(t_1 + t_2)) = x(z_1 + z_2) + \\ &+ ay^\theta(t_1 + t_2)^\theta + \lambda(y(z_1 + z_2) + x(t_1 + t_2)) = xz_1 + xz_2 + ay^\theta t_2^\theta + ay^\theta t_1^\theta + \lambda(yz_1 + \\ &+ yz_2 + xt_1 + xt_2) = (x + \lambda y)(z_1 + \lambda t_1) + (x + \lambda y)(z_2 + \lambda t_2). \end{aligned}$$

Torej je D komutativno polpolje. Da bi dokazali, da je D neasociativno polpolje, uporabimo prej napisano Lemo 3.4. Ker sta D in K različna, polpolje D ne more biti polje. □

3.6 Hughesove ravnine

V prejšnjih razdelkih smo prikazali nedesarguesove projektivne ravnine tako, da smo našli kvazi polja, ki niso obsegi. V tem razdelku bomo obravnavali razred končnih projektivnih ravnin imenovan *Hughesove ravnine*, ki ne more biti koordinatiziran z nobenim linearnim ravninskim ternarnim kolobarjem. Za vsako liho potenco praštevila q obstaja Hughesova ravnina reda q^2. Najmanjšo takšno ravnino (reda 9) sta prva odkrila Veblen in Wedderburn.

Druga lastnost, ki loči Hughesove ravnine od ostalih podanih primerov je ta, da za poljubno Hughesovo ravnino $\mathscr{H}$ njena polna kolineacijska grupa ne ohranja točke ali premice iz $\mathscr{H}$. Hughesove ravnine so v bistvu edine poznane nedesarguesove ravnine s to lastnostjo.

Če je q liha potenca praštevila, potem po Lemi 2.8 vedno obstaja vsaj eno takšno skoraj polje N reda q^2 z jedrom $F = GF(q)$, da vsak element iz F komutira z vsakim elementom iz N. S pomočjo elementov iz N bomo konstruirali Hughesovo ravnino $\mathscr{H}$ reda q^2.

Naj bo $V = N^3$ s seštevanjem po komponentah. Naj bo množenje s skalarjem z leve z elementi iz N definirano kot $k(x_1, x_2, x_3) = (kx_1, kx_2, kx_3)$. V bistvu hočemo iz množice V narediti nekakšen levi vektorski prostor nad N. Točke v $\mathscr{H}$ bodo ekvivalenčni razredi z relacijo $(x_1, x_2, x_3) \sim (kx_1, kx_2, kx_3)$, kjer so elementi (x_1, x_2, x_3) iz $V \setminus \{(0,0,0)\}$ in k neničelen element iz N. Če je $x = (x_1, x_2, x_3)$, potem označimo točko v $\mathscr{H}$ z $\langle x \rangle$. Če je $A = (a_{ij})$ poljuben element iz $GL_3(q)$ (to je 3×3 matrika z elementi iz $F = GF(q)$), potem je preslikava $\theta(x_1, x_2, x_3) = (a_{11}x_1 + a_{12}x_2 + a_{13}x_3, a_{21}x_1 + a_{22}x_2 + a_{23}x_3, a_{31}x_1 + a_{32}x_2 + a_{33}x_3)$ avtomorfizem aditivne grupe V. Ker je N asociativna in vsak element iz F komutira z vsemi elementi iz N, preslikava θ slika (kx_1, kx_2, kx_3) v

$$\begin{aligned}&(a_{11}(kx_1) + a_{12}(kx_2) + a_{13}(kx_3), a_{21}(kx_1) + a_{22}(kx_2) + a_{23}(kx_3), a_{31}(kx_1) + \\ &+ a_{32}(kx_2) + a_{33}(kx_3)) = \\ &= (k(a_{11}x_1 + a_{12}x_2 + a_{13}x_3), k(a_{21}x_1 + a_{22}x_2 + a_{23}x_3), k(a_{31}x_1 + a_{32}x_2 + a_{33}x_3)).\end{aligned}$$

Preslikava θ inducira permutacijo na točkah iz $\mathscr{H}$. Uporabili bomo oznako, ki se uporablja v vektorskih prostorih in predstavili preslikavo θ z $x' \mapsto Ax'$ ali pa bomo, če je P točka $\langle x \rangle$, pisali PA za sliko iz P pod θ.

