UNIVERZITET U BEOGRADU

MATEMATIČKI FAKULTET

Neophodnost uslova komutativnosti i asocijativnosti kod Dezargovih i Paposovih ravni

MASTER RAD

Autor
Snežana Milosavljević

Mentor
dr Miroslava Antić

Beograd
2014.

Sadržaj

Predgovor

Dezargova i Paposova teorema spadaju u teoreme klasične (realne) projektivne geometrije, koje stoga važe i u afinoj realnoj ravni, koja je uz dodate idealne tačke model te geometrije. Algebarski pristup geometriji i konstrukcije projektivnih i afinih ravni nad algebarskim strukturama koje nisu polje realnih brojeva aktualizovale su i pitanje važenja Dezargove i Paposove teoreme u njima. Naime, one nisu posledica aksioma projektivne (odnosno afine) ravni. U ovom radu bavimo se afinim ravnima i vezom između algebarske strukture koja odgovara jednoj takvoj ravni i činjenice da li je ona ne-Dezargova ili ne-Paposova.
U prvom poglavlju su predstavljene algebarske strukture prstena, kvazipolja, tela, polja, prstena sa deljenjem, ternarnog i ravanskog ternarnog prstena itd. Tu takođe dajemo primer kvaterniona koji čine tela i oktonione koji su primer prstena sa deljenjem. U drugom poglavlju uvodimo afine ravni i pojam izomorfizma među njima. Uvodimo pojmove translacije i dilatacije, pokazujemo kako se jedna afina ravan može koordinatizovati pomoću ravanskog ternarnog prstena i bavimo se pitanjem izomorfizma dve takve ravni. Pokazaćemo da je afina ravan definisana nad telom ako i samo ako u njoj važi Dezargova teorema, odnosno neophodnost asocijativnosti u ternarnom prstenu nad kojim je afina ravan izgrađena. Pokazaćemo i da Paposova teorema povlači Dezargovu, kao i da je neophodan i dovoljan uslov da ona važi komutativnost množenja u ravanskom ternarnom prstenu.

U trećem poglavlju dajemo primere nekih ravanskih ternarnih prstena koji nisu asocijativni ili komutativni i koji stoga određuju ne-Paposove i ne-Dezargove ravni.

Za čitaoce koji bi dublje da istraže ovu temu preporučujemo E. Artin [1] za upoznavanje sa teorijom afinih i projektivnih ravni (videti [1], Glava II) i D. Hughes i F. Piper [5], verovatno najsveobuhvatniju knjigu o projektivnim ravnima (studija koja je u suštini ekvivalentna studiji o afinim ravnima).

Zahvalila bih se članovima komisije, dr Zoranu Rakiću i dr Srđanu Vukmiroviću, na pažljivom čitanju rada i korisnim komentarima koji su ga poboljšali.

1 Algebarski pojmovi

1.1 Osnovne algebarske strukture

U ovom poglavlju daćemo kratak pregled algebarskih pojmova, a posebno struktura koje će nam biti od značaja u radu.

Dekartov proizvod proizvoljnih skupova A i B je skup čiji su elementi svi uređeni parovi (a, b) gde je $a \in A$ i $b \in B$ i označavamo ga

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

Ako je $A = B$, onda skup $A \times A$ označavamo sa

$$A^2 = \{(a, b) : a, b \in A\}$$

i zovemo **Dekartovim kvadratom** skupa A.

Binarna operacija u nepraznom skupu A je svako preslikavanje $\omega : A^2 \to A$ kojim se proizvoljnom paru (a, b) njegovih elemenata a i b pridružuje određen element $\omega(a, b)$ tog istog skupa A. Taj element još označavamo $a\ \omega\ b$.

Slično, **ternarna operacija** na skupu A je svako preslikavanje $\omega : A^3 \to A$ kojim se proizvoljnoj trojci (a, b, c) elemenata $a, b, c \in A$ pridružuje određen element $\omega(a, b, c)$ iz tog skupa.

Binarna operacija $*$ na skupu A je

1. **asocijativna** ako $(a * b) * c = a * (b * c),\ \ \forall\, a, b, c \in A$
2. **komutativna** ako $a * b = b * a,\ \ \forall\, a, b \in A$.

Neka je dat skup A sa dve binarne operacije $+$ i $\cdot$ koje zovemo sabiranje i množenje. Tada kažemo da je operacija $\cdot$

1. **levo distributivna** u odnosu na operaciju $+$ ako

$$a \cdot (b + c) = a \cdot b + a \cdot c,\ \ \forall\, a, b, c \in A$$

2. **desno distributivna** u odnosu na operaciju $+$ ako

$$(b + c) \cdot a = b \cdot a + c \cdot a,\ \ \forall\, a, b, c \in A$$

3. **distributivna** u odnosu na $+$ ako je levo i desno distributivna.

Uređeni par $(A, *)$, gde je A neki skup i $*$ binarna operacija u tom skupu nazivamo **grupoid**.

Asocijativni grupoid nazivamo **polugrupom**.

Ukoliko u polugrupi postoji element e takav da

$$a * e = a, e * a = a,\ \ \forall\, a \in A$$

onda taj element nazivamo **neutral**, a polugrupu sa neutralom nazivamo **monoid**.

Neprazni skup G sa binarnom operacijom $*$ zvaćemo **kvazigrupom** ako važi:

1. $a * x = b$ ima jedinstveno rešenje x, za sve $a, b \in G$,

2. $y * a = b$ ima jedinstveno rešenje y za sve $a, b \in G$.

Ukoliko u kvazigrupi postoji neutral, tada je G **petlja**.
Petlja G ispunjava **osobinu desnog inverza** ako

$$\forall x \in G,\ \exists x^{-1} \in G, (y * x) * x^{-1} = y,\ \ \forall y \in G.$$

Slično, u G važi **osobina levog inverza** ako

$$\forall x \in G,\ \exists x^{-1} \in G, x^{-1} * (x * y) = y,\ \ \forall y \in G.$$

Ako u G važe osobine desnog i levog inverza onda u G važi **osobina inverza**.
Element $a \in A$ jednog monoida je **inverzibilan** ako postoji element $b \in A$ takav da je

$$a * b = e, \qquad b * a = e.$$

Tada je b njegov inverz i još ga označavamo sa a^{-1}.
Monoide u kojima su svi elementi inverzibilni nazivamo **grupama**.
Grupa je **Abelova**, odnosno, **komutativna** ako je $*$ komutativna operacija.

Neka su na skupu K definisane dve binarne operacije $+$ i $\cdot$. Uređena trojka $(K, +, \cdot)$ je **prsten** ako zadovoljava sledeće uslove:

1. $(K, +)$ je komutativna grupa
2. $(K, \cdot)$ je monoid
3. operacija $\cdot$ je distributivna u odnosu na $+$.

U prstenu neutral za sabiranje obično nazivamo nulom i označavamo sa 0, a neutral za množenje zovemo jedinicom i označavamo sa 1. S obzirom da u prstenu važi distributivni zakon sledi da je $\forall a \in A,\ \ a \cdot 0 = 0 \cdot a = 0$. Zato, ukoliko prsten ima bar dva elementa važi $1 \neq 0$, i pri tom 0 nema inverz za množenje.
Slabo (levo) kvazipolje W je skup sa dve binarne operacija $+$ i $\cdot$ koji zadovoljava:

1. $(W, +)$ je Abelova grupa sa neutralom za sabiranje 0
2. $(W \backslash \{0\}, \cdot)$ je petlja
3. važi $0 \cdot x = 0\ \ \forall x \in W$
4. $x \cdot (y + z) = x \cdot y + x \cdot z\ \ \forall x, y, z \in W$.

Ako umesto uslova 4. važi uslov

$4'$. $(y + z) \cdot x = y \cdot x + z \cdot x\ \ \forall x, y, z \in W$

onda W nazivamo **slabo desno kvazipolje**.

Lema 1.1 Ako je W slabo kvazipolje onda

1. $a \cdot 0 = 0\ \ \forall a \in W$
2. $a \cdot (-b) = -(a \cdot b)\ \ \forall a, b \in W$.

Jezgro slabog kvazipolja W je skup svih elemenata $k \in W$ takvih da važi

1. $(x+y) \cdot k = x \cdot k + y \cdot k$
2. $(x \cdot y) \cdot k = x \cdot (y \cdot k)\ \ \forall x, y \in W$.

Kvazipolje (levo) je slabo levo kvazipolje $(K, +, \cdot)$ takvo da za $a \neq a'$ jednačina $ax = a'x + b$ ima jedinstveno rešenje za x.

Desno kvazipolje je slabo desno kvazipolje $(K, +, \cdot)$ takvo da za $a \neq a'$ jednačina $xa = xa' + b$ ima jedinstveno rešenje za x.

Levo skoro polje je levo kvazipolje sa asocijativnim množenjem. Nenula elementi skorog polja čine grupu u odnosu na množenje. Desno skoro polje je desno kvazipolje sa asocijativnim množenjem.

Konačno slabo kvazipolje je kvazipolje.

Svako kvazipolje koje ima asocijativno množenje naziva se **skoro polje**. Kvazipolje koje zadovoljava desni distributivni zakon nazivamo **prstenom sa deljenjem**.

Kako je prsten sa deljenjem ujedno i desno i levo kvazipolje, on sadrži levo i desno jezgro. Takođe sadrži i srednje jezgro. Ove podskupove nazivamo **seminukleusima**.

Desni nukleus N_d prstena sa deljenjem D je skup svih elemenata d iz D takvih da je $(xy)d = x(yd)\ \forall x, y \in D$. Levi i srednji nukleus se definišu analogno; N_l, N_s, N_d su seminukleusi od D. Presek N ova tri seminukleusa od D zovemo **nukleus** ili jezgro, dok skup svih $n \in N$ takvih da je $dn = nd, \forall d \in D$ nazivamo **centrom** od D i obeležavamo sa Z.

Neka je D prsten sa deljenjem. Ako D zadovoljava levi i desni alternativni zakon (levi: $x(xy) = x^2y$, desni: $(xy)y = xy^2\ \forall x, y \in D$) onda D zovemo **alternativnim prstenom sa deljenjem**.

Teorema 1.1 *Prsten sa deljenjem D sa osobinom desnog inverza je alternativni.*

Teorema 1.2 *Svaki alternativni prsten sa deljenjem D zadovoljava osobinu inverza.*

Teorema 1.3 *Svaki konačan alternativni prsten sa deljenjem je polje.*

Prstene u kojima jedino nula nema inverz zovemo **telima**.

Lema 1.2 Asocijativni prsten sa deljenjem je telo.

Komutativna tela zovemo **poljima**. Ako je n najmanji prirodan broj takav da je $n1 = 1 + \cdots + 1 = 0$ tada kažemo da je n **karakteristika polja**. Ako takav prirodan broj ne postoji, onda kažemo da je karakteristika polja ∞.

Navodimo Vederburnovu teoremu.

Teorema 1.4 *Svako konačno telo je polje.*

Ako je K polje, možemo govoriti o polinomima nad K. Predstavićemo ih u obliku $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ gde su a_i elementi iz K i x novi simbol koji nazivamo neodređenom. Sabiranje i množenje polinoma je definisano na uobičajeni način. Za neko b iz K govorimo o vrednosti $f(x)$ u b: to je $f(b) = a_n b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0$ što je element iz K. Reći ćemo da je $f(x)$ nesvodljiv ako ne postoje polinomi $g(x)$ i $h(x)$, oba manjeg stepena od $f(x)$, takvi da $f(x) = g(x)h(x)$.

Neka je p prost broj i $q = p^n$. Tada postoji jedinstveno polje, zvano Galoaovo polje sa q elemenata, koje označavamo sa $GF(q)$. Svako konačno polje je izomorfno sa nekim $GF(q)$. Važi:

1. $GF(q)$ je karakteristike p.
2. Multiplikativna grupa od $GF(q)$ je ciklična.
3. Ako je $p = 2$ onda je svaki element iz $GF(q)$ kvadrat, a ako je $p \neq 2$ onda su tačno pola od nenula elemenata iz $GF(q)$ kvadrati.
4. Svaki element iz $GF(q)$ je suma dva kvadrata.

Za neko telo K, **automorfizam** od K je $1-1$ preslikavanje $\alpha : K \to K, \alpha(x) = x^\alpha$ takvo da je

$$(x+y)^\alpha = x^\alpha + y^\alpha \quad \text{i} \quad (xy)^\alpha = x^\alpha y^\alpha, \quad \forall x, y \in K.$$

Skup automorfizama tela K čini grupu $Aut(K)$. Anti-automorfizam od K je $1-1$ preslikavanje β tako da je $(x+y)^\beta = x^\beta + y^\beta$ i $(xy)^\beta = y^\beta x^\beta$ $\forall x, y \in K$.

Neka je $(V, +)$ Abelova grupa, K telo i $\cdot : K \times V \to V$ preslikavanje takvo da je

1. $k \cdot (v + u) = k \cdot v + k \cdot u$
2. $(k \cdot l) \cdot u = k \cdot (l \cdot u)$
3. $(k + l) \cdot v = k \cdot v + l \cdot v$
4. $1 \cdot v = v$,

gde je $u, v \in V$ i $k, l \in K$ i 1 jedinični element u K. Tada je V **levi vektorski prostor** nad telom K.
Ako je $\cdot : V \times K \to V$ preslikavanje takvo da je

1. $(v + u) \cdot k = v \cdot k + u \cdot k$
2. $u \cdot (k \cdot l) = (u \cdot k) \cdot l$
3. $v \cdot (k + l) = v \cdot k + v \cdot l$
4. $v \cdot 1 = v$,

gde $u, v \in V$ i $k, l \in K$ i 1 jedinični element u K, onda je V **desni vektorski prostor** nad telom K.

Ako je K polje, odnosno množenje je komutativno, prethodne dve definicije se ne razlikuju i tada jednostavno kažemo da je V vektorski prostor nad poljem K.

Navešećemo nekoliko definicija vezanih za leve vektorske prostore. Odgovarajuće definicije za desne vektorske prostore formulišu se u analogiji sa njima.

Neka je V levi vektorski prostor nad telom K. Vektor $\alpha_1 v_1 + \cdots + \alpha_n v_n, v_i \in V, \alpha_i \in K$ je **linearna kombinacija** vektora $v_1, \ldots, v_n$. Vektori $v_1, \ldots, v_n$ su **linearno nezavisni** ako jednačina $\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$ ima po α_i samo trivijalno rešenje $\alpha_1 = \cdots = \alpha_n = 0$. Vektori $v_1, \ldots, v_n$ **generišu** prostor V, odnosno čine njegovu **generatrisu** ako se svi njegovi elementi mogu predstaviti kao linearne kombinacije $v_1, \ldots, v_n$. Generatrisa čiji su elementi linearno nezavisni naziva se **bazom** tog prostora. Svake dve baze imaju isti broj elemenata i taj broj nazivamo **dimenzijom** tog prostora.

Neka su V_1 i V_2 dva leva vektorska prostora nad telom K. Preslikavanje $f : V_1 \to V_2$ je **homomorfizam** ako je $(\alpha_1 v_1 + \alpha_2 v_2)^f = \alpha_1 v_1^f + \alpha_2 v_2^f, \alpha_1, \alpha_2 \in K, v_1, v_2 \in V_1$. Ako je, pri tom, f bijekcija tada kažemo da je f **izomorfizam**.

Svi levi vektorski prostori dimenzije n nad telom K su izomorfni.

Svi vektorski prostori dimenzije n nad poljem K su izomorfni.

Neka su V i W levi vektorski prostori nad telom K i α automorfizam od K. Ako je $\phi : V \to W$ preslikavanje takvo da

1. $\forall v_1, v_2 \in V : (v_1 + v_2)^\phi = v_1^\phi + v_2^\phi$
2. $\forall v \in V, k \in K : (kv)^\phi = k^\alpha (v^\phi)$

onda je ϕ **semi-linearna transformacija** iz V u W sa pridruženim automorfizmom α. Očigledno je semi-linearna transformacija sa pridruženim identitetom tela K homomorfizam. Tada ϕ nazivamo još i **linearnom transformacijom**.

Sada, posmatrajmo semi-linearne transformacije levog vektorskog prostora V na sebe samog; dobijamo zatvoren skup. Ako su ϕ_1 i ϕ_2 semi-linearne transformacije sa pridruženim automorfizmima α_1 i α_2, onda je $\phi_1\phi_2$ definisano sa: $v^{\phi_1\phi_2} = (v^{\phi_1})^{\phi_2}$ i ima pridruženi automorfizam $\alpha_1\alpha_2$. Semi-linearna transformacija iz V u V je ne-singularna ako je $1-1$ i na. Skup ne-singularnih semi-linearnih transformacija obrazuje grupu $\Gamma L(V)$.

Teorema 1.5 *Jezgro J slabog kvazipolja W je telo. Štaviše, W se može smatrati desnim vektorskim prostorom nad J.*

Teorema 1.6 *Neka je W slabo kvazipolje sa jezgrom J. Ako je W konačno dimenzioni vektorski prostor nad nekim pod-telom H od J onda je W kvazipolje.*

Primer 1.1 Neka je $H = \{a1 + bi + cj + dk | a, b, c, d \in \mathbb{R}\}$. Za svaka dva elementa $q_1 = a_1 1 + b_1 i + c_1 j + d_1 k$ i $q_2 = a_2 1 + b_2 i + c_2 j + d_2 k$ skupa H

definišemo binarnu operaciju $+$ na sledeći način:

$$\begin{aligned} q_1 + q_2 &= (a_1 1 + b_1 i + c_1 j + d_1 k) + (a_2 1 + b_2 i + c_2 j + d_2 k) \\ &= (a_1 + a_2)1 + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k. \end{aligned}$$

Nazivamo je *sabiranjem* u skupu H. Uređeni par $(H, +)$ je *grupoid*. Operacija $+$ je asocijativna jer se asocijativnost operacije $+$ svodi na asocijativnost sabiranja u skupu $\mathbb{R}$. Naime, iz definicije operacije $+$ sledi:

$$\begin{aligned} &(q_1 + q_2) + q_3 = \\ &((a_1 + a_2)1 + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k) + (a_3 1 + b_3 i + c_3 j + d_3 k) = \\ &((a_1 + a_2) + a_3)1 + ((b_1 + b_2) + b_3)i + ((c_1 + c_2) + c_3)j + ((d_1 + d_2) + d_3)k = \\ &(a_1 + (a_2 + a_3))1 + (b_1 + (b_2 + b_3))i + (c_1 + (c_2 + c_3))j + (d_1 + (d_2 + d_3))k = \\ &(a_1 1 + b_1 i + c_1 j + d_1 k) + ((a_2 + a_3)1 + (b_2 + b_3)i + (c_2 + c_3)j + (d_2 + d_3)k) = \\ &q_1 + (q_2 + q_3) \end{aligned}$$

odakle sledi da je $(H, +)$ *polugrupa*. Na osnovu definicije sabiranja kvaterniona sledi da je njen neutral element $01 + 0i + 0j + 0k$, a kvaternion $-q = -a1 - bi - cj - dk$ nazivamo inverzom kvaterniona $q = a1 + bi + cj + dk$. Kako se komutativnost operacije sabiranja kvaterniona svodi na komutativnost sabiranja u skupu $\mathbb{R}$, time smo dokazali da je algebarska struktura $(H, +)$ *Abelova grupa*.

Sada možemo definisati i jednu spoljnu $\mathbb{R}$-operaciju $*$ na skupu H tako da za svako $\alpha \in \mathbb{R}$ i svako $q \in H$ važi

$$\alpha * q = (\alpha a)1 + (\alpha b)i + (\alpha c)j + (\alpha d)k. \tag{1}$$

Tako definisanu spoljnu $\mathbb{R}$-operaciju zovemo *množenje skalarima*. Dakle, struktura $(H, +, *)$ postaje jedan vektorski prostor nad poljem $\mathbb{R}$ koji ćemo obeležavati sa $\mathbb{H} = (H, +, *)$. Prema definiciji strukture $\mathbb{H}$ sledi da se svaki element $a1 + bi + cj + dk \in H$ može na jedinstven način zapisati kao linearna kombinacija elemenata $1, i, j, k$. To upravo znači da je skup $\{1, i, j, k\}$ i jedna baza vektorskog prostora $\mathbb{H}$. Tada skup realnih brojeva identifikujemo sa skupom $\{a1 | a \in \mathbb{R}\}$, a element $a1 + bi + cj + dk$ zapisujemo i kao $a + bi + cj + dk$.

Množenje $\cdot$ na skupu H uvodimo kao distributivnu operaciju, koja je na baznim vektorima data sledećom tablicom množenja

·	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1,

dok je $(\alpha * q_1) \cdot q_2 = \alpha * (q_1 \cdot q_2) = q_1 \cdot (\alpha * q_2), q_1, q_2 \in \mathbb{H}, \alpha \in \mathbb{R}$.

Element 1 je neutral množenja, a direktnom proverom zaključujemo da je množenje na skupu H asocijativno. Za proizvoljna dva elementa $q_1, q_2 \in H$ dobijamo

$$\begin{aligned} q_1 &= (a_1 + b_1 i + c_1 j + d_1 k), \quad q_2 = (a_2 + b_2 i + c_2 j + d_2 k) \\ q_1 \cdot q_2 &= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2)i \\ &\quad + (a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2)j + (a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2)k. \end{aligned}$$

Dakle $(H, +, \cdot)$ je prsten, a njegove elemente nazivamo **kvaternionima**.