Če je t vnaprej določen element iz N, je $x_1 + x_2t + x_3 = 0$ natanko tedaj, ko je $kx_1 + (kx_2)t + kx_3 = 0$ za vsak neničelen $k \in N$. To je množica vseh takšnih elementov (x_1, x_2, x_3) iz V, da je $x_1 + x_2t + x_3 = 0$, sestavljena iz $(0,0,0)$ skupaj z množico točk iz $\mathscr{H}$. To množico točk označimo z $L(t)$. Grupa $GL_3(q)$ vsebuje takšno matriko A, da je $A^{q^2+q+1} = kI$ za nek $k \in GF(q)$ in da nobena manjša potenca matrike A nima te lastnosti. Torej je A reda $q^2 + q + 1$ kot permutacija točk iz $\mathscr{H}$. Premice v $\mathscr{H}$ definiramo kot množico točk

$$L(t)A^m = \left\{ \langle A^m x' \rangle \mid \langle x \rangle \in L(t) \right\}$$

za $0 \leq m \leq q^2 + q$, kjer je $t = 1$, ali pa je t vnaprej določen element iz $N \setminus F$.

Izrek 3.9. *Množica točk in premic iz $\mathscr{H}$ definirana zgoraj je končna projektivna ravnina reda q^2.*

Dokaz. Število točk v $\mathscr{H}$ je enako številu elementov iz V različnih od $(0,0,0)$, deljeno s številom, ki predstavlja iste točke iz $\mathscr{H}$. V skoraj polju N je q^2 elementov, zato je v množici V število neničelnih elementov $q^6 - 1$. Koliko pa je istih točk v $\mathscr{H}$? Toliko, kolikor je neničelnih elementov v N, saj je $(x_1, x_2, x_3) = (kx_1, kx_2, kx_3)$ za poljuben neničelen element $k \in N$. Zato je število točk iz $\mathscr{H}$ enako $(q^6 - 1)/(q^2 - 1) = q^4 + q^2 + 1$.

Za poljuben t je število točk na $L(t)$ enako $q^2 + 1$. Ker je vsaka premica slika ene izmed teh množic točk pod elementom iz $GL_3(q)$, vsaka premica vsebuje natanko $q^2 + 1$ točk.

Število premic je kvečjemu enako število različnih $L(t)$ pomnoženih s številom možnih moči A; tj. $(q^2-q+1)(q^2+q+1) = q^4+q^2+1$. Izrek bo dokazan, če pokažemo, da se poljubni različni premici sekata v natanko eni točki.

Ne glede na to, ali je $\mathscr{H}$ projektivna ravnina ali ne, vsaka preslikava A^i ohranja incidenčno relacijo v $\mathscr{H}$. Torej je za dokaz, da se poljuben par različnih premic seka natanko v eni točki dovolj, da pokažemo, da se poljuben par različnih premic $L(t)A^m$ in $L(s)$ seka v enolični točki. Naj bo A^{-m} matrika (a_{ij}). Točka $P = \langle(x,y,z)\rangle$ leži na obeh premicah $L(t)A^m$ in $L(s)$ natanko tedaj, ko leži P na $L(s)$ in PA^{-m} na $L(t)$. Torej leži P na obeh premicah natanko tedaj, ko velja

$$(a_{11}x + a_{12}y + a_{13}z) + (a_{21}x + a_{22}y + a_{23}z)t + (a_{31}x + a_{32}y + a_{33}z) = 0 \quad \text{in} \tag{1}$$

$$x + ys + z = 0. \tag{2}$$

Torej moramo pokazati, da imata enačbi (1) in (2) enolično rešitev (x,y,z), določeno do levega množenja z N natančno.