Množenje na skupu H nije komutativno, npr. $i \cdot j = -j \cdot i = k$.

Slično skupu kompleksnih brojeva i u skupu H možemo definisati operaciju konjugovanja kvaterniona. Neka je $q = a + bi + cj + dk$ proizvoljan kvaternion iz skupa H. Tada njegov konjugat definišemo sa $\bar{q} = a - bi - cj - dk$. Pri tom važi $\bar{\bar{q}} = q$. Važi sledeća lema:

Lema 1.3 Neka su $q_1 = a_1 + b_1 i + c_1 j + d_1 k$ i $q_2 = a_2 + b_2 i + c_2 j + d_2 k$ dva proizvoljna kvaterniona iz skupa H. Tada važi:

$$\overline{q_1 + q_2} = \overline{q_1} + \overline{q_2} \qquad i \qquad \overline{q_1 \cdot q_2} = \overline{q_2} \cdot \overline{q_1}.$$

Dokaz: Na osnovu definicije sabiranja kvaterniona imamo

$$\begin{aligned}
\overline{q_1 + q_2} &= \overline{(a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k)} \\
&= \overline{(a_1 + a_2)1 + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k} \\
&= (a_1 + a_2)1 - (b_1 + b_2)i - (c_1 + c_2)j - (d_1 + d_2)k \\
&= (a_1 - b_1 i - c_1 j - d_1 k) + (a_2 - b_2 i - c_2 j - d_2 k) \\
&= \overline{q_1} + \overline{q_2}.
\end{aligned}$$

Slično se dokazuje i druga relacija

$$\begin{aligned}
\overline{q_1 \cdot q_2} &= \overline{(a_1 + b_1 i + c_1 j + d_1 k) \cdot (a_2 + b_2 i + c_2 j + d_2 k)} \\
&= \overline{(a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2)i} \\
&+ \overline{(a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2)j + (a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2)k} \\
&= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) - (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2)i \\
&- (a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2)j - (a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2)k.
\end{aligned}$$

S druge strane važi

$$\begin{aligned}
\overline{q_2} \cdot \overline{q_1} &= (a_2 - b_2 i - c_2 j - d_2 k) \cdot (a_1 - b_1 i - c_1 j - d_1 k) \\
&= (a_2 a_1 - b_2 b_1 - c_2 c_1 - d_2 d_1) - (a_2 b_1 + b_2 a_1 + c_2 d_1 - d_2 c_1)i \\
&- (a_2 c_1 - b_2 d_1 + c_2 a_1 + d_2 b_1)j - (a_2 d_1 + b_2 c_1 - c_2 b_1 + d_2 a_1)k.
\end{aligned}$$

Kako su desne strane ovih jednakosti jednake, sledi da su i leve strane jednake. ∎

Neka je $q = a + bi + cj + dk$ proizvoljan kvaternion i $\bar{q} = a - bi - cj - dk$ njemu konjugovani kvaternion. Množenjem ova dva kvaterniona

$$q \cdot \bar{q} = (a + bi + cj + dk) \cdot (a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2$$

dobijamo da je taj broj realan i nenegativan. Stoga možemo govoriti i o normi kvaterniona

$$|q| = \sqrt{q\overline{q}} = \sqrt{a^2 + b^2 + c^2 + d^2}.$$

Na osnovu definicije norme kvaterniona sledi da važi

$$|\overline{q}| = \sqrt{\overline{q}\,\overline{\overline{q}}} = \sqrt{\overline{q}q} = \sqrt{a^2 + b^2 + c^2 + d^2} = |q|,$$

kao i

$$|q\overline{q}| = \sqrt{(q\overline{q})\overline{(q\overline{q})}} = \sqrt{(q\overline{q})(q\overline{q})} = \sqrt{(q\overline{q})}\sqrt{(q\overline{q})} = |q||q| = |q|^2 = |q||\overline{q}|.$$

Koristeći konjugaciju i normu kvaterniona možemo da definišemo *inverz* kvaterniona. Proizvod nenula kvaterniona i inverza treba da bude jednak 1, pa je inverz kvaterniona q dat sa

$$q^{-1} = \frac{\overline{q}}{|q|^2}.$$

Ovim smo dokazali da je struktura $(H\diagdown\{0\}, \cdot)$ jedna grupa. Ova grupa nije Abelova, jer operacija $\cdot$ nije komutativna. Dakle, algebarska struktura $(H, +, \cdot)$ je nekomutativno polje, odnosno telo.

Uočimo sledeće. Kompleksne brojeve $\mathbb{C}$ možemo identifikovati sa $\mathbb{R}^2$ gde je element $i = (0, 1)$ i pišemo $(a, b) = a + bi, a, b \in \mathbb{R}$. Sabiranje je definisano kao standardno sabiranje na Dekartovom proizvodu, a množenje se sa $\mathbb{R}$ distributivno proširuje na $\mathbb{C}$ sa $i^2 = -1$.

Slično, kvaternione možemo predstaviti kao $\mathbb{H} = \mathbb{C}^2 = \mathbb{C}\times\mathbb{C} = \{(x, y)|x, y \in \mathbb{C}\}$ gde je $j = (0, 1)$, a element tog skupa je $(a, b) = a + bj, a, b \in \mathbb{C}$. Sabiranje je definisano kao standardno sabiranje Dekartovog proizvoda, a množenje se sa $\mathbb{C}$ distributivno proširuje uz uslov $j^2 = -1$. Konjugovanje je tada dato sa $\overline{a + bj} = \overline{a} - bj$.

$\diamond$

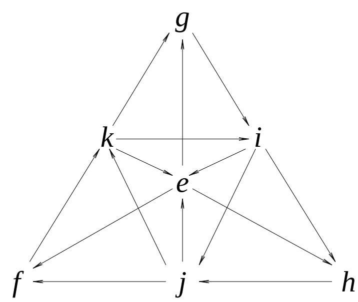
Primer 1.2

Slično kao u prethodnom primeru definišemo skup **oktoniona** kao skup $O = H^2 = H \times H = \{(x, y)|x, y \in H\}$. Svaki oktonion je oblika $\xi = x + ye$ gde su x, y kvaternioni i $e = (0, 1)$. Sabiranje je definisano kao sabiranje Dekartovog proizvoda. Kako je $(H, +)$ Abelova grupa, sledi i da je $(H^2, +)$ Abelova grupa kao i vektorski prostor nad $\mathbb{R}$.

Definišimo množenje na skupu O. Označimo $f = ie,\ g = je,\ h = ke$. Uz uslov da je množenje distributivno u odnosu na sabiranje i da važi $\alpha(\xi_1\xi_2) = (\alpha\xi_1)\xi_2 = \xi_1(\alpha\xi_2), \alpha \in \mathbb{R}, \xi_1, \xi_2 \in O$ množenje oktoniona je na jedinstven način zadato sledećom tablicom

$\cdot$	1	i	j	k	e	f	g	h
1	1	i	j	k	e	f	g	h
i	i	-1	k	$-j$	f	$-e$	h	$-g$
j	j	$-k$	-1	i	g	$-h$	$-e$	f
k	k	j	$-i$	-1	$-h$	$-g$	f	e
e	e	$-f$	$-g$	h	-1	i	j	$-k$
f	f	e	h	g	$-i$	-1	$-k$	$-j$
g	g	$-h$	e	$-f$	$-j$	k	-1	i
h	h	g	$-f$	$-e$	k	j	$-i$	$-1.$

Na slici 1.1 grafički su prikazani međusobni proizvodi baznih elemenata.



Sl. 1.1

Pored trojki koje su ilustrovane kao kolinearne, smatramo i da su i, j, k u istoj relaciji. Tada, proizvod dva elementa jednak je preostalom elementu sa odgovarajuće prave, a znak zavisi od orijentacije prave. Na primer, $jf = h$, a $ej = -g$, $ji = -k$. Element 1 je neutral za množenje. Uočimo, operacija $\cdot$ nije asocijativna, na primer $(ie)g = fg = -k$, a $i(eg) = ij = k$, a takođe operacija $\cdot$ nije ni komutativna jer $ij = -ji$.
Konjugovanje uvodimo analogno sa prethodnim primerima. Pomoću njega lako se dobija da jednačine $\xi_1 x = \xi_2$ i $y\xi_1 = \xi_2$ imaju jedinstvena rešenja po x i y, te je uređeni par $(O, \cdot)$ petlja. S obzirom da operacija množenja zadovoljava zakon distributivnosti struktura $\mathbb{O} = (O, +, \cdot)$ je prsten sa deljenjem.
Kako oktonioni nisu asocijativni, oni ne zadovoljavaju Lemu 2, pa $\mathbb{O}$ nije telo.

$\diamond$

1.2 Ternarni prsten

Neka je $\mathfrak{T}$ skup i $\mathbf{T}$ ternarna operacija definisana na skupu $\mathfrak{T}$. Uređeni par $(\mathfrak{T}, \mathbf{T})$ sa ternarnom operacijom se naziva **ternarni prsten**.
Ako postoje dva elementa ternarnog prstena, koje ćemo obeležiti sa 0 i 1, takvi da važi

T1 $\mathbf{T}(a, 0, c) = \mathbf{T}(0, b, c) = c, \ \forall a, b, c \in \mathfrak{T}$

T2 $\mathbf{T}(a, 1, 0) = \mathbf{T}(1, a, 0) = a, \ \forall a \in \mathfrak{T}$

T3 za sve $a, b, c, d \in \mathfrak{T}, a \neq c$ postoji jedinstveno $x \in \mathfrak{T}$ takvo da je $\mathbf{T}(x, a, b) = \mathbf{T}(x, c, d)$

T4 za sve $a, b, c \in \mathfrak{T}$ postoji jedinstveno $x \in \mathfrak{T}$ takvo da je $\mathbf{T}(a, b, x) = c$

T5 za sve $a, b, c, d \in \mathfrak{T}, a \neq c$ postoji jedinstven uređen par $(x, y) \in \mathfrak{T}$ takav da je $\mathbf{T}(a, x, y) = b$ i $\mathbf{T}(c, x, y) = d$

onda je $\mathfrak{T}$ **ravanski ternarni prsten**.

Uočimo da u ternarnom prstenu ne moraju biti definisane binarne operacije sabiranja i množenja. Ipak ako je $\mathfrak{T}$ ravanski ternarni prsten tada na prirodan način možemo definisati ove dve operacije, i to na sledeći način. Za $a, b \in \mathfrak{T}$ definišemo

$$a + b = \mathbf{T}(1, a, b) \quad \text{i} \quad a \cdot b = \mathbf{T}(a, b, 0).$$

Teorema 1.7 *Ako je $\mathfrak{T}$ ravanski ternarni prsten, onda su $(\mathfrak{T},+)$ i $(\mathfrak{T}^*,\cdot)$ petlje sa jediničnim elementima 0 i 1, gde je $\mathfrak{T}^*$ skup nenula elemenata iz $\mathfrak{T}$.*

Dokaz: Dokažimo prvo da je $(\mathfrak{T},+)$ petlja.

Za bilo koje $a \in \mathfrak{T}$, $0+a = \mathbf{T}(1,0,a) = a$ i $a+0 = \mathbf{T}(1,a,0) = a$ na osnovu svojstava T2. i T1. ternarne operacije, pa je 0 neutral za sabiranje.

Jednačina $a+x=b$ ima jedinstveno rešenje po x ako i samo ako $\mathbf{T}(1,a,x)=b$ ima jedinstveno rešenje po x. Ovo važi na osnovu svojstva T4.
Jednačina $x+a=b$ ima jedinstveno rešenje po x ako i samo ako $\mathbf{T}(1,x,a)=b$ ima jedinstveno rešenje po x. Na osnovu svojstva T5. postoji jedinstven uređeni par x,y takav da je $\mathbf{T}(1,x,y)=b$ i $\mathbf{T}(0,x,y)=a$. Na osnovu svojstva T1, $\mathbf{T}(0,x,y)=a$ ima $y=a$ za rešenje, pa postoji jedinstveno x takvo da je $\mathbf{T}(1,x,a)=b$. Dakle, $(\mathfrak{T},+)$ je petlja.

Pokažimo da je $(\mathfrak{T}^*,\cdot)$ petlja. Važi da je $1\cdot x = \mathbf{T}(1,x,0) = x$ i $x \cdot 1 = \mathbf{T}(x,1,0) = x$ na osnovu svojstva T2, pa je 1 jedinični element u $(\mathfrak{T}^*,\cdot)$.
Takođe treba pokazati i da je operacija $\cdot$ zatvorena u skupu $\mathfrak{T}^*$. Pretpostavimo da je $x\cdot y = 0$ i $y \neq 0$. Jednačina $T(u,y,0) = T(u,0,0)$ ima jedinstveno rešenje po u koje je očigledno $u=0$. Kako važi $T(x,y,0) = 0 = T(x,0,0)$ onda je rešenje po x, $x=0$. Zato je operacija množenja zatvorena u skupu $\mathfrak{T}^*$.

Jednačina $a\cdot x = b$ ima jedinstveno rešenje za x ako i samo ako $\mathbf{T}(a,x,0)=b$ ima jedinstveno rešenje za x. Na osnovu svojstva T5 važi

$$\mathbf{T}(a,x,y) = b, \quad \mathbf{T}(0,x,y) = 0. \tag{2}$$

Kako druga jednakost (2) povlači da je $y=0$, onda $\mathbf{T}(a,x,0)=b$ ima jedinstveno rešenje po x.
Jednačina $x\cdot a = b$ ima jedinstveno rešenje za x ako i samo ako $\mathbf{T}(x,a,0)=b$ ima jedinstveno rešenje za x. Na osnovu svojstva T3 $\mathbf{T}(x,a,0) = \mathbf{T}(x,0,b)$ ima jedinstveno rešenje po x (jer je $a \neq 0$), a na osnovu T1 $\mathbf{T}(x,0,b) = b \ \ \forall x$, pa $\mathbf{T}(x,a,0)=b$ ima jedinstveno rešenje po x i $(\mathfrak{T}^*,\cdot)$ je petlja. ∎

Neka je K levo ili desno kvazipolje. Tada ternarnu operaciju $(a,x,b) = [ax+b]$ možemo definisati sa $[ax+b] = ax+b$ i pokazaćemo da je K sa ovom ternarnom operacijom i elementima $0,1$ ternarni prsten.

Pokažimo da je svako levo kvazipolje ternarni prsten sa nulom i jedinicom.

- T1 važi na osnovu 3. osobine levog kvazipolja.
- T2 takođe važi na osnovu 3. osobine levog kvazipolja.
- T3 neka su $a,b,a',b' \in K$ i $a \neq a'$ pa je $xa+b = xa'+b'$ pa na osnovu 1. osobine levog kvazipolja ovo je ekvivalentno sa $ax = a'x + (b-b')$, a po 5. osobini levog kvazipolja ova jednačina ima jedinstveno rešenje.
- T4 sledi iz 1. osobine levog kvazipolja.
- T5 neka su $x,y,x',y' \in K$ i $x \neq x'$. Jednačine $y = ax+b$ i $y' = ax'+b$ za a,b postaju
$$y - y' = ax - ax'$$

na osnovu 1. osobine levog kvazipolja i

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

na osnovu 4. osobine levog kvazipolja. Ako je $y \neq y'$ jednačina je rešiva po a na osnovu 2. osobine levog kvazipolja. Ako znamo a onda lako možemo izračunati b iz jednačina $y = ax + b$ i $y' = ax' + b$. Jasno, b je jedinstveno. Ovo dokazuje T5 za slučaj $y \neq y'$.
Ako je $y = y'$ onda $a = 0$ na osnovu 2. osobine levog kvazipolja (jer je $x - x' \neq 0$). Odatle, $b = y = y'$. Ovo dokazuje T5 za slučaj $y = y'$.

2 Afine ravni

2.1 Tri aksiome afinih ravni. Preslikavanja

U ovom poglavlju uvešećemo pojam afinih ravni i predstaviti za njih karakteristična preslikavanja.

Data su nam dva osnovna pojma: skup čije elemente nazivamo "tačkama" i klasu njegovih podskupova koje nazivamo "pravama". Ukoliko tačka P pripada pravoj p, kažemo i da su P i p incidentni. Prva aksima koju ovi skupovi treba da ispunjavaju je sledeća:

Aksioma 1 Neka su date dve različite tačke P i Q. Tada postoji jedinstvena prava l koja sadrži obe tačke P i Q.
Za takvu pravu l koristićemo zapis $l = P + Q$.

Definicija 2.1 Ako su l i m dve prave takve da je ili $l = m$ ili prave l i m ne sadrže nijednu zajedničku tačku, onda kažemo da su one paralelne i pišemo $l \parallel m$.

Ako $l \nparallel m$, onda postoji tačno jedna tačka P koja pripada i l i m. Ako bi postojale dve takve tačke onda bi po prethodnoj aksiomi $l = m$ i to znači da je $l \parallel m$ što je suprotno od onoga što smo pretpostavili. U ovom slučaju kažemo da se l i m seku u P.

Aksioma 2 Neka su date tačka P i prava l. Tada postoji jedna i samo jedna prava m koja prolazi kroz tačku P i paralelna je pravoj l.

Teorema 2.1 *Relacija paralelnosti pravih je relacija ekvivalencije.*

Dokaz: Očigledno je da je ta relacija simetrična ($l_1 \parallel l_2 \Rightarrow l_2 \parallel l_1$) i refleksivna ($l_1 \parallel l_1$), treba dokazati da je tranzitivna. Pretpostavimo da je $l_1 \parallel l_2$ i $l_2 \parallel l_3$. Ako ne postoji tačka koja pripada obema pravama l_1 i l_3 onda je $l_1 \parallel l_3$. Ako postoji tačka P koja pripada obema pravama l_1 i l_3, onda je $l_1 = l_3$ po aksiomi 2 i zato što je $l_1 \parallel l_2$ i $l_2 \parallel l_3$, pa opet $l_1 \parallel l_3$. ∎

Definicija 2.2 Klasa ekvivalencije paralelnih pravih se naziva pramenom paralelnih pravih.

Teorema 2.2 *Pretpostavimo da postoje tri različita pramena paralelnih pravih π_1, π_2, π_3. Tada su svi pramenovi te ravni iste kardinalnosti k, a tada je i sa proizvoljnom pravom te ravni incidentno k tačaka.*

Dokaz: Neka je l prava pramena π_1, m prava pramena π_2. Tada, kako $l \nparallel m$, postoji tačno jedna tačka P koja pripada obema pravama l i m. Neka je Q proizvoljna tačka na pravoj l. Tada postoji tačno jedna prava m' koja je paralelna sa m i sadrži tačku Q, sledi da $m' \in \pi_2$. Dakle, postoji $1-1$ preslikavanje između tačaka prave l i pravih pramena π_2: broj tačaka prave l jednak je broju pravih pramena π_2. Dokazali smo da ako su data dva različita pramena onda svaka prava jednog pramena sadrži onoliko tačaka koliko je pravih u drugom pramenu. Ako je π proizvoljan pramen, onda je on različit od najmanje dva od data tri pramena; neka je $\pi \neq \pi_1$ i $\pi \neq \pi_2$. Broj tačaka na proizvoljnoj pravoj iz pramena π_1 jednak je broju pravih iz pramena π i jednak je broju pravih iz pramena π_2. Odavde lako sledi tvrđenje teoreme. ∎

Navedimo sada i treću aksiomu.

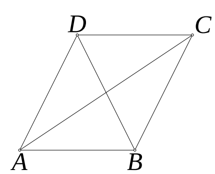
Aksioma 3 Postoje tri različite tačke A, B i C takve da tačka C ne pripada pravoj $A + B$. Kažemo da postoje tri nekolinearne tačke.

Prave $A+B$ i $A+C$ nisu paralelne jer imaju bar jednu zajedničku tačku A, a tada bi A, B i C pripadale istoj pravoj. Zato $A+B \nparallel B+C$ i $A+C \nparallel B+C$. To znači da sada postoje tri različita pramena paralelnih pravih i Teorema 2.2 važi.

Ukoliko skup tačaka i pravih zadovoljavaju tri gore navedene aksiome, onda kažemo da te tačke čine afinu ravan.

Primer 2.1 Uočimo da $\mathbb{R}^2$ tj. skup uređenih parova realnih brojeva, gde je prava skup tačaka (x, y) takvih da $ax + by + c = 0$ zadovoljava askiome.

Primer 2.2 Primer afine ravni sa konačnim brojem tačaka je Fanoova ravan. Ova ravan se sastoji od četiri tačke i šest pravih, pri čemu svaka prava sadrži tačno dve tačke (slika 2. 1).



Sl. 2.1

Ovim tačakama možemo pridužiti koordinate $(0:0), (0:1), (1:0), (1:1)$ odnosno reći da su njene koordinate iz polja $\mathbb{Z}_2$.

Definišimo sada i preslikavanja koja odgovaraju afinoj geometriji ravni, odnosno ona koja "čuvaju" invarijante afine geometrije ravni.

Definicija 2.3 Preslikavanje dve afine ravni koje preslikava kolinearne tačke u kolinearne, odnosno "čuva" relaciju incidencije naziva se kolineacija. Ukoliko je pri tom i bijekcija zovemo je i izomorfizam.

Navedimo sada i jednu vrstu kolineacija afine ravni.

Definicija 2.4 Preslikavanje σ afine ravni (koje tačke slika u tačke) naziva se **dilatacija** ako zadovoljava sledeće svojstvo: neka su P i Q proizvoljne dve razne tačke, a njihove slike P' i Q'; ako je prava l' paralelna sa pravom $P+Q$ i sadrži tačku P', onda tačka Q' pripada pravoj l'.

Primer 2.3

a) Preslikavanje u kom se sve tačke slikaju u neku fiksnu tačku. Za takvu dilataciju kažemo da je degenerisana. U suprotnom je nedegenerisana.

b) Identitet.

Primer 2.4 Primeri dilatacije u afinoj ravni $\mathbb{R}^2$ su sledeća preslikavanja.

a) $(x, y) \mapsto (x + a, y + b)$ gde su $a, b \in R$. Zove se translacija realne ravni za (a, b).

b) $(x, y) \mapsto ((1 - \lambda)a + \lambda x, (a - \lambda)b + \lambda y), a, b, \lambda \in R$. Ovo preslikavanje je homotetija realne ravni sa centrom (a, b) i koeficijentom λ.

Primer 2.5 Jedan primer dilatacije u Fanoovoj ravni je dat sa

$$f : \begin{pmatrix} A & D & B & C \\ D & A & C & B \end{pmatrix}.$$

Teorema 2.3 *Dilatacija σ je jednoznačno određena slikama P' i Q' dve razne tačke P i Q.*
Ako je $P' = Q'$ onda je σ degenerisana dilatacija i sve tačke se slikaju u P'.
Ako je $P' \neq Q'$ onda je σ bijekcija.

Dokaz: Treba pokazati da je za svaku tačku ravni njena slika određena na jedinstven način slikama tačaka P i Q.
Neka je, zato, prvo R proizvoljna tačka ravni koja ne pripada pravoj $P + Q$. Tada su $R + P$ i $R + Q$ dve neparalelne prave. Neka su l_1 i l_2 prave redom incidentne sa tačkama P' i Q' i paralelne $R + P$ i $R + Q$. Tada su i l_1 i l_2 neparalelne i imaju tačno jednu zajedničku tačku, a pri tom obe sadrže sliku tačke R. Tada je slika tačke R jedinstveno određena. Pri tom, ako je $P' = Q'$, prave l_1 i l_2 seku se u toj tački pa je i $R' = P'$.
Ako tačka R pripada pravoj $P + Q$, $R \neq P$, neka je S tačka koja ne pripada pravoj $P + Q$. Tada su P, S, R tri nekolinearne tačke. S obzirom da je slika tačke S određena na jedinstven način, ponavljajući postupak za tačke P, S i R zaključujemo da je slika tačke R jedinstveno određena. Pri tom, ako je $P' = Q'$ tada je i $P' = S'$, pa i $R' = P'$.
Dakle, ako se slike dve tačke poklapaju, onda se sve tačke ravni slikaju u istu tačku. Zato, ukoliko se za neke dve razne tačke P i Q njihove slike P' i Q' razlikuju, onda će se razlikovati i slike bilo kog drugog para različitih tačaka. Tada je preslikavanje injektivno.
Pokažimo da je tada preslikavanje i surjektivno. Ako je R' proizvoljna tačka ravni koja ne pripada pravoj $P' + Q'$, prave $P' + R'$ i $Q' + R'$ su neparalelne. Ako su p_1 i p_2 prave njima paralelne, a redom, incidentne sa P i Q, tada se p_1 i p_2 seku u tački koja se ovim preslikavanjem slika u R'. Ako tačka R' pripada pravoj $P' + Q'$, $R' \neq P'$, neka je S' tačka van te prave i S njen original. Ponavljajući prethodni postupak sa tačkama P', S' i R' dobijamo tačku koja se preslikala u R'. ∎

Posledica 1 Ako dilatacija σ ima dve fiksne tačke, onda je σ identitet, što ćemo zapisivati $\sigma = 1$.

Definicija 2.5 Neka je σ nedegenerisana dilatacija i P neka tačka. Svaka prava koja sadrži P i σP naziva se trag tačke P.
Ako je $P \neq \sigma P$ onda je trag tačke P jedinstveno određen, i to je prava $P + \sigma P$.

Teorema 2.4 *Neka je σ nedegenerisana dilatacija, P proizvoljna tačka i l trag tačke P. Ako tačka Q pripada pravoj l onda i tačka σQ pripada pravoj l.*

Dokaz: Možemo pretpostaviti da je $Q \neq P$ tako da je $l = P + Q$. Tada je $\sigma Q \neq \sigma P$ i $\sigma P + \sigma Q \parallel l$ po definiciji dilatacije. Međutim, prave l i $\sigma P + \sigma Q$ imaju zajedničku tačku σP, to znači da se poklapaju. Sledi, σQ pripada pravoj l. ∎

Znači, ako je prava l trag neke (svoje) tačke, onda je ujedno i trag svih svojih tačaka.

Neka se dva razna traga l_1 i l_2 seku u tački S. Tada su i l_1 i l_2 tragovi tačke S pa je ona fiksna tačka preslikavanja. Zato je i bilo koja druga prava incidentna sa S trag. Pretpostavimo da postoji trag l_3 koji nije incidentan sa S. Tada l_3 seče bar jednu od pravih l_1 i l_2, recimo l_1 u tački M, i pretpostavimo $M \neq S$, a tada je i M fiksna tačka preslikavanja, a dilatacija sa bar dve fiksne tačke je identitet. Tada je svaka prava ravni trag. Ako dilatacija nije identičko preslikavanje, sledi da l_3 mora biti incidentna sa S.

Sa druge strane, ako su neka dva traga neidentičke dilatacije paralelna onda svi tragovi pripadaju istom pramenu paralelnih pravih. Tada preslikavanje nema fiksnih tačaka. Dakle, zaključujemo sledeće.

Neka je σ nedegenerisana dilatacija:

1. Sve prave ravni su trag neke njene tačke ako i samo ako je $\sigma = 1$.
2. Ako je $\sigma \neq 1$ tada je skup svih tragova te dilatacije pramen pravih koje se seku u datoj tački P ako i samo ako je P fiksna tačka dilatacije σ.
3. Ako je $\sigma \neq 1$ tada je skup svih tragova te dilatacije pramen paralelnih pravih ako i samo ako dilatacija σ nema fiksne tačke.

Definicija 2.6 Nedegenerisana dilatacija τ naziva se **translacija** ako je ili $\tau = 1$ ili τ nema fiksnu tačku. Ako je τ translacija koja nije identitet ($\tau \neq 1$) onda tragovi translacije τ formiraju pramen π paralelnih pravih koji nazivamo "smerom" translacije τ.

Primer 2.6 Primetimo da su translacije realne ravni translacije i po ovoj definiciji.

Primer 2.7 Preslikavanje dato u Primeru 5 je translacija Fanoove ravni.

Teorema 2.5 *Translacija τ je jedinstveno određena slikom proizvoljne tačke P.*

Dokaz: Neka je l trag translacije τ koji sadrži tačku P. Svaka prava paralelna sa l takođe je trag preslikavanja τ; neka je $l' \parallel l, l' \neq l, Q$ tačka koja pripada l'.

Tada tačka τQ mora biti na l'. Neka je $m = P + Q$ i neka je m' prava paralelna pravoj m i koja sadrži tačku τP. Po definiciji dilatacije tačka τQ mora pripadati m'. Sada tačka τQ pripada obema pravama l' i m', pri čemu $l' \nparallel m'$ jer $l \nparallel m$. Tako je tačka τQ određena jednoznačno, a dilatacija je jednoznačno određena slikom dve tačke. ∎

Od sada ćemo pretpostaviti da je dilatacija nedegenerisana osim ako nije drugačije rečeno, odnosno, od sada pod dilatacijom podrazumevamo afinu transformaciju ravni takvu da važi: ako je $P \neq Q$ onda je $\sigma P \neq \sigma Q$ i $P{+}Q \parallel \sigma P{+}\sigma Q$. Neka su date dve dilatacije σ_1 i σ_2. Njihovu kompoziciju $P \mapsto \sigma_1(\sigma_2(P))$ obeležavamo sa $\sigma_1\sigma_2$.
Ako je $P \neq Q$ onda je $\sigma_2 P \neq \sigma_2 Q$, pa sledi da je $\sigma_1\sigma_2 P \neq \sigma_1\sigma_2 Q$ i $P + Q \parallel \sigma_2 P + \sigma_2 Q \parallel \sigma_1\sigma_2 P + \sigma_1\sigma_2 Q$. Zato je preslikavanje $\sigma_1\sigma_2$ je dilatacija.
Kako je σ bijekcija to je moguće formirati inverzno preslikavanje koje je takođe bijekcija. Ako je $P \neq Q$, onda $\sigma^{-1}P \neq \sigma^{-1}Q$ i

$$\sigma^{-1}P + \sigma^{-1}Q \parallel \sigma(\sigma^{-1}P) + \sigma(\sigma^{-1}Q) = P + Q,$$

a odavde sledi da je i σ^{-1} dilatacija. Dakle, važi sledeće tvrđenje.

Teorema 2.6 *Dilatacije afine ravni obrazuju grupu u odnosu na kompoziciju funkcija.*

Neka je τ translacija. Ako τ^{-1} nema fiksnih tačaka onda je ona translacija. Pretpostavimo da preslikavanje τ^{-1} ima fiksnu tačku P. Tada je $\tau^{-1}P = P$, pa i $P = \tau P$ što je moguće samo ako je $\tau = 1$, a u tom slučaju je i $\tau^{-1} = 1$ takođe translacija.
Neka su τ_1 i τ_2 translacije. Ako njihova kompozicija nema fiksnih tačaka, onda je u pitanju translacija. Pretpostavimo da njihova kompozicija ima fiksnu tačku, $\tau_1\tau_2 P = P$. Tada je $\tau_2 P = \tau_1^{-1}P$. Tada τ_2 i τ_1^{-1} na isti način preslikavaju tačku P, a kako je translacija na jedinstven način određena slikom jedne njene tačke sledi $\tau_2 = \tau_1^{-1}$. Tada je $\tau_1\tau_2 = 1$ translacija. Vidimo da je $\tau_1\tau_2$ translacija u bilo kom slučaju.

Teorema 2.7 *Translacije afine ravni obrazuju grupu, podgrupu grupe dilatacija afine ravni.*

Definicija 2.7 Grupu dilatacija označavamo sa $\mathbf{D}$, a grupu translacija sa $\mathbf{T}$.

Teorema 2.8 *Grupa $\boldsymbol{T}$ je normalna podgrupa grupe $\boldsymbol{D}$. Ako je σ dilatacija a τ translacija ($\tau \neq 1$), onda τ i $\sigma\tau\sigma^{-1}$ imaju isti smer.*

Dokaz: Pokažimo prvo da je $\sigma\tau\sigma^{-1} = \tau_1$ translacija.
Ako preslikavanje τ_1 ima fiksnu tačku P onda je $\sigma\tau\sigma^{-1}P = P$, a odatle sledi $\tau\sigma^{-1}P = \sigma^{-1}P$. Tačka $\sigma^{-1}P$ je fiksna tačka preslikavanja τ. Sledi $\tau = 1$, tj. $\tau_1 = 1$ je translacija.
Pretpostavimo sada da $\tau \neq 1$ i da je π smer preslikavanja τ. Prava $\sigma^{-1}P + \tau\sigma^{-1}P$ je τ-trag tačke $\sigma^{-1}P$ i prema tome to je prava pramena π. Pošto je σ dilatacija, onda $\sigma^{-1}P + \tau\sigma^{-1}P \parallel \sigma(\sigma^{-1}P) + \sigma\tau\sigma^{-1}P = P + \sigma\tau\sigma^{-1}P$. Prava $P + \sigma\tau\sigma^{-1}P$ takođe pripada pramenu π i ona je $\sigma\tau\sigma^{-1}$-trag tačke P. Odavde sledi da $\sigma\tau\sigma^{-1}$ takođe ima smer π. ∎

Teorema 2.9 *Translacije, određene datim smerom - pramenom paralelnih pravih π zajedno sa identitetom obrazuju grupu.*

Dokaz: Ako je $\tau \neq 1$ onda prava $P + \tau P = \tau P + \tau^{-1}\tau P$ je τ-trag tačke P i τ^{-1}-trag tačke τP. Ako translacije τ_1 i τ_2 ($\tau_1 \neq 1, \tau_2 \neq 1$) imaju pravac π, onda prava $P + \tau_2 P$ pripada pramenu π i sadrži tačku $\tau_2 P$. Po Teoremi 2.4 ona sadrži i tačku $\tau_1\tau_2 P$. Ako je $\tau_1\tau_2 P = P$, onda je $\tau_1\tau_2 = 1$; ako je $\tau_1\tau_2 P \neq P$ onda je prava $P + \tau_2 P = P + \tau_1\tau_2 P$ trag preslikavanja $\tau_1\tau_2$ i pripada pramenu π. ∎

Teorema 2.10 *Ako postoje translacije sa različitim smerovima onda je grupa **T** komutativna.*

Dokaz: Neka su τ_1 i τ_2 translacije u neparalelnim smerovima. Tada $\tau_1\tau_2\tau_1^{-1}$ i τ_2, kao i τ_2^{-1} imaju iste smerove. Pretpostavimo da translacija $\tau = \tau_1\tau_2\tau_1^{-1}\tau_2^{-1}$ nije identitet. Tada kao kompozicija $\tau_1\tau_2\tau_1^{-1}$ i τ_2^{-1}, τ ima smer kao i τ_2, a kao kompozicija τ_1 i $\tau_2\tau_1^{-1}\tau_2^{-1}$ ima isti smer kao i τ_1, što je kontradikcija. Zato je $\tau = 1$ i $\tau_2\tau_1 = \tau_1\tau_2$. Ako su τ_1 i τ_2 translacije istog smera, neka je τ_3 translacija nekog drugog smera. Tada τ_3 komutira sa τ_1 i τ_2. Pri tom $\tau_2\tau_3$ ima drugačiji smer od τ_2, a samim tim i od τ_1. Zato i $\tau_2\tau_3$ i τ_1 takođe komutiraju, pa važi

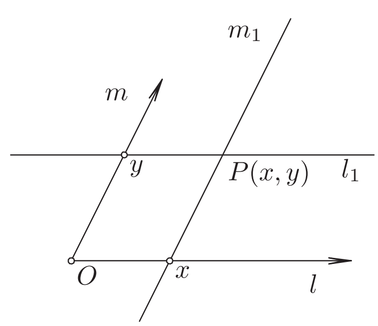
$$(\tau_1\tau_2)\tau_3 = \tau_1(\tau_2\tau_3) = (\tau_2\tau_3)\tau_1 = \tau_2(\tau_3\tau_1) = \tau_2(\tau_1\tau_3) = (\tau_2\tau_1)\tau_3$$

odakle sledi tvrđenje. ∎

2.2 Koordinatizacija afine ravni

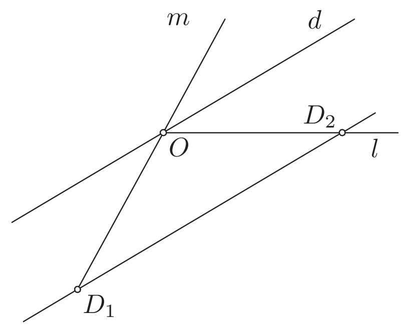
U ovom poglavlju ćemo pokazati kako u proizvoljnoj afinoj ravni možemo uvesti koordinate, odnosno jednoznačnu korespondenciju između tačaka te ravni i skupa $K^2 = K \times K$, gde je K ravanski ternarni prsten. Pokazaćemo da važi i obrnuto, odnosno da skup K^2 sa izvesnom klasom podskupova koji zovemo prave zadovoljava aksiome afine ravni. Tada za afinu ravan kažemo da je izgrađena nad K. Ispitaćemo takođe da li se jedna afina ravan moze izgraditi nad dva različita ternarna prstena.

Neka je A afina ravan i l i m njene dve prave koje se seku i koje nazivamo osama. Njihovu tačku preseka označimo sa O. Zvaćemo je nadalje koordinatnim početkom. Neka je P proizvoljna tačka ravni i l_1 i m_1 prave incidentne sa P i redom paralelne pravama l i m. Tačke preseka l i m_1, odnosno m i l_1 označimo redom sa x i y. Tački P pridružujemo uređen par (x, y).



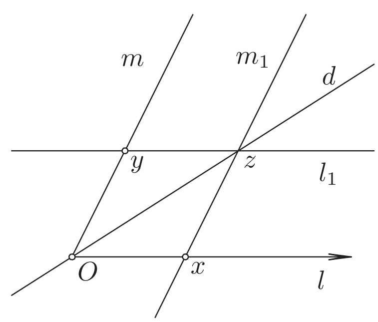
Sl. 2.2

Na ovaj način definišemo preslikavanje $\phi : A \to l \times m$. Obrnuto, svakom uređenom paru tačaka $(x, y) \in l \times m$ možemo pridružiti jedinstvenu tačku ravni u kojoj se seku prave incidentne sa tačkama x i y, a redom paralelne osama m i l. Time dobijamo preslikavanje $\psi : l \times m \to A$. Preslikavanja ϕ i ψ su očigledno, jedno drugom inverzna, x i y nazivamo kordinatama tačke P. Kako svaka prava sadrži više od jedne tačke postoje tačke D_1 i D_2 različite od O na osama l i m. Prava d_1 njima određena nije paralelna osama. Zato se prava incidentna sa O paralelna d_1 razlikuje od osa l i m. Dakle, postoji prava kroz O različita od l i m. Neka je d jedna takva prava.



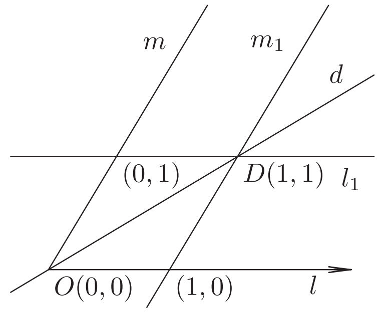
Sl. 2.3

Neka je x proizvoljna tačka ose l, z tačka u kojoj prava incidentna sa x i paralelna m seče d, a y tačka ose m u kojoj prava incidentna sa z a paralelna l seče m. Na ovaj način smo definisali bijekciju između osa l i m. S obzirom na ovu bijekciju identifikujemo tačke prave l i tačke prave m i tako dobijeni skup označimo sa K.



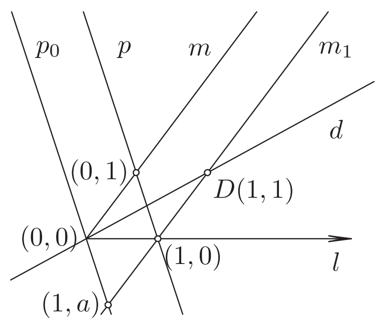
Sl. 2.4

Sada možemo da identifikujemo afinu ravan A sa skupom K^2. Pri tom, tačke prave d imaju koordinate $(x, x), x \in K$. Pokazaćemo da je skup K ternarni prsten, te da je afina ravan izgrađena nad ternarnim prstenom K. Iako još nismo definisali operacije u ovom skupu, formalno koordinatnom početku dodeljujemo koordinate $(0, 0)$. Neka je $D \in d$ proizvoljna, od sada fiksirana tačka različita od koordinatnog početka. Njene koordinate od sada nazivamo $(1, 1)$. Time su određene i tačke jedinica na osama l i m.



Sl. 2.5

Ako je prava afine ravni paralelna osi l kažemo da je nagiba 0, odnosno horizontalna. Ako je prava paralelna osi m, kažemo da je nagiba ∞, odnosno da je vertikalna. Neka je sada p proizvoljna prava, ni horizontalna, ni vertikalna, a p_0 njoj paralelna prava incidentna sa koordinatnim početkom. Prava p_0 seče vertikalnu pravu kroz $(1,0)$ u nekoj tački sa koordinatama $(1,a)$. Kažemo, onda, da je p prava nagiba a. Očigledno je da paralelne prave imaju iste nagibe, postoji jednoznačna korespondencija između klasa paralelnih pravih i skupa $K \cup \{\infty\}$, odnosno klasa paralelnih pravih koje nisu vertikalne i K. Ako p nije vertikalna prava, onda ona seče m u tački oblika $(0,b)$. Očigledno je p na jedinstven način određena koordinatom b i svojim nagibom a.



Sl. 2.6

Neka je $x \in K$ proizvoljno. Tada p seče vertikalnu pravu kroz x u tački (x,y) i uspostavlja preslikavanje $x \mapsto y$. Ovo preslikavanje koje koordinati x tačke prave p dodeljuje njenu y koordinatu tada možemo formalno označiti i sa $y = [ax+b]$ i reći da je prava l data ovom jednačinom. Za vertikalne prave ćemo tada reći da su date jednačinama oblika $x = c$ gde je $c \in K$.
Posmatrajmo ternarno preslikavanje $(a,x,b) \mapsto [ax+b]$ u skupu K.