Če rešimo enačbo (2) po x in rešitev vstavimo v (1), dobimo

$$yu + za + (yv + zb)t = 0, \tag{3}$$

kjer velja

$$\begin{aligned} u &= a_{12} + a_{32} - (a_{11} + a_{31})s, & v &= a_{22} - a_{21}s, \\ a &= a_{13} + a_{33} - (a_{11} + a_{31}), & b &= a_{23} - a_{21}. \end{aligned} \tag{4}$$

Ker so vsi a_{ij} iz F, sta tudi a in b iz F in komutirata z vsakim elementom iz N. Sedaj moramo preveriti nekaj primerov:

a) $b \neq 0$. V tem primeru lahko enačbo (3) zapišemo malo drugače:

$$(yv + zb)b^{-1}a + y(u - vb^{-1}a) + (yv + zb)t = 0$$

to pa se poenostavi v

$$(yv + zb)(b^{-1}a + t) + y(u - vb^{-1}a) = 0. \tag{5}$$

Če je $t = 1$, potem lahko vidimo, da imata (2) in (3) natanko eno skupno rešitev za točko $\langle(x,y,z)\rangle$. Če je je $t \neq 1$, potem t ni v F in zato je v tem primeru $w = b^{-1}a + t$ neničelen. Potem (5) postane $(yv + zb)w = -y(u - vb^{-1}a)$. Če pomnožimo to enačbo z w^{-1}, dobimo

$$y(v + (u - vb^{-1}a)w^{-1}) + zb = 0. \tag{6}$$

Ker je $b \neq 0$, imata (6) in (2) natanko eno skupno rešitev za točko $\langle(x,y,z)\rangle$.

b) $b = 0, a \neq 0$. V tem primeru iz (3) dobimo

$$y(u + vt) + za = 0. \tag{7}$$

Ker je $a \neq 0$, imata (7) in (2) enolično rešitev.

c) $a = b = 0$. Iz teh pogojev sledi

$$a_{13} + a_{33} = a_{11} + a_{31} \quad \text{in} \quad a_{23} = a_{21}. \tag{8}$$

Poglejmo si sedaj točko $P = \langle(1, 0, -1)\rangle$. Iz (8) dobimo, da je $PA^{-m} = (c, 0, -c)$, kjer je $c = a_{11} - a_{13}$. Ker je A^{-m} nesingularna je $c \neq 0$ in $PA^{-m} = P$. Torej po začetni izbiri A velja $m \equiv 0 (\mathrm{mod}\, q^2 + q + 1)$ in $L(t)A^m = L(t)$. Ampak sedaj lahko vidimo, da imata $L(t)$ in $L(s)$ skupno le točko $\langle(1, 0, -1)\rangle$.

□

Lema 3.5. *Množica $\mathscr{H}_0$ vseh točk oblike $\langle x\rangle$, kjer je $x \in F^3 \setminus \{(0, 0, 0)\}$, skupaj s premicami, ki povezujejo te točke, tvori Desarguesovo podravnino ravnine $\mathscr{H}$.*

Dokaz. Iz enačbe (1) iz Izreka 3.9 opazimo, da lahko premico $L(t)A^m$ iz $\mathscr{H}$ zapišemo kot enačbo oblike $xa + yb + zc + (xa' + yb' + zc')t = 0$, kjer so a, b, c, a', b', c' elementi iz F. Torej ima poljubna premica oblike $L(1)A^m$ enačbo oblike $xa + yb + zc = 0$, kjer so $a, b, c \in F$. Ker imamo v $L(1)A^m$ natanko $q^2 + q + 1$ različnih premic, vsaka enačba oblike $xa + by + zc = 0$, kjer so $a, b, c \in F$, predstavlja eno izmed premic $L(1)A^m$.