Teorema 2.11 *Ternarni prsten K je ravanski ternarni prsten, odnosno, u njemu važi*

1. $[1x+0] = x = [x1+0]$
2. $[a0+b] = [0a+b] = b$
3. *za proizvoljne $a, x, y \in K$ postoji jedinstveno $b \in K$ takvo da je $[ax+b] = y$*
4. *ako su $a, a_1, b, b_1 \in K$ takvi da je $a \neq a_1$ tada jednačina $[ax+b] = [a_1x+b_1]$ ima jedinstveno rešenje $x \in K$*

5. *ako su* $x, x_1, y, y_1 \in K$ *takvi da je* $x \neq x_1$ *tada postoji jedinstveni par* $a, b \in K$ *takav da je* $[ax+b] = y$ *i* $[ax_1+b] = y_1$.

Dokaz:

1. $[1x+0] = x$ važi jer je d prava nagiba 1 incidentna sa koordinatnim početkom, a pri tom njene tačke su oblika $(x,x), x \in K$. S obzirom da je nagib prave kroz $(0,0)$ i $(1,x)$ jednak x, važi i $[x1+0] = x$.

2. Kako prava $y = [ax+b]$ sadrži tačku $(0,b)$ važi i $[a0+b] = b$, a kako horizontalna prava incidentna sa $(0,b)$ sadrži tačke oblika $(a,b), a \in K$ važi i $[0a+b] = b$.

3. Ako su $a, x, y \in K$, postoji jedinstvena prava incidentna sa (x,y) nagiba a, pa i jedinstveno $b \in K$ takvo da je $[ax+b] = y$.

4. S obzirom da se dve neparalelne prave seku u tačno jednoj tački sledi i da za $a \neq a_1$ jednačina $[ax+b] = [a_1x+b_1]$ ima tačno jedno rešenje po x.

5. Ako je $x \neq x_1$, sledi da tačke čije su ovo koordinate ne pripadaju istoj vertikalnoj pravoj. Ali tada postoji tačno jedna prava konačnog nagiba njima određena, odnosno postoji tačno jedan par $a, b \in K$ takav da je $y = [ax+b]$ i $y_1 = [ax_1+b]$.

∎

Dakle, u proizvoljnu afinu ravan uveli smo koordinate iz ternarnog prstena K.

Kako je K ravanski ternarni prsten, operacije sabiranja i množenja su u njemu date sa $a+b = [1a+b]$ i $a \cdot b = [ab+0]$ i pri tom $(K,+)$ i $(K \backslash \{0\}, \cdot)$ su petlje.

Učimo, međutim da ovakav ternarni prsten nije jedinstveno određen. Prilikom njegove konstrukcije izabrali smo par neparalelnih pravih l i m, zatim sa njima konkurentnu pravu d, a pomoću nje i tačke pravih l i m sa koordinatama 1. Ovaj poslednji izbor je ekvivalentan izboru tačke z koja nije incidentna sa pravama l i m i kojoj dodeljujemo koordinate $(1,1)$. Dakle, polje K je određeno izborom pravih l i m i tačke z.

Pokažimo da važi i obrnuto tvrđenje, odnosno da nad svakim ternarnim prstenom možemo izgraditi afinu ravan.

Teorema 2.12 *Neka je* K *ternarni prsten. Ako elemente skupa* K^2 *zovemo tačkama, dok podskupove oblika* $\{(x,y) | y = [ax+b]\}$ *pravama, tada ovi pojmovi zadovoljavaju aksiome afine ravni.*

Dokaz:

1. Neka su date tačke $P(x_1, y_1)$ i $Q(x_2, y_2)$, $P \neq Q$. Ako P i Q ne pripadaju vertikalnoj pravoj, tj. pravoj nagiba ∞, onda na osnovu uslova 5. postoji tačno jedna prava konačnog nagiba njima određena. Inače P i Q pripadaju vertikalnoj pravoj, dakle postoji prava njima odredjena.
   Ovim je dokazano da važi aksioma 1.

2. Razmataramo dva slučaja:

   1.1 Neka su date tačka $P \in l$: $P(x, y)$ i prava l: $y = [ax + b]$. Tada prava m koja sadrži tačku P ima oblik $y = [a_1x + b_1]$. Da bi $m \parallel l$ mora biti $a = a_1$, a kako $P \in l$ i $P \in m$, mora biti $[ax + b] = [a_1x + b_1]$ odnosno $[ax + b] = [ax + b_1]$ pa je i $b = b_1$. Tada prava m ima oblik $y = [ax + b]$ a to je upravo prava l koja je jedinstvena.

   1.2 Neka su date tačka $P \notin l$: $P(x, y)$ i prava l: $y_1 = [ax_1 + b]$. Tada prava m koja sadrži tačku P ima oblik $y = [a_1x + b_1]$ i $m \parallel l$ ako je $a_1 = a$. Dakle m: $y = [ax + b_1]$ je jedinstvena prava kroz P paralelna sa l.
   Ovim je dokazano da važi aksioma 2.

3. Da bismo dokazali da važi aksioma 3 pretpostavimo da su date tačka $A(0, 0), B(1, 0), C(0, 1)$ i treba pokazati da ove tri tačke nisu kolinearne. Na osnovu 5. sledi da postoji jedinstvena prava određena tačkama A i B, tj. da postoji tačno jedan par $(a, b) \in K^2$ takav da $0 = [a0 + b]$ i $0 = [a1 + b]$. Odavde dobijamo da je $b = 0, a = 0$. Da bi tačka C pripadala pravoj $A + B$ mora biti $1 = [a0 + b]$ odnosno $1 = [0 + 0]$ što je nemoguće, pa tačka C ne pripada pravoj $A + B$.
   Ovim je dokazano da važi aksioma 3.

$\blacksquare$

2.3 Pitanje jedinstvenosti ternarnog prstena

Ako su A i A_1 afine ravni izgrađene, redom, nad ternarnim prstenima K i K_1 određenim pravama l i m i tačkom z, odnosno, l_1 i m_1 i tačkom z_1 onda će postojati izomorfizam, odnosno kolineacija $f : A \to A_1$ koja slika redom l, m i z u l_1, m_1 i z_1 ako i samo ako postoji bijekcija $F : K \to K_1$ takva da je $F(0) = 0, F(1) = 1$, i $F([ax + b]) = [F(a)F(x) + F(b)]$ za sve $a, x, b \in K$, odnosno ako postoji izomorfizam ternarnih prstena. Naglasimo da ukoliko ovaj izbor učinimo manje strogim, odnosno tačku z ne preslikamo u z_1 već u neku drugu, ternarni prsteni K i K_1 tako dobijeni više, u opštem slučaju ne moraju biti izomorfni. Ipak, pokazaćemo da važi sledeće tvrđenje.

Teorema 2.13 *Neka je K telo, a K_1 ternarni prsten. Neka su afine ravni K^2 i K_1^2 izomorfne. Tada su ternarni prsteni K i K_1 izomorfni.*

Dokazaćemo ovo tvrđenje u nekoliko koraka.

Lema 2.1 Neka je K telo, a l i m ose afine ravni K^2, dok su z i z_1 dve tačke neincidentne sa osama. Tada postoji izomorfizam afine ravni K^2 koji preslikava ose l i m u sebe, a tačku z u tačku z_1.

Dokaz: Neka su koordinate tačaka z i z_1, redom $(1,1)$ i (u,v). Pri tom, $u, v \neq 0$ jer z_1 ne pripada osama. Neka je preslikavanje ravni dato sa $f(x,y) = (ux, vy)$. Tada, očigledno, $f(1,1) = (u,v)$. Neka je prava data jednačinom $y = ax + b$. Množenjem ove jednačine sa v sa leve strane dobijamo

$$vy = v(ax) + vb = (vau^{-1})ux + vb,$$

prvo zbog zakona leve distributivnosti, a zatim i zbog asocijativnosti množenja. Kako se tačka (x,y) slika u (ux, vy) sledi da se prava $y = ax + b$ slika u pravu datu jednačinom $y = (vau^{-1})x + vb$. Takođe, očigledno je i da se vertikalne prave $x = c$ preslikavaju u prave $x = cu$. Dakle, preslikavanje f zadovoljava uslove leme. ∎

Lema 2.2 Neka je K telo i l i m ose ravni K^2, a l_1 i m_1 neki par pravih te ravni koji se seku. Tada postoji izomorfizam ravni K^2 kojim se l i m slikaju u l_1 i m_1.
Dokaz: Dokazaćemo prvo da su sledeća preslikavanja izomorfizmi afine ravni.

1. Preslikavanje $f_1(x,y) = (y,x)$ je izomorfizam jer slika pravu $x = a$ u pravu $y = 0x + a$, i pravu $y = 0x + b$ u pravu $x = b$. Ako je $a \neq 0$, onda pravu $y = ax + b$, odnosno $x = a^{-1}y - a^{-1}b$ slika u pravu $y = a^{-1}x - a^{-1}b$. Iskoristili smo levu distributivnost i asocijativnost množenja.

2. Za $c, d \in K$ preslikavanje $f_2(x,y) = (x + c, y + d)$ je izomorfizam jer slika pravu $x = a$ u pravu $x = a+c$ i pravu $y = ax+b$ u pravu $y = ax-ac+b+d$. Ovde smo iskoristili levu distributivnost.

3. Za $c \in K$ preslikavanje $f_3(x,y) = (x, y-cx)$ je izomorfizam jer slika svaku pravu $x = a$ na sebe a pravu $y = ax + b$ slika u pravu $y = (a - c)x + b$. Ovde smo iskoristili desnu distributivnost.

4. Za $c \in K$ preslikavanje $f_4(x,y) = (x - cy, y)$ je izomorfizam jer se može predstaviti kao kompozicija izomorfizama $f_4 = f_1 \circ f_3 \circ f_1$

Preslikavanje f_2 nam omogućava da možemo da pretpostavimo da se l_1 i m_1 seku u koordinatnom početku, a preslikavanje f_1 da se prava l_1 ne poklapa sa osom m. Zato l_1 ima jednačinu oblika $y = cx$. Tada se preslikavanjem f_3 prava l_1 preslikava u osu l. Pri tome m_1 sadrži koordinatni početak i ukoliko se ne poklapa sa osom m ima jednačinu oblika $x = cy$, pa se preslikavanjem f_4 slika u m. Pri tome, prava l je invarijantna za preslikavanje f_4, pa je kompozicija ovih izomorfizama traženi izomorfizam.

∎

Dakle, na osnovu prethodne dve leme zaključujemo da u slučaju tela K postoji izomorfizam afine ravni K^2 koji preslikava jedan par osa l i m i tačku z u drugi par osa l_1 i m_1 i tačku z_1, odnosno za svaki par pravih koje se seku i tačku koja sa njima nije incidentna možemo reći da su ose i tačka jedinice.

Neka je sada $f : K_1^2 \to K^2$ izomorfizam afinih ravni izgrađenih nad ternarnim prstenom i telom. Ako se ose ravni K_1^2, p i q i tačka jedinice w redom, slikaju u prave l i m i tačku z, na osnovu prethodnog, možemo l i m proglasiti osama ravni

K^2, a z tačkom jedinice, a tada, kao što smo već zaključili, izomorfizam koji ose, koordinatni početak i jedinice jedne ravni slika u ose, koordinatni početak i jedinicu druge ravni indukuje izomorfizam ternarnih prstena. Kako je jedan od njih telo, tada je to i drugi.

2.4 Četvrta aksioma

Navešćemo još jednu aksiomu koju afine ravni mogu, ali ne moraju zadovoljavati. Videćemo da ukoliko ova aksioma važi u afinoj ravni da je onda ona izgrađena nad telom. Četvrtu aksimu smo podelili u dva iskaza: 4a i 4b.

2.4.1 Konstrukcija tela

Aksioma 4a Za svaki par tačaka P, Q postoji translacija $\tau_{P,Q}$ koja tačku P slika u tačku Q: $\tau_{P,Q}(P) = Q$.

Primer 2.8 Primer jedne afine ravni u kojoj ne važi Aksioma 4a je Multonova ravan, a o kojoj opširnije možete pročitati u sekciji 3.1.

Primedba Kako je translacija određena slikom jedne tačke, to znači da je $\tau_{P,Q}$ jednoznačno određeno; posebno, $\tau_{P,P} = 1$. Kako sada imamo translacije sa različitim pravcima, sledi da je grupa translacija $\mathbf{T}$, ukoliko važi Aksioma 4a, komutativna.

Definicija 2.8 Preslikavanje $\alpha : \mathbf{T} \to \mathbf{T}$ naziva se "homomorfizam koji čuva trag" ako:

1. je ono homomorfizam grupe $\mathbf{T}$, tj. $(\tau_1\tau_2)^\alpha = \tau_1^\alpha\tau_2^\alpha$.
   (Simbol τ^α koristimo za označavanje slike preslikavanja τ prilikom dejstva preslikavanja α.)

2. ono čuva tragove, ili bolje rečeno: tragovi translacije τ su u isto vreme tragovi τ^α. To znači da ili $\tau^\alpha = 1$, ili translacije τ i τ^α imaju iste smerove.

Navedimo važne primere homomorfizama koji čuvaju tragove.

1) Preslikavanje koje svaku translaciju τ iz $\mathbf{T}$ slika u identitet: $\tau^\alpha = 1, \forall \tau \in \mathbf{T}$. Označićemo ovo preslikavanje sa 0 i pisati $\tau^0 = 1$.

2) Identitet, koji cemo označiti simbolom 1; sledi $\tau^1 = \tau, \forall \tau \in \mathbf{T}$.

3) Preslikavanje koje svaki element τ slika u njemu inverzni τ^{-1}. Označićemo ovo preslikavanje sa -1. Tada važi $(\tau_1\tau_2)^{-1} = \tau_2^{-1}\tau_1^{-1} = \tau_1^{-1}\tau_2^{-1}$ pošto je grupa $\mathbf{T}$ komutativna. Translacije τ^{-1} i τ imaju iste smerove.

4) Neka je σ fiksna dilatacija. Tada σ indukuje preslikavanje svake translacije τ na $\sigma\tau\sigma^{-1}$. Već znamo da τ i $\sigma\tau\sigma^{-1}$ imaju iste tragove. Šta više, $\sigma(\tau_1\tau_2)\sigma^{-1} = \sigma\tau_1\sigma^{-1}\sigma\tau_2\sigma^{-1}$.

Skup svih homomorfizama koji čuvaju tragove označavamo sa K.

Primer 2.9 Odredimo homomorfizme u ravni $\mathbb{R}^2$. Translacije τ_v i τ_v^α imaju iste pravce, pa je tada $\tau_v^\alpha = \tau_{f(v)\cdot v}$ (ako je $\tau_v^\alpha = 1$ ako i samo ako $f(v) = 0$).

Tada $(\tau_{v_1+v_2})^\alpha = \tau_{v_1}^\alpha \tau_{v_2}^\alpha$ pa

$$\tau_{f(v_1+v_2)(v_1+v_2)} = \tau_{f(v_1)v_1}\tau_{f(v_2)v_2} = \tau_{f(v_1)v_1+f(v_2)v_2}.$$

Odavde je $f(v_1+v_2)v_1+f(v_1+v_2)v_2 = f(v_1)v_1+f(v_2)v_2, \;\; \forall\, v_1, v_2$, a za linearno nezavisne $f(v_1+v_2) = f(v_1) = f(v_2) = const. = k$.
Odavde sledi $\tau_v^\alpha = \tau_{k\cdot v}$, pa skup svih homomorfizama za $\mathbb{R}^2$ možemo zapisati kao $\{k|k \in \mathbb{R}\}$ tj. $\mathbb{R}$.

Primer 2.10 Nađimo homomorfizme Fanoove ravni. Jedna neidentička translacija je $\tau = \begin{pmatrix} A & D & B & C \\ D & A & C & B \end{pmatrix}$. Ako α slika jednu neidentičku translaciju u identitet, onda sve translacije slika u identitet. Jedan trag τ je prava $A + D$. Neidentička transalcija τ^α ne fiksira A jer je translacija, $\tau^\alpha(A) = X$ i $A + X \parallel A + D$, pa je $X = D$. Slično i nalazimo slike i za ostale tačke. Dakle $\tau^\alpha = \tau$ pa ili α slika sve τ u identitet ili $\tau^\alpha = \tau$. Skup homomorfizama se sastoji od dva preslikavanja $\{0, \alpha\}$

Definicija 2.9 Neka su α i β elementi iz K. Tada je i kompozicija $\tau^\alpha\tau^\beta$ translacija sa istim tragom kao i τ. Preslikavanje koje τ slika u $\tau^\alpha\tau^\beta$ označimo sa $\alpha + \beta$. Zvaćemo ga sumom preslikavanja α i β. Tako je $\tau^{\alpha+\beta} = \tau^\alpha\tau^\beta$.
Takođe, preslikavanje koje τ slika u $(\tau^\beta)^\alpha$ nazivamo proizvodom preslikavanja α i β i označavamo $\alpha\beta$. Tako je $\tau^{\alpha\beta} = (\tau^\beta)^\alpha$.

Teorema 2.14 *Ako α i β pripadaju K, onda i $\alpha+\beta$ i $\alpha\beta$ takođe pripadaju K. Pod ovim okolnosima skup K postaje asocijativni prsten sa jediničnim elementom* 1.

Dokaz:

1. $(\tau_1\tau_2)^{\alpha+\beta} = (\tau_1\tau_2)^\alpha(\tau_1\tau_2)^\beta = \tau_1^\alpha\tau_2^\alpha\tau_1^\beta\tau_2^\beta = \tau_1^\alpha\tau_1^\beta\tau_2^\alpha\tau_2^\beta$, jer je grupa $\mathbf{T}$ komutativna. Sledi, $(\tau_1\tau_2)^{\alpha+\beta} = \tau_1^{\alpha+\beta}\tau_2^{\alpha+\beta}$.
   Ako je $\tau = 1$, tada $\tau^\alpha = \tau^\beta = 1$. Odatle, $\tau^{\alpha+\beta} = 1$.
   Ako je $\tau \neq 1$ onda se njegovi pravci π pojavljuju među tragovima od τ^α i τ^β, i takođe među tragovima od $\tau^\alpha\tau^\beta = \tau^{\alpha+\beta}$. Odavde sledi da je $\alpha + \beta \in K$.

2. $(\tau_1\tau_2)^{\alpha\beta} = ((\tau_1\tau_2)^\beta)^\alpha = (\tau_1^\beta\tau_2^\beta)^\alpha = (\tau_1^\beta)^\alpha(\tau_2^\beta)^\alpha = \tau_1^{\alpha\beta}\tau_2^{\alpha\beta}$.
   Tragovi od τ pripadaju onima od τ^β, pa prema tome i onima od $(\tau^\beta)^\alpha = \tau^{\alpha\beta}$.

3. Ako je $\alpha, \beta, \gamma \in K$, onda je $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$:
   $\tau^{(\alpha+\beta)+\gamma} = \tau^{\alpha+\beta}\tau^\gamma = \tau^\alpha\tau^\beta\tau^\gamma = \tau^\alpha\tau^{\beta+\gamma} = \tau^{\alpha+(\beta+\gamma)}$, jer je $\mathbf{T}$ grupa, pa i asocijativna.

4. Pokažimo da je $\alpha + \beta = \beta + \alpha$. Kako je $\mathbf{T}$ komutativna grupa, sledi $\tau^{\alpha+\beta} = \tau^\alpha\tau^\beta = \tau^\beta\tau^\alpha = \tau^{\beta+\alpha}$.

5. Pokažimo da je 0 neutral za sabiranje. Važi $\tau^{0+\alpha} = \tau^0\tau^\alpha = 1\tau^\alpha = \tau^\alpha$, pa je $0 + \alpha = \alpha$.

6. Jednakost $\alpha + (-1)\alpha = 0$ sledi iz $\tau^{\alpha+(-1)\alpha} = \tau^\alpha\tau^{(-1)\alpha} = \tau^\alpha(\tau^\alpha)^{-1} = 1 = \tau^0$, pa je $-\alpha = (-1)\alpha$.

7. Pokažimo $(\beta+\gamma)\alpha = \beta\alpha + \gamma\alpha$. Važi $\tau^{(\beta+\gamma)\alpha} = (\tau^\alpha)^{\beta+\gamma} = (\tau^\alpha)^\beta(\tau^\alpha)^\gamma = \tau^{\beta\alpha}\tau^{\gamma\alpha} = \tau^{\beta\alpha+\gamma\alpha}$.

8. Slično, $\alpha(\beta+\gamma) = \alpha\beta + \alpha\gamma$ sledi iz $\tau^{\alpha(\beta+\gamma)} = (\tau^{\beta+\gamma})^\alpha = (\tau^\beta\tau^\gamma)^\alpha = (\tau^\beta)^\alpha(\tau^\gamma)^\alpha = \tau^{\alpha\beta}\tau^{\alpha\gamma} = \tau^{\alpha\beta+\alpha\gamma}$.
   Ovde smo iskoristili činjenicu da je α homomorfizam.

9. Jednakost $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ sledi iz $\tau^{(\alpha\beta)\gamma} = (\tau^\gamma)^{\alpha\beta} = ((\tau^\gamma)^\beta)^\alpha = (\tau^{\beta\gamma})^\alpha = \tau^{\alpha(\beta\gamma)}$.

10. Pokažimo i $1\alpha = \alpha$ i $\alpha 1 = \alpha$. Ove jednakosti slede iz $\tau^{1\alpha} = (\tau^\alpha)^1 = \tau^\alpha$ i $\tau^{\alpha 1} = (\tau^1)^\alpha = \tau^\alpha$.
    Ovim je pokazano da je K asocijativni prsten sa jedinicom.