Iz razprave v [2, stran 23] sledi, da točke iz $\mathscr{H}_0$ in premice $L(1)A^m$, kjer je $m = 0, 1, \ldots, q^2 + q$, sestavljajo Desarguesovo ravnino reda q. □

Iz konstrukcije ravnine vidimo, da vsaka izmed matrik A^i inducira kolineacijo v ravnini $\mathscr{H}$ in da ciklična grupa, ki jo generirajo, ne ohranja točke ali premice iz $\mathscr{H}$. Torej, če $\mathscr{H}$ vsebuje translacijsko premico, mora vsebovati več kot eno. Ampak končna ravnina, ki ima 2 translacijski premici, je Desarguesova (glej knjigo [2, poglavje VI]). Torej imamo dve možnosti. Ali je $\mathscr{H}$ Desarguesova, ali pa je ne moremo koordinatizirati s kvazi poljem.

Da bi pokazali, da je $\mathscr{H}$ nedesarguesova, jo bomo koordinatizirali na takšen način, da ne bo ravninski ternarni kolobar niti linearen. Z uporabo urejene trojice, bomo koordinatizirali $\mathscr{H}$ z metodo, ki je bila predstavljena v razdelku 3.2. Naj bo (∞) točka $(0, 0, 1)$, točka (0) bo $(1, 0, 0)$, točka $(0, 0)$ bo $(0, 1, 0)$ in (1) bo točka $(1, 0, -1)$. Premica l_∞ predstavlja premico $y = 0$. Nova x os je $z = 0$, nova y os

pa $x = 0$. Sedaj lahko označimo točke na novi y osi tako, da bo točka $(0, 1, v)$ postala točka $(0, v)$ v našem novem sistemu. Vsaka premica skozi (1) ali $(1, 0, -1)$ je oblike $x + yt + z = 0$. Točka $(v, 0)$ na x osi bo točka $(u, 1, 0)$, ki je kolinearna z $(1, 0, -1)$ in $(0, 1, v)$. Ampak $(1, 0, -1)$ in $(0, 1, v)$ ležita na premici $L(-v)$, če v ni iz F. Torej je $u + 1(-v) + 0 = 0$ ali $u = v$. Če je $v \in F$, potem je očitno, da je $u = v$ in je $(v, 0)$ točka $(v, 1, 0)$.

Ker je točka (m) na l_∞, bo to točka oblike $(1, 0, v)$. Hkrati je (m) točka na l_∞, ki je kolinearna z $(1, 1, 0)$ in $(0, 1, m)$. Naj bo $xa + yb + zc + (xa' + yb' + zc')t = 0$ premica, ki vsebuje $(1, 1, 0)$ in $(0, 1, m)$. Potem velja:

$$a + b + (a' + b')t = 0, \tag{1}$$

$$b + mc + (b' + mc')t = 0. \tag{2}$$

Ker so $a, a', b, b' \in F$, iz (1) sledi, da velja bodisi $t = 1$ in $a + a' = -(b + b')$ bodisi $t \neq 1$ in $a + b = a' + b' = 0$. Če je $t = 1$, potem je $a + a' + v(c + c') = 0$ in iz (2) dobimo

$$a + a' + (-m)(c + c') = 0.$$

Torej je $v = -m$. Če je $t \neq 1$, potem je $a + vc + (a' + vc')t = 0$ in iz (2) dobimo $-a + mc + (-a' + mc')t = 0$ in je spet $v = -m$. Torej je (m) točka $(1, 0, -m)$.

Naj točka (u, v) leži na premici m_1, ki gre skozi točki $(0, 0, 1)$ in $(u, 1, 0)$ ter na m_2, ki gre skozi $(1, 0, 0)$ in $(0, 1, v)$. Potem imamo:

$$\begin{aligned} m_1 &: xa + yb + zc + (xa' + yb' + zc')t = 0, \\ m_2 &: xd + ye + zf + (xd' + ye' + zf')s = 0, \end{aligned} \tag{3}$$

kjer je

$$c + c't = d + d's = ua + b + (ua' + b')t = e + vf + (e' + vf')s = 0. \tag{4}$$

Naredimo kot prej: imamo bodisi $t = 1$ in $c = -c'$ bodisi $t \neq 1$ in $c = c' = 0$ in podobno bodisi $s = 1$ in $d = -d'$ bodisi $s \neq 1$ in $d = d' = 0$.