∎

Teorema 2.15 *Neka $\alpha \in K, \alpha \neq 0$ i P data tačka. Postoji jednistvena dilatacija σ sa fiksnom tačkom P tako da $\tau^\alpha = \sigma\tau\sigma^{-1}$, $\forall\, \tau \in \boldsymbol{T}$.*

Dokaz: Posmatrajmo preslikavanje dato sa $\sigma : Q \mapsto \tau^\alpha_{PQ}(P)$. Tačka P je očigledno fiksna tačka preslikavanja σ. Neka su Q_1 i Q_2 proizvoljne različite tačke, a $\tau^\alpha_{PQ_1}(P) = Q_1'$ i $\tau^\alpha_{PQ_2}(P) = Q_2'$ njihove slike u preslikavanju σ. S obzirom da je $\tau_{PQ_2} = \tau_{Q_1Q_2}\tau_{PQ_1}$, a α homomorfizam, onda je i

$$\tau^\alpha_{PQ_2} = \tau^\alpha_{Q_1Q_2}\tau^\alpha_{PQ_1},$$

što, kad preslikamo tačku P znači $Q_2' = \tau^\alpha_{Q_1Q_2}(Q_1')$. Pretpostavimo da se Q_1' i Q_2' ne poklapaju. Jasno je da je $Q_1' + Q_2'$ jedan trag $\tau^\alpha_{Q_1Q_2}$. Prava $Q_1 + Q_2$ je trag $\tau_{Q_1Q_2}$, pa i od $\tau^\alpha_{Q_1Q_2}$. Zato su $Q_1 + Q_2$ i $Q_1' + Q_2'$ paralelne, pa u tom slučaju, kao i ako se Q_1' i Q_2' poklapaju direktno sledi da je σ dilatacija.
Kako je $\sigma(Q) = \tau^\alpha_{PQ}(P)$, onda je i

$$Q = \sigma^{-1}\tau^\alpha_{PQ}\sigma(P),$$

pa se translacija $\sigma^{-1}\tau^\alpha_{PQ}\sigma$ poklapa sa τ_{PQ}. S obzirom da se proizvoljna translacija može, na osnovu Aksiome 4a, zapisati kao τ_{PQ} za neko Q, sledi tvrđenje.
∎

Primedba Primer 4) homomorfizama koji čuvaju trag pokazuje da važi i za obratno tvrđenje. Ako je σ dilatacija, onda preslikavanje $\tau \to \sigma\tau\sigma^{-1}$ je homomorfizam koji čuva trag α; ne može biti 0, jer $\sigma\tau\sigma^{-1} = 1$ važi samo za $\tau = 1$, a ne za sve τ.

Teorema 2.16 *Prsten K je telo.*

Dokaz: Neka $\alpha \in K, \alpha \neq 0$ i neka je σ dilatacija takva da je $\tau^\alpha = \sigma\tau\sigma^{-1}$. Preslikavanje koje τ slika u $\sigma^{-1}\tau\sigma = \sigma^{-1}\tau(\sigma^{-1})^{-1}$ takođe je element prstena K, i označavaćemo ga sa α^{-1}. Tako imamo $\tau^\alpha = \sigma\tau\sigma^{-1}$ i $\tau^{\alpha^{-1}} = \sigma^{-1}\tau\sigma$. Dalje je $\tau^{\alpha\alpha^{-1}} = (\tau^{\alpha^{-1}})^\alpha = \sigma(\sigma^{-1}\tau\sigma)\sigma^{-1} = \tau = \tau^1$ i
$\tau^{\alpha^{-1}\alpha} = (\tau^\alpha)^{\alpha^{-1}} = \sigma^{-1}(\sigma\tau\sigma^{-1})\sigma = \tau = \tau^1$.
Iz poslednjih jednakosti vidimo da $\alpha\alpha^{-1} = \alpha^{-1}\alpha = 1$, tj. ustanovili smo postojanje inverznog elementa. ∎

Teorema 2.17 *Ako je $\tau^\alpha = 1$ za neko α i neko τ, onda je ili $\alpha = 0$ ili $\tau = 1$. Ako za neke α, β, τ imamo $\tau^\alpha = \tau^\beta$, onda ili $\tau = 1$ ili $\alpha = \beta$.*

Dokaz: Pretpostavimo da $\tau^\alpha = 1$ za $\alpha \neq 0$. Primenimo α^{-1}:
$(\tau^\alpha)^{\alpha^{-1}} = 1^{\alpha^{-1}} = 1$ ili $\tau = 1$.
Pretpostavimo sada da $\tau^\alpha = \tau^\beta$. Posle množenja sa $\tau^{-\beta}$ imamo $\tau^{\alpha-\beta} = 1$. Ako je $\alpha \neq \beta$ onda je $\tau = 1$. ∎

2.4.2 Uvođenje koordinata

Aksioma 4b Ako su τ_1 i τ_2 translacije sa istim tragovima takve da je $\tau_1 \neq 1, \tau_2 \neq 1, \tau_1 \neq \tau_2$ tada postoji $\alpha \in k$ tako da je $\tau_2 = \tau_1^\alpha$.

Primedba Ako je $\tau_2 = \tau_1$, onda $\tau_2 = \tau_1^1$; ako je $\tau_2 = 1$ onda $\tau_2 = \tau_1^0$.

Aksioma 4b P (za datu tačku P) Neka su date dve tačke Q i R takve da su tačke P, Q, R različite ali sve incidentne sa istom pravom. Tada postoji dilatacija σ koja tačku Q slika u tačku R, a tačku P ostavlja fiksnom.

Teorema 2.18 *Ako Aksioma 4bP važi za jednu tačku P onda važi i aksioma 4b. Obrnuto, iz aksiome 4b sledi aksioma 4bP za svaku tačku P.*

Dokaz: Neka su τ_1 i τ_2 različite, neidentičke translacije sa istim tragovima i $Q = \tau_1(P)$ i $R = \tau_2(P)$. Kako su tragovi isti, tačke P, Q i R su kolinearne. Neka je σ dilatacija sa fiksnom tačkom P koja preslikava Q u R. Tada je $\sigma\tau_1\sigma^{-1}$ translacija koja preslikava P u R, pa je $\sigma\tau_1\sigma^{-1} = \tau_2$. Ako je α takvo da je $\tau^\alpha = \sigma\tau\sigma^{-1}$, onda je $\tau_2 = \tau_1^\alpha$.
Obrnuto, neka su P, Q i R tri različite kolinearne tačke. Tada τ_{PQ} i τ_{PR} zadovoljavaju iskaz Aksiome 4b, pa postoji α takvo da je $\tau_{PR} = \tau_{PQ}^\alpha$. Ako je σ dilatacija koja fiksira tačku P, takva da za proizvoljnu translaciju važi $\tau^\alpha = \sigma\tau\sigma^{-1}$, onda je
$$\tau_{PR} = \sigma\tau_{PQ}\sigma^{-1},$$
pa je $\tau_{PR}\sigma(P) = \sigma\tau_{PQ}(P)$, odnosno $R = \sigma(Q)$. ∎

Teorema 2.19 *Neka su date translacije τ_1 i τ_2 ($\tau_1 \neq 1, \tau_2 \neq 1$) sa različitim pravcima. Tada za svaku translaciju $\tau \in \boldsymbol{T}$ postoje jedinstveni elementi $\alpha, \beta \in K$ tako da $\tau = \tau_1^\alpha\tau_2^\beta = \tau_2^\beta\tau_1^\alpha$.*

Dokaz: Komutativnost je jasna s obzirom da je T komutativno.

1. Neka je P proizvoljna tačka i pretpostavimo da je $\tau(P) = Q$. Neka je prava l_1 τ_1-trag kroz tačku P a l_2 τ_2-trag kroz tačku Q. Tada $l_1 \nparallel l_2$, pa postoji tačka R koja pripada l_1 i l_2.

   Translacija τ_{PR} je ili identitet ili ima isti pravac kao τ_1. Slično, translacija τ_{RQ} je ili identitet ili ima isti pravac kao τ_2.

   Na osnovu aksiome 4b i primedbe postoje elementi $\alpha, \beta \in K$ tako da $\tau_{PR} = \tau_1^\alpha$ i $\tau_{RQ} = \tau_2^\beta$. Sledi da je $\tau_2^\beta\tau_1^\alpha(P) = \tau_{RQ}\tau_{PR}(P) = Q$ i sledi $\tau = \tau_{PQ} = \tau_2^\beta\tau_1^\alpha$.

2. Ako je $\tau_1^\alpha \tau_2^\beta = \tau_1^\gamma \tau_2^\delta$ onda $\tau_1^{\alpha-\gamma} = \tau_2^{\delta-\beta}$. Ako je $\tau_1^{\alpha-\gamma} \neq 1$ onda leva strana jednakosti $\tau_1^{\alpha-\gamma} = \tau_2^{\delta-\beta}$ ima pravac kao τ_1, a desna kao τ_2 što je nemoguće. Dakle, $\tau_1^{\alpha-\gamma} = 1$ i $\tau_2^{\delta-\beta} = 1$. Iz Teoreme 2.17 sledi $\alpha = \gamma, \delta = \beta$.

∎

Nadalje u ovom poglavlju pretpostavljamo da u afinoj ravni važi Aksioma 4b. Sada ćemo pokazati da je takva ravan izgrađena nad telom K. Neka je data tačka O koordinatni početak i dve translacije τ_1 i τ_2 sa različitim tragovima: tragovi ovih translacija koji prolaze kroz tačku O mogu se predstaviti kao koordinatne ose l i m, a tačke $\tau_1(O)$ i $\tau_2(O)$ kao tačke jedinica na tim osama.

Neka je P proizvoljna tačka. Zapišimo translaciju τ_{OP} u obliku $\tau_{OP} = \tau_1^\xi \tau_2^\eta$ s jedinstvenim $\xi, \eta \in K$ i dodelimo tački P koordinate (ξ, η). I obrnuto, ako je dat par (ξ, η) onda je $\tau_1^\xi \tau_2^\eta$ translacija koja tačku O slika u neku tačku P, tako da je $\tau_{OP} = \tau_1^\xi \tau_2^\eta$ i ova tačka P će imati date koordinate (ξ, η). Pišemo $P = (\xi, \eta)$. Tačka $\tau_1(\tau_2(O))$ je tačka sa koordinatama $(1, 1)$.

Za $P = O$ imamo $\tau_{OO} = \tau_1^0 \tau_2^0$ pa su koordinate koordinatnog početka $P = O = (0, 0)$.

Neka je p prava, $P = (\alpha, \beta)$ tačka na pravoj p, a $\tau = \tau_1^\gamma \tau_2^\delta$ je neidentička translacija kojoj je trag prava p. Neka je $Q = (\xi, \eta)$ proizvoljna tačka na p. Tada ili $\tau_{PQ} = 1$ ili τ_{PQ} i τ imaju isti pravac. Po Aksiomi 4b i Primedbi imamo $\tau_{PQ} = \tau^t$ za neko $t \in K$.

Obrnuto, za proizvoljno t prava p će pripadati tragovima τ^t, gde je $\tau^t(P) = Q$ neka tačka na l. To pokazuje da će svaka translacija τ^t imati oblik τ_{PQ}, gde je Q tačka sa prave p. Takođe nam je poznato da je t jedinstveno određeno preslikavanjem τ_{PQ} (Teorema 2.17). Da bismo dobili koordinate tačke Q moramo izračunati τ_{OQ}. Imamo da je $\tau_{OQ} = \tau_{PQ}\tau_{OP} = (\tau_1^\gamma \tau_2^\delta)^t \tau_1^\alpha \tau_2^\beta = \tau_1^{t\gamma+\alpha} \tau_2^{t\delta+\beta}$. Sledi da tačka Q ima koordinate $(t\gamma + \alpha, t\delta + \beta)$, a sve tačke prave p se dobijaju za $t \in K$. Dakle onda jednačinu prave možemo zapisati na sledeći način $y = x\gamma^{-1}\delta - \alpha\gamma^{-1}\delta + \beta$.

Kako $P = (\alpha, \beta)$ može biti bilo koja tačka, onda α i β mogu biti proizvoljni. Preslikavanje $\tau = \tau_1^\gamma \tau_2^\delta$ mora biti neidentička translacija, pa γ i δ ne mogu biti istovremeno nula.

Sada možemo preći na vektorski zapis: stavimo $A = (\gamma, \delta), P = (\alpha, \beta)$. Tada formula $Q = P + tA$, $t \in K$, predstavlja tačke na pravoj. Jedino ograničenje je da je $A \neq O$.

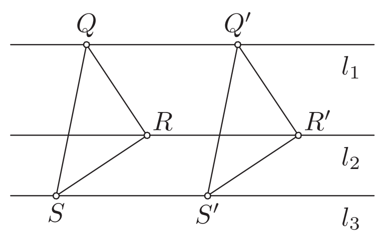
Očigledno, ovaj način uvođenja koordinata odgovara koordinatizaciji nad ternarnim prstenom koju smo ranije upoznali. Važenje Aksioma 4a i 4b nam omogućuje da u skupu tačaka jedne prave definišemo operacije sabiranja i množenja sa kojima taj skup postaje telo, a samim tim i ternarni prsten sa nulom i jedinicom, a data ravan je onda izgrađena nad telom.

2.5 Dezargova i Paposova teorema

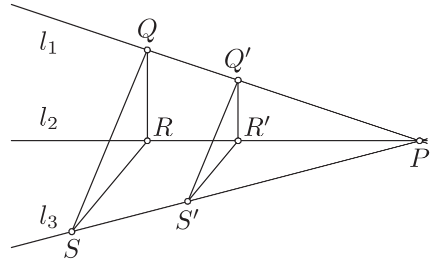
U ovom poglavlju izložićemo iskaze tvrđenja koja u proizvoljnoj afinoj ravni (u kojoj ne mora da važi Aksioma 4) mogu, ali ne moraju da važe. Ipak, iz tradicionalnih razloga, nazvaćemo ih teoremama.

2.5.1 Dezargova teorema

Teorema 2.20 *(Dezarg) Neka su l_1, l_2, l_3 tri različite prave koje su ili sve paralelne ili se sve seku u tački P. Neka su Q i Q' tačke na pravoj l_1, R i R' tačke na pravoj l_2 i S i S' tačke na pravoj l_3, pri čemu su sve različite od tačke P ukoliko se prave seku. Pretpostavimo da $Q + R \parallel Q' + R'$ i $Q + S \parallel Q' + S'$. Tada $R + S \parallel R' + S'$.*



Sl. 2.7



Sl. 2.8

Primedba Postoje trivijalni slučajevi u kojima je ova teorema očigledno tačna:

1. Ako je $Q = Q'$, onda je $Q+R = Q'+R'$ i kako l_2 i $Q+R$ imaju zajedničku tačku R ali ne i Q, sledi $R = R'$ i $S = S'$.

2. Ako su tačke Q, R, S kolinearne, onda su i tačke Q', R', S' kolinearne pa će i za ove tačke tvrđenje važiti.

Ako su prave l_1, l_2, l_3 paralelne onda ćemo teoremu zvati Da; ako se prave seku u tački P, zvaćemo je DP.

Teorema 2.21 *Teorema Da sledi iz Aksiome 4a, a Teorema DP iz Aksiome 4bP.*

Dokaz: Neka je σ translacija koja tačku Q slika u Q' (ukoliko dokazujemo Da), ili je σ dilatacija sa fiksnom tačkom P, koja Q slika u Q' (ako dokazujemo DP). Tada su prave l_1, l_2, l_3 tragovi preslikavanja σ. Kako je $Q + R \parallel \sigma Q + \sigma R = Q' + \sigma R$, to je $\sigma R = R'$ i analogno $\sigma S = S'$. Tada $R + S \parallel \sigma R + \sigma S = R' + S'$. ∎

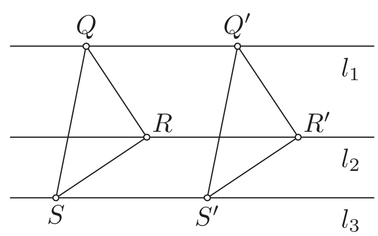
Pokažimo da važi i obrnuto tvrđenje.

Teorema 2.22 *Aksioma 4a sledi iz Teoreme Da, a Aksioma 4bP iz Teoreme DP.*

Dokaz:

1. Pretpostavimo da svaka prava sadrži samo dve tačke. To znači da dati pramen paralelnih pravih sadrži samo dve prave pa u ovakvoj geometriji imamo samo četiri tačke A, B, C, D i šest pravih: $A+B, A+C, \ldots$ Svaka prava sadrži tačno dve tačke kojima je određena. Takva geometrija mora imati jedinstvenu strukturu. S druge strane postoji polje K sa samo dva elementa 0 i 1 i u kom važi $1+1=0$. Geometrija izgrađena nad ovim poljem ima svojstvo da svaka prava sadrži samo dve tačke, pa je ovo geometrija od četiri tačke. U ovoj geometriji važe sve aksiome sem 4a i 4b.

2. Pretpostavimo da važi Teorema Da. Sa nekim parom Q, Q' različitih tačaka definisaćemo preslikavanje $\tau^{Q,Q'}$ koje će biti definisano samo za tačke R koje ne pripadaju pravoj $Q+Q'$.
Neka je $l \parallel Q+Q'$ i l sadrži tačku R; tada je $l \neq Q+Q'$.
Neka je $m \parallel Q+R$ i m sadrži Q'; tada je $m \neq Q+R$.
Kako je $Q+Q' \nparallel Q+R$, sledi $l \nparallel m$. Neka je R' tačka preseka m i l.



Sl. 2.9

R' pripada l, dakle ne pripada $Q+Q'$ i pripada m, pa ne pripada $Q+R$. To znači da je $R' \neq Q'$ i $R' \neq R$. Dobijamo $R+R' \parallel Q+Q'$ i $Q+R \parallel Q'+R'$. Tako smo odredili sliku R' tačke R i $\tau^{Q,Q'}$

Sa parom tačaka R i R' možemo konstruisati preslikavanje $\tau^{R,R'}$. Jasno je da će se ovim preslikavanjem Q preslikati u Q'. Neka je sada S tačka koja ne pripada $R+R'$ ni $Q+Q'$ i S' slika tačke S pri $\tau^{Q,Q'}$. Imamo $Q+Q' \parallel R+R' \parallel S+S'$ i ove tri prave su različite. Još važi i $Q+R \parallel Q'+R'$ i $Q+S \parallel Q'+S'$. Tvrđenje da je $R+R' \parallel S+S'$ i $R+S \parallel R'+S'$ znači da je S' slika tačke S pri preslikavanju $\tau^{R,R'}$. Kako smo pretpostavili da postoji tačka S koja ne pripada $Q+Q'$ i $R+R'$, možemo formirati preslikavanje $\tau^{S,S'}$. Traženo preslikavanje τ je kombincija ova tri preslikavanja: za neku tačku T njena slika će biti slika pri jednom od ova tri preslikavanja koje je definisano. Preslikavanje τ ima osobinu da $\tau(Q) = Q'$ što smo već pokazali sa preslikavanjem $\tau^{R,R'}$. Ako pokažemo da je τ dilatacija onda će τ biti translacija jer su svi tragovi paralelni (slučaj $Q = Q'$ je trivijalan - to je identitet).
Neka su U, V dve različite tačke. Jedna od pravih $Q+Q'$, $R+R'$, $S+S'$

neće sadržati U i V; pretpostavimo da je $Q + Q'$ takva prava i možemo koristiti $\tau^{Q,Q'}$ za nalaženje slika. Ako je $U+V \parallel Q+Q'$ onda $U+V$ sadrži U' i V'. Zato ćemo pretpostaviti da $U + V \nparallel Q + Q'$. Onda su U i V na istom položaju kao što su malopre bili R i S, za koje smo već dokazali da $R + S \parallel R' + S'$. Ovim je dokaz završen.

3. Ako pretpostavimo da važi DP, možemo dokazati 4bP na isti način kao u prethodnom slučaju korišćenjem pravih kroz P umesto pravih koje su paralelne se $Q + Q'$.

∎

Dezargova teorema je, dakle, ekvivalentna, Aksiomama 4a i 4b i njihova je geometrijska interpretacija. Ona važi u nekoj afinoj ravni ako i samo ako ta ravan zadovoljava iskaz Aksiome 4. Videli smo da je u tom slučaju, ravan izgrađena nad telom.

Važi i obrnuto.

Lema 2.3 Neka je afina ravan izgrađena nad telom. Tada u njoj važi Dezargova teorema.

Dokaz: Neka su date tačke $Q(\alpha_1, \beta_1)$, $Q'(\alpha_1', \beta_1')$, $R(\alpha_2, \beta_2)$, $R'(\alpha_2', \beta_2')$, $S(\alpha_3, \beta_3)$, $S'(\alpha_3', \beta_3')$. Pokazaćemo tvrđenje u slučaju da su prave QQ', SS', RR' paralelne. Taj uslov je ekvivalentan sa

$$(\beta_1' - \beta_1)(\alpha_1' - \alpha_1)^{-1} = (\beta_2' - \beta_2)(\alpha_2' - \alpha_2)^{-1} = (\beta_3' - \beta_3)(\alpha_3' - \alpha_3)^{-1}. \quad (3)$$

Ako su prave QQ' i RR' paralelne, tada važi

$$(\beta_2 - \beta_1)(\alpha_2 - \alpha_1)^{-1} = (\beta_2' - \beta_1')(\alpha_2' - \alpha_1')^{-1} \quad (4)$$

i QQ' i SS' paralelne, važi

$$(\beta_3 - \beta_1)(\alpha_3 - \alpha_1)^{-1} = (\beta_3' - \beta_1')(\alpha_3' - \alpha_1')^{-1}. \quad (5)$$

Treba da pokažemo da su tada RR' i SS' paralelne, odnosno da važi

$$(\beta_3 - \beta_2)(\alpha_3 - \alpha_2)^{-1} = (\beta_3' - \beta_2')(\alpha_3' - \alpha_2')^{-1}.$$

Sredimo jednakosti (3) i (4), dobijamo

$$\beta_2(\alpha_2' - \alpha_2)^{-1}(\alpha_1' - \alpha_1) - \beta_1 = -\beta_1' + \beta_2'(\alpha_2' - \alpha_2)^{-1}(\alpha_1' - \alpha_1) \quad (6)$$

$$\beta_2 - \beta_1 = -\beta_1'(\alpha_2' - \alpha_1')^{-1}(\alpha_2 - \alpha_1) + \beta_2'(\alpha_2' - \alpha_1')^{-1}(\alpha_2 - \alpha_1). \quad (7)$$

Sada (6) pomnožimo sa desne strane sa $(\alpha_1' - \alpha_1)^{-1}(\alpha_2' - \alpha_2)$ i od nje oduzmimo (7), dobijamo

$$\begin{aligned}\beta_1(1 - (\alpha_1' - \alpha_1)^{-1}(\alpha_2' - \alpha_2)) = \\ &- \beta_1'[(\alpha_1' - \alpha_1)^{-1}(\alpha_2' - \alpha_2) - (\alpha_2' - \alpha_1')^{-1}(\alpha_2 - \alpha_1)] \\ &+ \beta_2'(1 - (\alpha_2' - \alpha_1')^{-1}(\alpha_2 - \alpha_1)). \quad (8)\end{aligned}$$

Dobijamo

$$\begin{aligned}\beta_1 = \\ &\{-\beta_1'[(\alpha_1' - \alpha_1)^{-1}(\alpha_2' - \alpha_2) - (\alpha_2' - \alpha_1')^{-1}(\alpha_2 - \alpha_1)] \\ &+ \beta_2'[(1 - (\alpha_2' - \alpha_1')^{-1}(\alpha_2 - \alpha_1))]\} \cdot [1 - (\alpha_1' - \alpha_1)^{-1}(\alpha_2' - \alpha_2)]^{-1}. \quad (9)\end{aligned}$$

Izračunajmo β_2 tako što ćemo (7) oduzeti od (6)

$$\begin{aligned}\beta_2 = \\ &\{\beta_2'[(\alpha_2'-\alpha_2)^{-1}(\alpha_1'-\alpha_1)-(\alpha_2'-\alpha_1')^{-1}(\alpha_2-\alpha_1)] \\ &+\beta_1'[(\alpha_2'-\alpha_1')^{-1}(\alpha_2-\alpha_1)-1]\}\cdot[(\alpha_2'-\alpha_2)^{-1}(\alpha_1'-\alpha_1)-1]^{-1}.\end{aligned} \tag{10}$$

Sličnim postupkom dobijamo

$$\begin{aligned}\beta_3 =&\{\beta_3'[(\alpha_3'-\alpha_3)^{-1}(\alpha_1'-\alpha_1)-(\alpha_3'-\alpha_1')^{-1}(\alpha_3-\alpha_1)] \\ &\beta_1'[(\alpha_3'-\alpha_1')^{-1}(\alpha_3-\alpha_1)-1]\}\cdot[(\alpha_3'-\alpha_3)^{-1}(\alpha_1'-\alpha_1)-1]^{-1}\end{aligned} \tag{11}$$

i

$$\begin{aligned}\beta_1 = \{&-\beta_1'[(\alpha_1'-\alpha_1)^{-1}(\alpha_3'-\alpha_3)-(\alpha_3'-\alpha_1')^{-1}(\alpha_3-\alpha_1)] \\ &+\beta_3'[(1-(\alpha_3'-\alpha_1')^{-1}(\alpha_3-\alpha_1))]\}\cdot[1-(\alpha_1'-\alpha_1)^{-1}(\alpha_3'-\alpha_3)]^{-1}.\end{aligned} \tag{12}$$

Kako važi da je $[1-(\alpha_1'-\alpha_1)^{-1}(\alpha_2'-\alpha_2)]^{-1} = [(\alpha_1'-\alpha_1)^{-1}(\alpha_1'-\alpha_1-\alpha_2'+\alpha_2)]^{-1} = (\alpha_1'-\alpha_1-\alpha_2'+\alpha_2)^{-1}(\alpha_1'-\alpha_1)$ jednakost (9) postaje

$$\begin{aligned}\beta_1 =&\{\beta_1'[(\alpha_1'-\alpha_1)^{-1}(\alpha_1'-\alpha_1-\alpha_2'+\alpha_2)+(\alpha_2'-\alpha_1')^{-1}(\alpha_1'-\alpha_1-\alpha_2'+\alpha_2)] \\ &+\beta_2'(\alpha_2'-\alpha_1')^{-1}(-\alpha_1'+\alpha_1+\alpha_2'-\alpha_2)\}\cdot(\alpha_1'-\alpha_1-\alpha_2'+\alpha_2)^{-1}(\alpha_1'-\alpha_1) \\ =&\{\beta_1'((\alpha_1'-\alpha_1)^{-1}+(\alpha_2'-\alpha_1')^{-1})-\beta_2'(\alpha_2'-\alpha_1')^{-1}\}\cdot(\alpha_1'-\alpha_1).\end{aligned} \tag{13}$$

Slično dobijamo za (12)

$$\beta_1 = \{\beta_1'((\alpha_1'-\alpha_1)^{-1}+(\alpha_3'-\alpha_1')^{-1})-\beta_3'(\alpha_3'-\alpha_1')^{-1}\}\cdot(\alpha_1'-\alpha_1). \tag{14}$$

Sada iz jednačina (13) i (14) dobijamo

$$\beta_1' = (\beta_2'(\alpha_2'-\alpha_1')^{-1}-\beta_3'(\alpha_3'-\alpha_1')^{-1})((\alpha_2'-\alpha_1')^{-1}-(\alpha_3'-\alpha_1')^{-1})^{-1}. \tag{15}$$

Iz (10) i (11) dobijamo

$$\beta_2 = \beta_1'(\alpha_2'-\alpha_1')^{-1}(\alpha_2'-\alpha_2)+\beta_2'[1-(\alpha_2'-\alpha_1')^{-1}(\alpha_2'-\alpha_2)]. \tag{16}$$

Slično

$$\beta_3 = \beta_1'(\alpha_3'-\alpha_1')^{-1}(\alpha_3'-\alpha_3)+\beta_3'[1-(\alpha_3'-\alpha_1')^{-1}(\alpha_3'-\alpha_3)], \tag{17}$$

pa je

$$\begin{aligned}\beta_3-\beta_2 =&\beta_1'[(\alpha_3'-\alpha_1')^{-1}(\alpha_3'-\alpha_3)-(\alpha_2'-\alpha_1')^{-1}(\alpha_2'-\alpha_2)] \\ &+\beta_3'[1-(\alpha_3'-\alpha_1')^{-1}(\alpha_3'-\alpha_3)]-\beta_2'[1-(\alpha_2'-\alpha_1')^{-1}(\alpha_2'-\alpha_2)].\end{aligned}$$

Kada zamenimo β_1' sa (10) i sredimo izraz dobijamo

$$\begin{aligned}&\beta_3-\beta_2 = -\beta_2'(\alpha_3'-\alpha_2')^{-1}(\alpha_3-\alpha_2)+\beta_3'(\alpha_3'-\alpha_2')^{-1}(\alpha_3-\alpha_2) \\ &\beta_3-\beta_2 = (\beta_3'-\beta_2')(\alpha_3'-\alpha_2')^{-1}(\alpha_3-\alpha_2) \\ &(\beta_3-\beta_2)(\alpha_3-\alpha_2)^{-1} = (\beta_3'-\beta_2')(\alpha_3'-\alpha_2')^{-1}\end{aligned} \tag{18}$$

što je i trebalo dokazati. ∎

Definicija 2.10 Afinu ravan u kojoj važi Dezargova teorema nazivamo **Dezargovom ravni**.

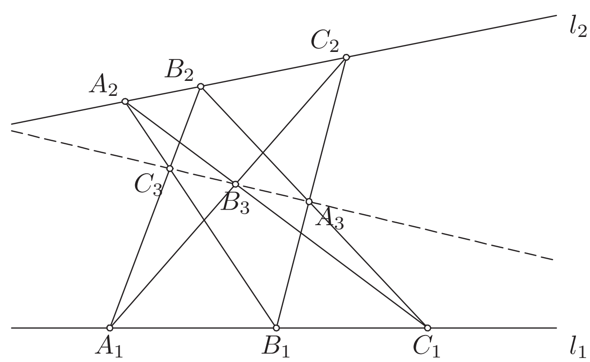
Dakle, afina ravan je Dezargova ako i samo ako je izgrađena nad telom.

Primer 2.11 Primer afine ravni izgrađene nad telom je Fanoova ravan nad $\mathbb{Z}_2^2$.

2.5.2 Paposova teorema i komutativni zakon

Navedimo sada još jedno tvrđenje koje može, a ne mora važiti u proizvoljnoj afinoj ravni, ali ga iz tradicionalnih razloga zovemo teoremom.

Teorema 2.23 *(Papos) Neka su A_1, B_1, C_1 tri različite tačke na pravoj l_1 i A_2, B_2, C_2 tri različite tačke na pravoj $l_2 \neq l_1$. Neka su redom A_3, B_3, C_3 preseci pravih $(B_1 + C_2) \cap (B_2 + C_1), (A_1 + C_2) \cap (A_2 + C_1)$ i $(A_1 + B_2) \cap (A_2 + B_1)$. Ako nijedna od tačaka $A_1, A_2, B_1, B_2, C_1, C_2$ nije zajednička za l_1 i l_2 onda su tačke A_3, B_3, C_3 kolinearne.*

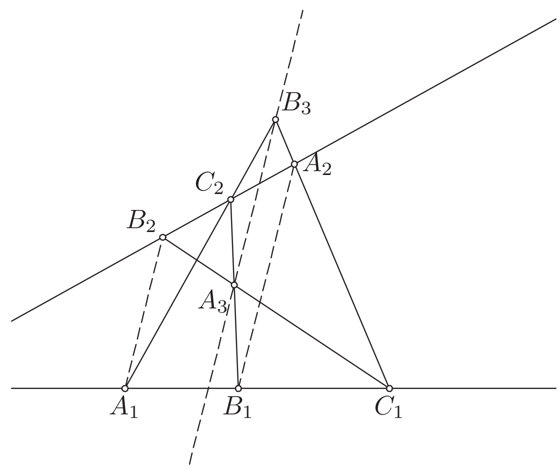


Sl. 2.10

Definicija 2.11 Ako u afinoj ravni važi Paposova teorema, onda tu ravan zovemo **Paposovom**.

Pokažimo, prvo neke direktne posledice Paposove teoreme. Neka su A_1, B_1, C_1 tri različite tačke na pravoj l_1 i A_2, B_2, C_2 tri različite tačke na pravoj $l_2 \neq l_1$.

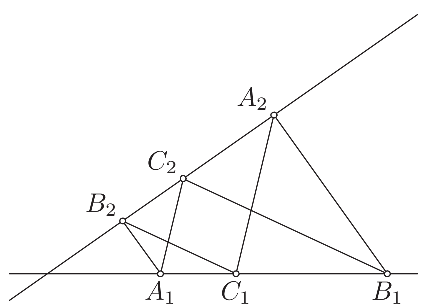
Lema 2.4 Neka se prave $(B_1 + C_2)$ i $(B_2 + C_1)$, odnosno $(A_1 + C_2)$ i $(A_2 + C_1)$ seku u tačkama A_3 i B_3, dok je $(A_1 + B_2) || (A_2 + B_1)$. Tada je i $(A_3 + B_3) || (A_1 + B_2)$.



Sl. 2.11

Dokaz: Pretpostavimo suprotno, neka se A_3+B_3 i A_1+B_2 seku u tački Z. Tada primenom Teoreme 2.23 na dve trojke kolinearnih tačaka A_3, B_2, C_1 i A_1, B_3, C_2 daje da su odgovarajuće presečne tačke Z, B_1 i A_2 kolinearne, odnosno (A_1+B_2) i (A_2+B_1) nisu paralelne. ∎

Lema 2.5 Neka je $(A_1+C_2)||(A_2+C_1)$ i $(A_1+B_2)||(A_2+B_1)$. Tada je i $(B_1+C_2)||(B_2+C_1)$.



Sl. 2.12

Dokaz: Pretpostavimo suprotno, neka se (B_1+C_2) i (B_2+C_1) seku u tački X. Neka je p prava takva da $X \in p$ i $p \parallel (A_1+C_2) \parallel (A_2+C_1)$. Na pravoj p postoji beskonačno mnogo tačaka W takvih da B_1+W seče A_2+B_2, i B_2+W seče B_1+A_1. Izaberimo jednu takvu tačku. Neka je $(B_1+W)\cap(A_2+B_2) = D_2$ i $(B_2+W)\cap(A_1+B_1) = D_1$.
Primenimo Paposovu teoremu na dve trojke kolinearnih tačaka B_1, C_1, D_1 i B_2, C_2, D_2. Tada su X, W i $(C_1+D_2)\cap(C_2+D_1) = V$ ili kolinearne ili $(X+W) \parallel (C_1+D_2) \parallel (C_2+D_1)$. Ako je $(X+W) \parallel (C_1+D_2)$, onda kako je $(X+W) \parallel (C_1+A_2)$ sledi da je $(C_1+A_2) \parallel (C_1+D_2)$ što je nemoguće, pa su X, W, V kolinearne, odnosno $V \in p$.
Neka je $(A_1+D_2)\cap p = T$, i neka je $(A_1+C_2)\cap(A_2+C_1) = J$ beskonačno daleka tačka. Primenimo Paposa na D_2, V, C_1 i J, A_1, C_2. Dobijamo da su tačke T, A_2, D_1 kolinearne, ali i T, A_1, D_2 su kolinearne, pa je $(A_2+D_1)\cap(A_1+D_2) =$

$T \in p$.
Na kraju primenimo Paposa na A_1, B_1, D_1 i A_2, B_2, D_2, dobijamo da je $(T + W) \parallel (A_1 + B_2) \parallel (A_2 + B_1)$. Ali $(T + W) \parallel (A_1 + C_2)$ što je kontradikcija.
∎

Uočimo i sledeće. Neka su date prave l_1 i l_2 i tačke A_1, B_1, C_1 prave l_1 i A_2, B_2 prave l_2. Neka se $(A_1 + B_2)$ i $(A_2 + B_1)$ seku u tački C_3 i neka je l_3 prava kroz C_3. Neka $(A_2 + C_1)$ i $(B_2 + C_1)$ seku l_3 u B_3 i A_3. Ako $(A_1 + B_3)$ seče l_2 u C_2 tada su i A_3, B_1, C_2 kolinearne. Zato, ako je $(A_1 + B_3)||l_2$ onda je i $(A_3 + B_1)||l_2$. Možemo formalno reći da se paralelne prave seku u (zamišljenoj) beskonačno dalekoj tački. Tada svakom pramenu paralelnih pravih odgovara tačno jedna takva tačka. Zato možemo reći da Paposova teorema važi i kada je jedna od tri kolinearne tačke beskonačno daleka.

Teorema 2.24 *Ako je afina ravan Paposova, onda je i Dezargova.*

Dokaz: Neka su A_1, B_1, C_1 i A_2, B_2, C_2 dve trojke nekolinearnih tačaka takvih da se $(A_1 + A_2)$, $(B_1 + B_2)$, $(C_1 + C_2)$ seku u tački P. Pretpostavimo da su parovi pravih $(C_1 + B_1)$ i $(C_2 + B_2)$, odnosno, $(A_1 + C_1)$ i $(A_2 + C_2)$ paralelni. Tada prava $(A_2 + C_2)$ seče $(A_1 + B_1)$ u nekoj tački S.
Pretpostavimo, prvo, da je $S \neq B_1$. Tada su S, B_1 i A_1 tri kolinearne tačke. Pretpostavimo i da $(P + S)$ nije paralelna sa $(B_1 + C_1)$, odnosno $(B_2 + C_2)$, i neka ih seče u T i V. Primenićemo Paposovu teoremu u nekoliko koraka

1. Trojke S, B_1, A_1 i C_1, P, C_2. S obzirom da je $(S + C_2)||(A_1 + C_1)$ i $T = (S + P) \cap (C_1 + B_1)$ sledi da se $(B_1 + C_2)$ i $(P + A_1)$ seku u nekoj tački U, takvoj da je $(T + U)||(S + C_2)||(A_1 + C_1)$.

2. Trojke P, B_2, B_1 i C_2, S, A_2. Direktno sledi da su prave $(V + U), (A_2 + B_2), (S + B_1)$ ili sve paralelne ili se seku u jednoj tački.

3. Trojke B_1, C_2, U i V, T, S. Kako je $(B_1 + T)||(V + C_2), (T + U)||(S + C_2)$ onda je i $(B_1 + S)||(V + U)$, pa je $(A_2 + B_2)||(B_1 + S)$.

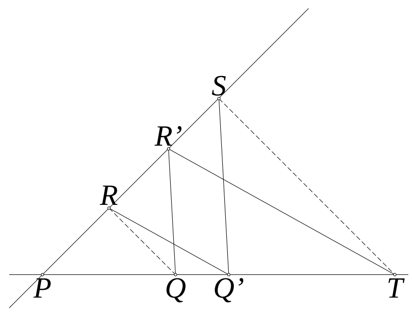
Ukoliko je $(P + S)||(B_1 + C_1)$ tada posmatramo iste trojke tačaka kao malo pre. Zaključak prethodnog koraka 1. je tada da je $(B_1 + C_2)||(P + A_1)$, a koraka 2. da je $(A_2 + B_2)||(B_1 + S)$.
Pretpostavimo, sada da je $S = B_1$. Neka je tada X_1 tačka prave $(B_1 + C_1)$ različita od B_1 i C_1. Tada prava $(P + X_1)$ seče $(B_2 + C_2)$ u tački X_2. Tada dve trojke nekolinearnih tačaka A_1, C_1, X_1 i A_2, C_2, X_2 zadovoljavaju uslove pod kojima smo tvrđenje dokazali, pa zaključujemo da je $(A_1 + X_1)||(A_2 + X_2)$. Zatim prethodni zaključak primenimo još jednom na trojke nekolinearnih tačaka A_1, X_1, B_1 i A_2, X_2, B_2 i zaključujemo $(A_1 + B_1)||(A_1 + B_1)$.

Ako su prave $(A_1 + A_2)$, $(B_1 + B_2)$ i $(C_1 + C_2)$ paralelne, možemo ponoviti prethodni postupak, uzimajući da je P beskonačno daleka tačka. ∎

Dakle, ako je ravan Paposova, onda je i Dezargova, te je izgrađena nad telom K. Obrnuto ne važi, odnosno, ako je ravan Dezargova, ne mora biti i Paposova. Pokazaćemo da je Dezargova ravan Paposova ako i samo ako je telo K komutativno.

Izaberimo proizvoljnu tačku P. Element $\alpha \neq 0$ tela K može se dobiti uz pomoć jedne i samo jedne dilatacije σ_α sa fiksnom tačkom P u obliku $\tau^\alpha = \sigma_\alpha \tau \sigma_\alpha^{-1}$. Ako je $\tau^\beta = \sigma_\beta \tau \sigma_\beta^{-1}$, onda $\tau^{\alpha\beta} = (\tau^\beta)^\alpha = \sigma_\alpha \sigma_\beta \tau \sigma_\beta^{-1} \sigma_\alpha^{-1} = \sigma_\alpha \sigma_\beta \tau (\sigma_\alpha \sigma_\beta)^{-1}$, a s druge strane $\tau^{\alpha\beta} = \sigma_{\alpha\beta} \tau \sigma_{\alpha\beta}^{-1}$.
Sad, kako je dilatacija σ jednoznačno određena elementom α, to je $\sigma_{\alpha\beta} = \sigma_\alpha \sigma_\beta$. To znači da je multiplikativna grupa nenula elemenata iz K izomorfna grupi dilatacija sa fiksnom tačkom P. Telo K je komutativno ako i samo ako je grupa dilatacija komutativna.

Izaberimo sada dve proizvoljne prave l i m koje prolaze kroz tačku P. Neka je $Q, Q \neq P$ proizvoljna tačka na pravoj l. Ako je σ_1 dilatacija sa fiksnom tačkom P, onda je prava l σ_1-trag, tačka $\sigma_1 Q = Q'$ je različita od P i po Aksiomi 4bP ona će biti tačka prave l. Tako jednačina $\sigma_1 Q = Q'$ potpuno određuje dilataciju σ_1. Slično, na pravoj m biramo tačke R i R', različite od P i zadajemo drugu dilataciju σ_2 jednačinom $\sigma_2 R = R'$.