Preveriti moramo štiri primere:

i) Če je $t \neq 1$ in $s \neq 1$, z uporabo (4) hitro vidimo, da $(u, 1, v)$ leži na obeh premicah m_1 in m_2. Če je $t \neq 1$ imamo

$$xa + yb + (xa' + yb')t = 0,$$

kjer je $ua + b + (ua' + b')t = 0$ in točka $(u, 1, v)$ leži na premici m_1. Ko je $s \neq 1$, je

$$ye + zf + (ye' + zf')s = 0,$$

kjer je $e + vf + (e' + vf')s = 0$. Torej $(u, 1, v)$ leži tudi na m_2.

ii) Če je $t = 1$ in $s \neq 1$, potem je m_1 oblike

$$x(a + a') + y(b + b') = 0,$$

kjer je $u(a + a') + b + b' = 0$, zato $(u, 1, v)$ leži na m_1. Premica m_2 je potem

$$ye + zf + (ye' + zf')s = 0,$$

kjer je $e + vf + (e' + vf')s = 0$ in zato leži $(u, 1, v)$ tudi na m_2.

iii) Če je $t \neq 1$ in $s = 1$, smo že pokazali, da leži točka $(u, 1, v)$ na m_1. Preverimo še, da leži tudi na m_2. V tem primeru je m_2 oblike

$$y(e + e') + z(f + f') = 0,$$

kjer je $e + e' + v(f + f') = 0$. Vidimo, da leži $(u, 1, v)$ tudi na m_2.

iv) Iz prejšnjih primerov vidimo, da leži $(u, 1, v)$ na obeh premicah m_1 in m_2 tudi, ko je $t = 1$ in $s = 1$.

V vseh primerih ugotovimo, da leži $(u, 1, v)$ na m_1 in m_2, zato je (u, v) res $(u, 1, v)$. Iz povedanega dobimo naslednjo lemo.

Lema 3.6. *Če je ravnina $\mathscr{H}$ koordinatizirana kot zgoraj, je (u, v) točka $(u, 1, v)$, točka (m) je $(1, 0, -m)$ in (∞) je $(0, 0, 1)$.*

Poglejmo si sedaj ternarni kolobar za $\mathscr{H}$, kjer uporabimo $T(a, b, c) = ab + c$ za ternarno operacijo. Naj bo $a \oplus b = T(1, a, b)$ in $a \otimes b = T(a, b, 0)$. Da bi izračunali vrednost $T(m, u, v)$, imejmo še premico l, ki gre skozi točki $(1, 0, -m)$ in $(u, 1, v)$ ter naj bo $(0, 1, k)$ presečišče l z y osjo. Potem je $k = T(m, u, v)$. Naj bo l premica

$$xa + yb + zc + (xa' + yb' + zc')t = 0.$$

Potem imamo:

$$a - mc + (a' - mc')t = 0 \qquad \text{in} \tag{5}$$

$$ua + b + vc + (ua' + b' + vc')t = 0. \tag{6}$$

Lema 3.7. *Za vsak a in b je $a \oplus b = a + b$.*

Dokaz. Naj bo $m = 1$ v (5). Potem je $a - c + (a' - c')t = 0$. Če je $t = 1$, imamo $a + a' = c + c'$ in je (6) enako $u(a + a') + (b + b') + v(c + c') = 0$ ali $(u + v)(a + a') + (b + b') = 0$. Ampak potem točka $(0, 1, u + v)$ leži na l in je $k = u \oplus v = u + v$. Če je $t \neq 1$, je $a = c$ in $a' = c'$, iz (6) pa dobimo