Sl. 2.13

Konstruisaćemo prvo dve tačke: $S = \sigma_1 \sigma_2 R$ na pravoj m i $T = \sigma_2 \sigma_1 Q$ na pravoj l. One su jednoznačno date sledećim uslovima:

$$Q + R' \parallel \sigma_1 Q + \sigma_1 R' = Q' + \sigma_1 \sigma_2 R = Q' + S,$$

$$R + Q' \parallel \sigma_2 R + \sigma_2 Q' = R' + \sigma_2 \sigma_1 Q = R' + T.$$

Da bismo dokazali da je $\sigma_1 \sigma_2 = \sigma_2 \sigma_1$ potrebno je i dovoljno dokazati da je $\sigma_1 \sigma_2 Q = \sigma_2 \sigma_1 Q$ ili $\sigma_1 \sigma_2 Q = T$. Kako tačka $\sigma_1 \sigma_2 Q$ leži na pravoj l, ona zadovoljava uslove: $Q + R \parallel \sigma_1 \sigma_2 Q + \sigma_1 \sigma_2 R = \sigma_1 \sigma_2 Q + S$, i vidimo da je uslov za komutativnost $Q + R \parallel T + S$.

Teorema 2.25 *Telo K je komutativno ako i samo ako u datoj afinoj ravni važi Paposova teorema.*

Ako geometrija sadrži konačan broj tačaka onda je grupa $\mathbf{T}$ konačna i telo K konačno, pa i komutativno.

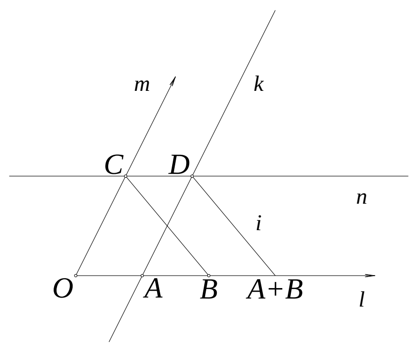
Primer 2.12 U ravnima $\mathbb{R}^2$ i $\mathbb{Z}_p^2$, gde je p prost broj, važi Paposova teorema.

Teorema 2.26 *U Dezargovoj ravni koja se sastoji od konačnog broja tačaka važi Paposova teorema.*

2.6 Konstrukcije zbira i proizvoda

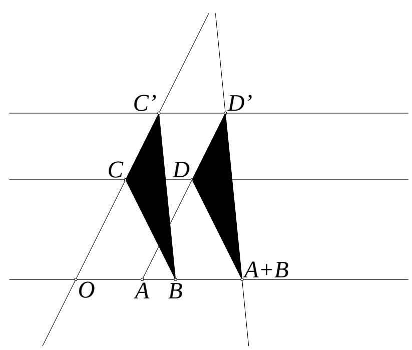
Pretpostavimo da u datoj ravni važi Dezargova teorema. Neka su l i m ose u afinoj ravni i $O = l \cap m$ koordinatni početak i neka su date tačke A i B sa ose l. Ilustrujmo konstrukciju zbira $A + B$:

1. Neka je $C \in m$.
2. Neka je n prava kroz C paralelna sa l.
3. Neka je k prava kroz A paralelna ili jednaka sa m.
4. Neka je $D = n \cap k$.
5. Neka je i prava kroz D paralelna ili jednaka sa pravom BC.
6. Tada je tačka $i \cap l$ zbir tačaka A i B.



Sl. 2.14

Zbir $Z = A + B$ ne zavisi od izbora tačke C, odnosno od izbora prave n.



Sl. 2.15

Neka su C' i D' drugi par odgovarajućih tačaka. Po konstrukciji je $C + B \parallel D + Z$ i $C + C' \parallel D + D'$ i prave $l = O + Z, n = C + D$ i $n' = C' + D'$ su paralelne, pa je po Dezargovoj teoremi $C' + B \parallel D' + Z$, odnosno dobijamo opet istu presečnu tačku Z.

Konstruišimo proizvod dve tačke $A \cdot B$. Izaberimo fiksnu tačku I, tačku jedinice, različitu od O.

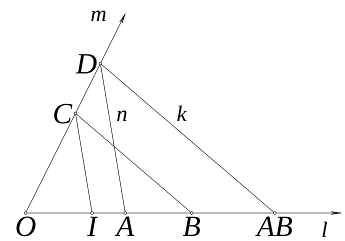
1. Izaberimo $C \in m$.

2. Neka je n prava kroz A paralelna ili jednaka sa pravom $I + C$.

3. Neka je $D = n \cap m$.

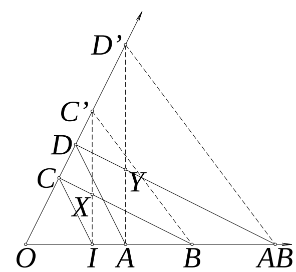
4. Neka je k prava kroz D paralelna ili jednaka sa $B + C$.

5. Tačka $P = k \cap l$ je proizvod tačaka A i B.



Sl. 2.16

Pokažimo da proizvod $A \cdot B$ na zavisi od izbora tačke C.
Na slici 2.17 je punim linijama predstavljena konstrukcija množenja uz pomoć tačke C, a isprekidanim linijama konstrukcija množenja pomoću tačke C'.



Sl. 2.17

Neka je $X = (I + C') \cap (C + B), Y = (A + D') \cap (A + B)$. Posmatrajmo trouglove IXC i AYD: $IX \parallel AY$ (po konstrukciji proizvoda uz pomoć tačke C'), $CX \parallel DY, IC \parallel AD$ (po konstrukciji proizvoda uz pomoć tačke C) pa na osnovu Dezargove teorema sledi da su prave l, XY, m ili paralelne ili se seku. Kako se l i m seku u tački O, sledi da se l, m, XY seku u tački O.

Neka je proizvod A i B pomoću tačke C' tačka P'. Posmatrajmo trouglove $BC'X$ i $P'D'Y$. Kako se prave BP', $C'D'$, XY seku u tački O to po Dezargovoj teoremi sledi da je $P' = P$.

Tačka I je jedinica dužine na osi l i pozicija proizvoda AB zavisi od izbora te tačke. Na primer, $AB = B$ ako je $A = I$ ali $AB \neq B$ ako je $A \neq I$.

2.7 Afini prostor

Afina ravan je samo specijalni primer jedne veće klase geometrija, a to su n-dimenzioni afini prostori. Navešćemo ovde aksiome trodimenzionog prostora. Osnovni pojmovi ove geometrije su skup čije elemente nazivamo tačkama i dve klase podskupova koje nazivamo pravama i ravnima. Kažemo da su tačke kolinearne ako pripadaju jednoj pravoj, a komplanarne su ako pripadaju istoj ravni. Ako se prave poklapaju ili su disjunktne, a komplanarne kažemo da su paralelne. Ovi pojmovi treba da zadovolje sledeće aksiome.

- Dve različite tačke su incidentne sa tačno jednom pravom.
- Svaka prava je incidentna sa bar dve tačke.
- Tri nekolinearne tačke su incidentne sa tačno jednom ravni.
- Ako dve tačke prave pripadaju ravni, onda sve tačke prave pripadaju ravni.
- Ako dve ravni imaju bar jednu zajedničku tačku, onda imaju bar još jednu zajedničku tačku.
- Postoje četiri nekomplanarne tačke.
- Za datu pravu i tačku postoji tačno jedna prava incidentna sa tačkom i paralelna datoj pravoj.

Očigledno svaka ravan u afinom prostoru zadovoljava aksiome afine ravni. Međutim tada ona mora biti Dezargova. Navešćemo, bez dokaza, neke od direktnih posledica ovih aksioma koje će nam biti neophodne da dođemo do ovog zaključka.

- Postoji tačno jedna ravan koja sadrži dve prave koje se seku.
- Ako dve različite ravni nisu disjunktne, onda se seku po pravoj. Ako se ravni poklapaju, ili su disjunktne onda kažemo da su paralelne.
- Relacija paralelnosti pravih, kao i relacija paralelnosti ravni su relacije ekvivalencije.
- Ako neka ravan seče dve paralelne ravni, onda ih seče po paralelnim pravama.
- Ako su $l_1||l_2$ i $p_1||p_2$ dva para paralelnih pravih, takvih da se l_1 i p_1 seku onda ravni koje sadrže prave l_1 i p_1, odnosno l_2 i p_2 su paralelne.

Pokažimo da u afinom prostoru važi Dezargova teorema.

Teorema 2.27 *Neka su A_1, B_1, C_1 i A_2, B_2, C_2 dve trojke nekolinearnih tačaka takvih da su $(A_1 + A_2)$, $(B_1 + B_2)$ i $(C_1 + C_2)$ tri prave koje su ili paralelne ili se seku u jednoj tački i neka je $(C_1 + A_1)||(C_2 + A_2)$ i $(C_1 + B_1)||(C_2 + B_2)$. Tada je $(B_1 + A_1)||(B_2 + A_2)$.*

Dokaz: Postoje ravni α i β koje sadrže, redom, trojke tačaka A_1, B_1, C_1 i A_2, B_2, C_2. Kako je $(C_1 + A_1)||(C_2 + A_2)$ i $(C_1 + B_1)||(C_2 + B_2)$ sledi da su ravni α i β paralelne. Pretpostavimo, prvo da je $\alpha \neq \beta$. Postoji ravan koja sadrži $(A_1 + A_2)$ i $(B_1 + B_2)$. Ona seče α i β po disjunktnim, ali komplanarnim

pravama, i to $(B_1 + A_1)$ i $(B_2 + A_2)$ pa su one paralelne.
Neka je sada $\alpha = \beta$. Postoji tačka P_1 koja ne pripada α.

Neka se $(A_1 + A_2)$, $(B_1 + B_2)$ i $(C_1 + C_2)$ seku u P. Postoji ravan koja sadrži $(A_2 + A_1)$ i $(P + P_1)$. Prava koja sadrži A_2 i paralelna je $(P + P_1)$ joj pripada i nije paralelna sa $(A_1 + P_1)$, pa je seče u tački A. Slično, prave kroz B_2 i C_2 paralelne $(P + P_1)$ redom seku $(B_1 + P_1)$ i $(C_1 + P_1)$ u tačkama B i C. Pri tom, tačke A, B, C ne pripadaju ravni α i $(C + B)||(C_1 + B_1)$ i $(C + A)||(C_1 + A_1)$, te trojke tačaka A, B, C i A_1, B_1, C_1 ispunjavaju uslove teoreme, a nisu u istoj ravni, pa je $(A + B)||(A_1 + B_1)$. Slično zaključujemo i da je $(A + B)||(A_2 + B_2)$, pa je i $(A_2 + B_2)||(A_1 + B_1)$.

Ako su prave $(A_1 + A_2)$, $(B_1 + B_2)$ i $(C_1 + C_2)$ paralelne možemo posmatrati pravu kroz P paralelnu $(A_1 + A_2)$. Postoji na njoj bar još jedna tačka P_1. Tačke A_1, A_2, P, P_1 pripadaju jednoj ravni pa se neki od parova pravih $(A_1 + P), (A_2 + P_1)$ ili $(A_1 + P_1), (A_2 + P)$ seku. Neka se $(A_1 + P)$ i $(A_2 + P_1)$ seku u A. Tada se i $(B_1 + P)$ i $(B_2 + P_1)$ seku u B, i $(C_1 + P)$ i $(C_2 + P_1)$ seku u C. Tada je $(B_1 + C_1)||(B + C)$ i $(A_1 + C_1)||(A + C)$, pa možemo dokazano primeniti na trojke A_1, B_1, C_1 i A, B, C, te važi $(A + B)||(A_1 + B_1)$. Slično $(A + B)||(A_2 + B_2)$, pa važi tvrđenje. ∎

Dakle, ako je afina ravan podskup nekog afinog prostora (i njena afina struktura je nasleđena iz tog prostora) tada u njoj mora važiti Dezargova teorema. Zato ima smisla afine strukture koje ne zadovoljavaju Dezargovu teoremu tražiti isključivo među ravnima.

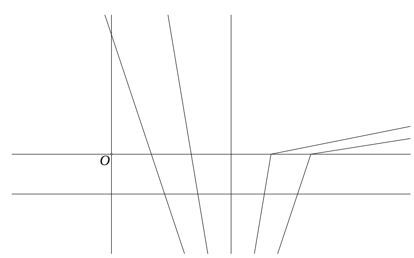
3 Primeri ne-Dezargovih i ne-Paposovih ravni

Navešćemo sada primere različitih afinih ravni sa osvrtom na to da li u njima važi Dezargova i Paposova teorema. Najčešći primer afine ravni je ravan $\mathbb{R}^2$ izgrađena nad poljem $\mathbb{R}$ i samim tim i Dezargova i Paposova. Takva je i ravan $\mathbb{C}^2$ izgrađena nad kompleksnim brojevima. Uopštavanjem kompleksnih brojeva dobijamo kvaternione $\mathbb{H}$. Ovaj prsten sa delenjem jeste telo, pa je ravan $\mathbb{H}^2$ Dezargova. Međutim to telo nije komutativno pa ravan $\mathbb{H}^2$ nije Paposova. Daljim uopštavanjem dobijamo oktonione. Međutim struktura $\mathbb{O}$ nije ni asocijativna te je ravan $\mathbb{O}^2$ ne-Dezargova. Ipak, kvaternioni i oktonioni su 4-dimenzioni i 8-dimenzioni realni vektorski prostori. Sada ćemo pažnju posvetiti ne-Paposovoj i ne-Dezargovoj afinoj ravni koju možemo vizuelizovati.

3.1 Ravan Multona

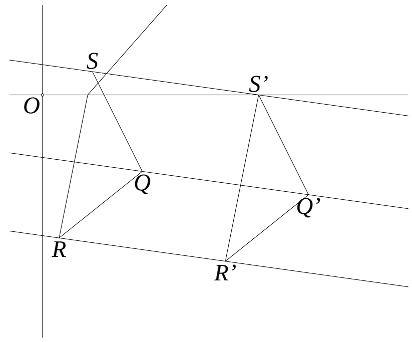
Posmatrajmo ravan $\mathbb{R}^2$ izgrađenu nad realnim brojevima. Neka su l i m ose. Tada, prave, kao i u svim ostalim ravnima, mogu biti horizontalne, vertikalne, ili sa koeficijentom a koji može biti pozitivan ili negativan. Nazovimo ih *običnim pravama.* Ako je prava p_1 sa pozitivnim koeficijentom $a > 0$, ona seče l osu u nekoj tački X. Postoji i prava p_2 koja sadrži X, i ima koeficijent $\frac{a}{2}$. Posmatrajmo uniju tačaka prave p_1 koje imaju drugu koordinatu negativnu i tačaka prave p_2 koje imaju drugu koordinatu nenegativnu (dakle, uniju dve poluprave sa zajedničkim temenom X). Ovakvu uniju nazovimo *izlomljenom pravom.*

Tačke Multonove ravni su elementi $\mathbb{R}^2$. Prave Multonove ravni su obične horizontalne, vertikalne i prave čiji je koeficijent pravca $a < 0$, kao i izlomljene prave koje su imale pozitivan koeficijent (videti sliku 3.1).



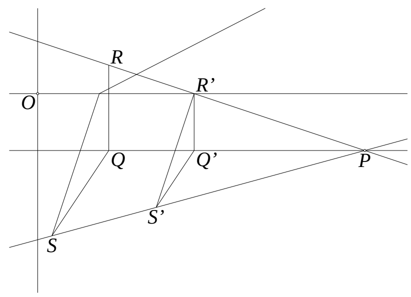
Sl. 3.1

Nije teško uočiti da Multonova ravan zadovoljava aksiome afine ravni. Međutim ona nije Dezargova. Kako neizlomljene prave (afine ravni $\mathbb{R}$) zadovoljavaju Dezargovu teoremu, dovoljno je uočiti slučaj gde je jedna od pravih sa pozitivnim koeficijentom, te nakon *izlomljavanja* više nije incidentna sa traženom tačkom. Na slici 3.2 je prikazan takav slučaj kada su $Q + Q'$, $R + R'$, $S + S'$ paralelne.



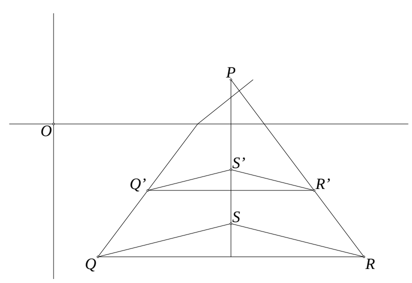
Sl. 3.2

Na slici 3.3 je prikazan sličan slučaj ali takav da se $Q+Q'$, $R+R'$, $S+S'$ seku u tački P.



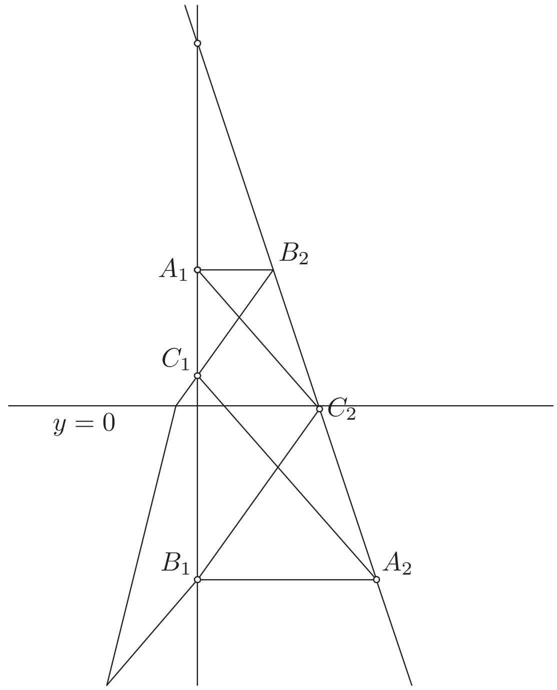
Sl. 3.3

Drugi način da pokažemo da Dezargova teorema ne važi u Multonovoj ravni jeste da pokažemo da obrnuta Dezargova teorema ne važi, odnosno da postoji slučaj u kom $Q+R \parallel Q'+R'$, $Q+S \parallel Q'+S'$ $R+S \parallel R'+S'$ da se tada prave $Q+Q'$, $R+R'$, $S+S'$ ne seku u jednoj tački.



Sl. 3.4

Samim tim u Multonovoj ravni ne važi ni Paposova teorema. Jedan geometrijski primer je dat na slici 3.5.



Sl. 3.5

3.2 Halovo kvazipolje

U ovom i sledećim odeljcima pokazaćemo konstrukcije ternarnih prstena koji nisu tela ili barem nisu komutativne strukture.

Neka je F polje i $f(s) = s^2 - as - b$ nesvodljivi polinom nad F. Neka je H dvodimenzionalni desni vektorski prostor nad poljem F, sa baznim elementima 1 i λ tako da H sadrži sve elemente oblika $x + \lambda y$ gde $x, y \in F$. Tada F identifikujemo sa skupom $\{x + \lambda 0 | x, y \in F\}$. Pretpostavimo sledeće:

1. svaki element α iz H koji nije iz F (odnosno koji nije oblika $x + \lambda 0$) zadovoljava kvadratnu jednačinu $f(\alpha) = 0$;

2. F je u jezgru od H;

3. svaki element iz F u množenju komutira sa svim elementima iz H.

Pretpostavimo da postoji kvazipolje Q koje je dvodimenzionalni vektorski prostor nad F tako da njegovo množenje zadovoljava uslove 1, 2 i 3.

Neka je $1, \lambda$ baza za Q kao vektorskog prostora nad F, Q sadrži elemente oblika $x + \lambda t$. Ako je $y \neq 0$ onda, kako je F u jezgru od Q, trebalo bi da možemo zapisati proizvoljni element

$$(z + \lambda t) = (x + \lambda y)y^{-1}t + z - xy^{-1}t,$$

pa kada sa leve strane pomnožimo sa $(x + \lambda y)$ dobijamo

$$\begin{aligned}(x + \lambda y)(z + \lambda t) &= (x + \lambda y)[(x + \lambda y)y^{-1}t + z - xy^{-1}t] \\ &= (x + \lambda y)^2 y^{-1}t + (x + \lambda y)(z - xy^{-1}t).\end{aligned}$$

Po pretpostavci je $f(\alpha) = 0, \ \ \alpha = x + \lambda y$, pa $f(x + \lambda y) = 0$ pa je

$$(x + \lambda y)^2 = a(x + \lambda y) + b.$$

Sledi

$$(x + \lambda y)(z + \lambda t) = [a(x + \lambda y) + b]y^{-1}t + (x + \lambda y)(z - xy^{-1}t)$$

ili

$$(x + \lambda y)(z + \lambda t) = axy^{-1}t + a\lambda t + by^{-1}t + xz - x^2y^{-1}t + \lambda yz - \lambda xt,$$

odnosno

$$(x + \lambda y)(z + \lambda t) = xz - y^{-1}t(x^2 - ax - b) + \lambda(at + yz - xt),$$

odnosno

$$(x + \lambda y)(z + \lambda t) = xz - y^{-1}tf(x) + \lambda(at + yz - xt). \tag{19}$$

Sada, zbog (19), množenje u H možemo definisati sa :

$$\text{Ako je } y \neq 0, \ \ (x + \lambda y)(z + \lambda t) = xz - y^{-1}tf(x) + \lambda(at + yz - xt) \tag{20}$$

$$\text{ako je } y = 0, \ \ x(z + \lambda t) = xz + \lambda(xt). \tag{21}$$

Sa (20) i (21) je definisano množenje za H, pa sada treba da pokažemo da su aksiome kvazipolja zadovoljene.
Pokazaćemo prvo da važi levi distributivni zakon, tj. za neke elementi $\alpha, \beta, \gamma \in H$ treba da važi $\alpha(\beta+\gamma) = \alpha\beta+\alpha\gamma$. Neka je $\alpha = x+\lambda y, \ \beta = z+\lambda t, \ \gamma = h+\lambda k$, tada

$$\begin{aligned}
\alpha(\beta + \gamma) &= (x + \lambda y)((z + \lambda t) + (h + \lambda k)) = (x + \lambda y)((z + h) + \lambda(t + k)) \\
&= x(z + h) - y^{-1}(t + k)f(x) + \lambda(y(z + h) - x(t + k) + a(t + k)) \\
&= xz - y^{-1}tf(x) + \lambda(yz - xt + at) + xh - y^{-1}kf(x) + \lambda(yh - xk + ak) \\
&= (x + \lambda y)(z + \lambda t) + (x + \lambda y)(h + \lambda k) \\
&= \alpha\beta + \alpha\gamma.
\end{aligned}$$

Sabiranje u H je komutativno, i pišući 0 za $0 + \lambda 0$, jasno je da $0(x + \lambda y) = 0x + \lambda(0y) = 0$.