$$(u + v)a + b + \left[(u + v)a' + b'\right] t = 0.$$

Torej $(0, 1, u + v)$ spet leži na l in je $u \oplus v = u + v$. □

Izrek 3.10. *Ternarni kolobar (N, T) ni linearen.*

Dokaz. Naj bosta m in u v (5) in (6) takšna elementa, da je $u \neq 0$ in v izbran tako, da je $k = T(m, u, v) = 0$. Potem leži $(0, 1, 0)$ na l in je $b + b't = 0$. Predpostavimo, da je $t = 1$ in je $b = -b'$. Potem je (5) kar $a + a' - m(c + c') = 0$ in (6) je

$$u(a + a') + v(c + c') = 0.$$

Iz tega sledi $u^{-1}v = -m$ ali $um + v = 0$. Če je $t \neq 1$ in $b = b' = 0$, iz (5) dobimo $a - mc + (a' - mc')t = 0$ in (6) lahko zapišemo kot

$$a + u^{-1}vc + (a' + u^{-1}vc')t = 0$$

in ponovno dobimo $u^{-1}v = -m$ ali $um + v = 0$.

Predpostavimo sedaj, da je (N, T) linearen. Za poljubna m in u, kjer je $u \neq 0$, naj bo $p = m \otimes u$. Potem je $m \otimes u \oplus (-p) = T(m, u, -p) = 0$ in po zgornjem dobimo $um + (-p) = 0$ ali $um = p = m \otimes u$. Torej je (N, T) multiplikativno antiizomorfen skoraj polju N in je desno skoraj polje. Vsaka končna projektivna ravnina, ki jo lahko koordinatiziramo z desnim kvazi poljem in katere polna kolineacijska grupa ne ohranja točke, je Desarguesova. Torej je $\mathscr{H}$ Desarguesova in mora biti N polje. Ker je N izbran tako, da ne more biti polje, pridemo do protislovja in ravninski ternarni kolobar (N, T) ne more biti linearen. □

Posledica 3.2. *Hughesove ravnine so nedesarguesove.*

Literatura

[1] D. R. Hughes in E. Kleinfeld, *Seminuclear extensions of Glois fields*, Amer. J. Math. 82, 389–392, 1960.

[2] D. R. Hughes in F. C. Piper, *Projective planes*, Graduate Texts in Mathematics, Vol. 6. Springer-Verlag, New York-Berlin, 1973.

[3] N. I. Ivanov, *Affine planes, ternary rings, and examples of non-Desarguesian planes*, verzija 2014, [ogled 15. 6. 2015], dostopno na http://www.researchgate.net/publication/276355010_Affine_planes_ternary_rings_and_examples_of_non-Desarguesian_planes.

[4] N. I. Ivanov, *Non-Desarguesian planes*, verzija 2008, [ogled 3. 1. 2015], dostopno na http://www.researchgate.net/publication/228839738_Non-Desarguesian_planes.

[5] E. J. Landquist, *On nonassociative division rings and projective planes*, Master of Science in Mathematics, Blacksburg, 2000, [ogled 10. 9. 2015], dostopno na http://scholar.lib.vt.edu/theses/available/etd-05182000-12080004/unrestricted/sfield.pdf.

[6] G. E. Moorehouse, *On projective planes of order less than 32*, verzija 2000, [ogled 11. 7. 2015], dostopno na http://www.uwyo.edu/moorhouse/pub/wyoming.pdf.

[7] A. Vavpetič, *Afina in projektivna geometrija*, verzija 2011, [ogled 10. 5. 2015], dostopno na http://www.fmf.uni-lj.si/~vavpetic/APG/APG.pdf.

[8] O. Veblen in J. H. Maclagan-Wedderburn, *Non-Desarguesian and non-Pascalian geometries*, Trans. Amer. Math. Soc. 8, no. 3, 379—388, 1907.

[9] C. Weibel, *Survey of Non-Desarguesian planes*, Notices Amer. Math. Soc. 54, no. 10, 1294–1303, 2007.

Stvarno kazalo