Da bismo pokazali da je H slabo kvazipolje, treba da pokažemo da je $(H^*, \cdot)$ petlja. Jasno je da je $1 = 1 + \lambda 0$ njegov identitet.

Kako bismo rešili $(x + \lambda y)(z + \lambda t) = p + \lambda q$, $x + \lambda y \neq 0$ za $z + \lambda t$ moramo rešiti linearne jednačine

$$xz - y^{-1}tf(x) = p, \quad at + yz - xt = q \tag{22}$$

za $y \neq 0$ i

$$xz = p, \quad xt = q$$

za $y = 0$.

Ako je $y = 0$ onda, kako $x + \lambda y \neq 0$, $x \neq 0$, pa su $z = x^{-1}p$, $t = x^{-1}q$ jedinstvena rešenja.
Ako je $y \neq 0$, $-b$ ne može biti nula, jer u protivnom $f(s) = s^2 - as$ bi bio svodljiv, pa iz jednakosti (22) kada prvu jednačinu pomnožimo sa y a drugu sa x sa leve strane i kada ih oduzmemo, dobijamo da je $t = (yp - xq)b^{-1}$, $z = y^{-1}(q + xt - at)$.

Ostaje još da se reši $(x + \lambda y)(z + \lambda t) = p + \lambda q$ za x i y takve da $z + \lambda t \neq 0$.
Ako je $t = 0$ onda, kako je $z + \lambda t \neq 0$, $z \neq 0$ i rešenje je $y = 0$ ako i samo ako je $q = 0$, i u tom slučaju je rešenje $y = 0 (= qz^{-1})$, $x = pz^{-1}$.
Za $z = 0$ rešenje je $y = 0$ ako i samo ako $p = 0$, pa je rešenje $y = 0$, $x = qt^{-1}$.
Ako je $t \neq 0 \neq z$ onda je rešenje $y = 0$, $x = pz^{-1}$ ako i samo ako $pz^{-1} = qt^{-1}$.
Ostaje još da pokažemo da ako je ili $z = 0$ i $p = 0$, ili $t = 0$ i $q = 0$, ili $pz^{-1} = qt^{-1}$ onda ne postoji rešenje za $y \neq 0$, a da u bilo kom drugom slučaju postoji jedinstveno rešenje za $y \neq 0$.

Množenjem prve jednačine u (22) sa y, druge sa x i oduzimajući ih dobijamo

$$bt = py - qx. \tag{23}$$

Kombinujući (23) sa drugom jednačinom u (22) dobijamo sledeće dve linearne jednačine čija su rešenja po x i y ista kao i za (22):

$$py - qx = bt \quad zy - tx = q - at. \tag{24}$$

Ako je $t = 0$ onda (24) ima jedinstveno rešenje $y = qz^{-1}$, $x = pz^{-1}$, za koje je $y = 0$ ako i samo ako $q = 0$.
Ako je $t \neq 0$ množenjem druge jednačine u (24) sa qt^{-1} i oduzimajući je od prve, dobijamo $y(p - qt^{-1}z) = bt - q^2t^{-1} + aq$ odnosno

$$y(pt - qz) = -t^2 f(qt^{-1}). \tag{25}$$

Kako je $t \neq 0$ i $f(s)$ je nesvodljiv nad F, desna strana u (25) je uvek različita od nule. Zato, ako je $pt - qz = 0$, odnosno ako je ili $p = 0$ i $z = 0$ ili $z \neq 0$ i $pz^{-1} = qt^{-1}$, onda je jednačina (24) nerešiva i zato (22) nema rešenje za $y \neq 0$.
Konačno, ako je $pt - qz \neq 0$ onda $y = -t^2 f(qt^{-1})(pt - qz)^{-1} \neq 0$ što se i tražilo.

Do sada smo pokazali da je H slabo kvazipolje. Međutim, jasno je iz definicije množenja da je F u jezgru od H i kako je H dvodimenzionalni vektorski prostor nad F, Teorema 1.6 dokazuje tvrđenje da je H kvazipolje.

Halovo kvazipolje, kako ćemo nazvati sistem koji smo upravo definisali, uglavnom ne može biti polje. Ako bi H bilo polje, onda bi svi njegovi elementi van potpolja F zadovoljavali istu kvadratnu jednačinu, a kako kvadratna jednačina ima najviše dve nule u bilo kom polju, H bi posedovalo najviše dva elementa izvan F, i F bi bilo $GF(2)$. Obratno, ako $F = GF(2)$ onda je H reda 4. Sledi da je H polje ako i samo ako je $F = GF(2)$.

Afine ravni koordinatizovane pomoću Halovog kvazipolja zvačemo Halove ravni, one su ne-Dezargove u slučaju kada im je red veći od 4.

3.3 Andreovo kvazipolje

Neka je F polje, Γ konačna grupa automorfizama od F i K potpolje polja F koje sadrži sve elemente koje Γ fiksira. Tada je dimenzija od F nad K jednaka redu od Γ, a to znači da je konačna. Neka je ν normirano preslikavanje definisano pomoću Γ na sledeći način

$$x^\nu = \prod_{\alpha\in\Gamma} x^\alpha$$

Jasno, $x^\nu \in K\ \forall x \in K$ i ν je homomorfizam iz F^* u K^*.

Neka $N = (F^*)^\nu$, i neka je ϕ neko preslikavanje iz N u Γ koje preslikava jedinični element iz F^* u jedinični element iz Γ. U opštem slučaju ϕ ne mora biti homomorfizam. Kompozicijom ν i ϕ dobijamo preslikavanje $\alpha = \nu\phi$ iz F^* u Γ. Za bilo koji $x \in F^*$ pisaćemo α_x za x^α da bismo istakli činjenicu da je x^α automorfizam u Γ.

Sada definišemo sistem F_ϕ na sledeći način: elementi iz F_ϕ su elementi iz F, sabiranje u F_ϕ je isto kao u F, dok je množenje $\odot$ definisano:

$$x \odot y = xy^{\alpha_x},\ \ 0 \odot y = 0\ \ \forall x, y \in F,\ \ x \neq 0. \tag{26}$$

Teorema 3.1 *F_ϕ je kvazipolje.*

Dokaz: $(F_\phi, +)$ je Abelova grupa jer je $(F, +)$ Abelova.
Rešimo jednačinu $x \odot y = z$; tj. $xy^{\alpha_x} = z$. Ako su x i z dati, onda je $y = (x^{-1}z)^{\alpha_x^{-1}}$ jedinstveno rešenje. S druge strane, ako su y i z dati onda ćemo α_x odrediti tako što ćemo koristiti činjenicu da je $(x^\beta)^\nu = x^\nu$ za svako $\beta \in \Gamma$ i svako $x \in F$: ako $x \odot y = z$ onda je $(x \odot y)^\nu = z^\nu$. Ali važi $(x \odot y)^\nu = (xy^{\alpha_x})^\nu = x^\nu (y^{\alpha_x})^\nu = x^\nu y^\nu$, pa je $x^\nu = (zy^{-1})^\nu$ i $\alpha_x = \alpha_w$, gde $w = zy^{-1}$. Dakle, bilo koje rešenje x mora zadovoljavati $x = zy^{-\alpha_w}$ gde $w = zy^{-1}$. Lako je uočiti da je takvo x rešenje.
Konačno, $x \odot 1 = x1^{\alpha_x} = x$ i $1 \odot x = 1x^{\alpha_1} = x$, jer $\alpha_1 = 1^\alpha = \epsilon$, gde je ϵ jedinični element iz Γ, pa je $(F_\phi^*, \odot)$ petlja.
Kako $x \odot (y + z) = x(y + z)^{\alpha_x} = x(y^{\alpha_x} + z^{\alpha_x}) = xy^{\alpha_x} + xz^{\alpha_x} = x \odot y + x \odot z$, sledi da F_ϕ zadovoljava levi distributivni zakon.

Primetimo da $a^{\alpha_x} = a$ za neko $x \in F, a \in K$ jer su u K svi fiksirani elementi iz Γ. Ako je k bilo koji element iz K onda $x \odot k = xk$, $\forall x \in F$ i lako je videti da je K sadržano u jezgru od F_ϕ; dakle F_ϕ je slabo kvazipolje koje je konačno dimenziono nad svojim jezgrom i po Teoremi 1.6 ono je kvazipolje, koje nazivamo Andreovo kvazipolje. ∎

Sledeće dve leme pokazuju da u levom Andreovom kvazipolju množenje gotovo nikad nije asocijativno i da desni distributivni zakon važi samo ako je ϕ trivijalno preslikavanje koje svaki element slika u $1 \in \Gamma$.

Lema 3.1 Andreovo kvazipolje F_ϕ je asocijativno ako i samo ako je ϕ antihomomorfizam (multiplikativne) grupe N u Γ.

Dokaz: Imamo

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

jer $(xy^{\alpha_x})^\alpha = (x \odot y)^\alpha = (xy)^\alpha$. Dakle, asocijativnost u F_ϕ zahteva da $\alpha_{xy} = \alpha_y \alpha_x$, pa je α antihomomorfizam; ali ν je homomorfizam pa ϕ mora biti antihomomorfizam. ∎

Lema 3.2 Neka je F_ϕ Andreovo kvazipolje. Tada su sledeći iskazi ekvivalentni:

1. F_ϕ je prsten sa deljenjem,
2. F_ϕ je polje,
3. F_ϕ je izomorfno sa F,
4. $k^\phi = \epsilon$, $\forall k \in N$, gde je ϵ identitet iz Γ.

Dokaz: Pretpostavimo da je F_ϕ prsten sa deljenjem. Tada F_ϕ zadovoljava desni distributivni zakon tako da $\forall a, b, x \in F^*$ imamo

$$ax^\alpha + bx^\beta = (a+b)x^\lambda \tag{27}$$

gde je $\alpha = \alpha_a,\ \beta = \alpha_b,\ \lambda = \alpha_{a+b}$. Ako su a i b fiksni, (27) je identitet po x i onda, zamenivši x sa xy, imamo

$$a(x^\alpha y^\alpha) + b(x^\beta y^\beta) = (a+b)(x^\lambda y^\lambda) = [(a+b)x^\lambda]y^\lambda. \tag{28}$$

Iz (27) i (28) dobijamo

$$ax^\alpha y^\alpha + bx^\beta y^\beta = (ax^\alpha + bx^\beta)y^\lambda. \tag{29}$$

Ako pomnožimo obe strane u (29) sa $(a+b)$ i iskoristimo (27) tako što x zamenimo sa y, dobijamo

$$(a+b)(ax^\alpha y^\alpha + bx^\beta y^\beta) = (ax^\alpha + bx^\beta)(ay^\alpha + by^\beta). \tag{30}$$

Kada izmnožimo obe strane u (30) i iskoristimo činjenicu da $ab \neq 0$ dobijamo

$$x^\alpha y^\alpha + x^\beta y^\beta = x^\alpha y^\beta + x^\beta y^\alpha, \tag{31}$$

što implicira i da je $(x^\alpha - x^\beta)(y^\alpha - y^\beta) = 0,\ \forall x, y \in F$. Dakle, važi $x^\alpha = x^\beta,\ \forall x \in F$ što povlači $\alpha_a = \alpha_b,\ \forall a, b \in F^*$. Ali važi i $\alpha_1 = \epsilon$, pa je $\alpha_a = \epsilon,\ \forall a \in F^*$. Dakle, 1) povlači 2), 3) i 4), a jasno je i da svaki od 2), 3) i 4) povlači 1). ∎

3.4 Klasa prstena sa deljenjem

Neka je F telo sa centrom Z (Z je polje), i neka je θ antiautomorfizam od F konačnog reda m i $a, b \in F$ tako da

- F ima konačnu dimenziju nad Z i xx^θ je u Z za sve x iz F.
- $a = x^{1+\theta} + xb$ nema rešenje za x iz F.

Ako je $xx^\theta = y$, tada je $x^\theta = x^{-1}y = yx^{-1}$ jer je $y \in Z$, pa je $xx^\theta = y = x^\theta x$ i možemo pisati $x^{1+\theta} = x^{\theta+1} = xx^\theta$.

Sada neka je D dvodimenzionalni vektorski prostor nad F sa baznim elementima 1 i λ. Definisaćemo množenje u D tako da, zajedno sa sabranjem u vektorskom prostoru, ono postane prsten sa deljenjem. Množenja je dato sa:

$$(x + \lambda y)(z + \lambda t) = (xz + aty^\theta) + \lambda(zy + x^\theta t + y^\theta bt). \tag{32}$$

Teorema 3.2 *D je prsten sa deljenjem.*

Dokaz: Jasno je da je množenje sleva i zdesna aditivno (tj. $(x+y)T = xT + yT$ gde T može biti i levo i desno množenje) i zbog toga D zadovoljava oba distributivna zakona.

Kako θ ima red m kao antiautomorfizam od F, i kako θ mora da fiksira Z, ono ima red koji deli m, budući da je automorfizam od Z. Ako je K potpolje od Z koje sadrži elemente fiksirane pomoću θ, onda Z ima konačnu dimenziju nad K, pa F ima konačnu dimenziju nad K. Neka je z dimenzija od F nad K. Onda D ima dimenziju $2z$ nad K, i K je u centru od D. Kako je D konačno dimenzioni vektorski prostor nad svojim centrom, treba pokazati da jednačina $(x+\lambda y)(z+\lambda t) = (p+\lambda q)$ ima jedinstveno rešenje za jedan činilac sa leve strane, pri čemu su dati drugi činilac i $(p+\lambda q)$, odnosno treba pokazati da jedino rešenje za $(x+\lambda y)(z+\lambda t) = 0$ je $x+\lambda y = 0$ ili $z+\lambda t = 0$. Stavljajući da desna strana u (32) bude jednaka 0 dobijamo:

$$xz + aty^\theta = 0, \quad zy + x^\theta t + y^\theta bt = 0. \tag{33}$$

Množenjem prve jednačine u (33) sa desna sa y, a druge sa leva sa x i oduzimajući ih dobija se

$$aty^{1+\theta} - x^{1+\theta}t - xy^\theta bt = 0. \tag{34}$$

Ako je $t = 0$, jednačina (33) daje $xz = zy = 0$ pa ili $x = y = 0$ ili $z = 0$. Možemo pretpostaviti da je $t \neq 0$ i onda kako je $y^{1+\theta}$ u Z, (34) postaje

$$ay^{1+\theta} - x^{1+\theta} - xy^\theta b = 0. \tag{35}$$

Ako $y = 0$ onda (35) povlači da je $x = 0$, pa pretpostavimo da $y \neq 0$. Neka je $x = x_1 y$ tako da $x^\theta = y^\theta x_1^\theta$.Tada $x^{1+\theta} = x_1 y^{1+\theta} x_1^\theta = x_1^{1+\theta} y^{1+\theta}$, jer $y^{1+\theta}$ je u Z. Sada (35) postaje $ay^{1+\theta} - x_1^{1+\theta} y^{1+\theta} - x_1 y^{1+\theta} b = 0$ ili

$$(a - x_1^{1+\theta} - x_1 b) y^{1+\theta} = 0. \tag{36}$$

Prvi faktor u (36) ne može biti 0 na osnovu drugog uslova koji smo naveli na početku poglavlja, pa je $y^{1+\theta}$ jedino rešenje. Ali ovo povlači $y = 0$, a zatim iz (35) $x = 0$.

Ostaje još da pokažemo da je $1 = 1 + \lambda 0$ jedinica za množenje, a to važi jer je $(x+\lambda y)(1+\lambda 0) = x + \lambda y$. ∎

Uočimo i sledeće

1. Neka je F polje realnih brojeva i izaberimo $\theta = 1, a = -1, b = 0$; tada je D (izomorfno sa) poljem kompleksnih brojeva.

2. Neka je F polje kompleksnih brojeva i neka $a = -1, b = 0$ i θ takvo da $(x+iy)^\theta = x - iy$; tada je D telo kvaterniona koje nije polje.

3. Neka je F telo kvaterniona i neka $a = -1, b = 0$ i θ definisano sa $(x + iy + jz + kt)^\theta = x - iy - jz - kt$. Tada je D oktonionski neasocijativni prsten sa deljenjem.

Ako je F konačno, onda je ono polje i zato θ mora biti automorfizam. Ovo znači da prsten sa deljenjem D ima neke dodatne osobine koje ćemo sada proučavati.

U bilo kom kvazipolju Q asocijator $[r, s, t]$ od tri elementa $r, s, t \in Q$ je definisan sa $[r, s, t] = (rs)t - r(st)$. Ako je F polje i ako izračunamo asocijator u D dobijamo

$$\begin{aligned}[x + \lambda y, z + \lambda t, h + \lambda k] = at^{\theta}k((x^{\theta^2} - x) + (b^{\theta}y^{\theta^2} - by^{\theta})) \\ + \lambda t^{\theta}k((a^{\theta}y^{\theta^2} - ay) + b(x^{\theta^2} - x^{\theta}) + b(b^{\theta}y^{\theta^2} - by^{\theta})).\end{aligned} \tag{37}$$

Sada zapažamo da, kako je F polje, F je sam sebi centar i zahtevati da θ zadovoljava $x^{1+\theta} \in Z$ je besmisleno.

Lema 3.3 Ako je F konačno onda, ako je $0 \neq 1$, F je desno i srednje jezgro od D.

Dokaz: Lako se vidi da za $t = 0$ ili $k = 0$ u (37) dobijamo nula za desnu stranu, za sve x, y, z, h. Dakle F je u desnom i srednjem nukleusu. Međutim, svaki seminukleus je telo, pa kako je D konačno, ono je polje. Dalje, ako D ima desni i srednji nukleus veći od F, onda bi D bilo polje i desna strana (37) bi bila jednaka nuli za sve vrednosti svih promenljivih. Ako pretpostavimo da D jeste polje, treba da pokažemo da ovo vodi u kontradikciju. Prvo primetimo da je $a \neq 0$, jer inače $k = 0$ bi bilo rešenje druge jednačine iz uslova na početku. Kako je D asocijativno, svaki asocijator je jednak nuli i zato, stavljajući $t = k = 1$ i $y = 0$, (37) nam govori da $x^{\theta^2} = x$ i $b(x^{\theta^2} - x^{\theta}) = 0\ \forall x$. Kako $\theta \neq 1$ to povlači da je $\theta^2 = 1$ i $b = 0$. Stavljajući $b = 0$ u (37) dobijamo $t^{\theta}k(a^{\theta} - a)y = 0\ \forall t, k, y$. A ovo je tačno ako i samo ako $a^{\theta} = a$, tj. ako i samo ako je a iz potpolja K svih elemenata fiksiranih sa θ. Kako $\theta^2 = 1$, K mora biti $GF(q)$ gde je $F = GF(q^2)$ i θ je dato sa $x^{\theta} = x^{q}\ \forall x \in F$. Ali kako x varira nad F, $x^{1+\theta}$ što je x^{1+q} varira nad celim K pa ima neko x iz F tako da $x^{1+\theta} = a$; ovo narušava (2) (setimo se da je $b = 0$) i dokazuje lemu. ∎

Primetimo da smo dokazali i više:

Lema 3.4 Ako je F konačno, onda je D asocijativno ako i samo ako je $\theta = 1$.

Da bismo konstruisali D treba da pretpostavimo postojanje elemenata a, b iz F i antiautomorfizma θ koji zadovoljava zadate uslove. Kako je $\theta \neq 1$, ako je F konačno, onda F mora biti $GF(p^n)$ gde je p prost broj i $n \neq 1$.

Teorema 3.3 *Ako je $F = GF(p^n)$ gde je p prost broj i $n > 1$, onda postoji izbor a, b i θ tako da D nije asocijativno.*

Dokaz: Ako je p neparan, izaberimo $x^{\theta} = x^{p}$, $b = 0$ i a da ne bude kvadrat iz F. Zatim, kako je x^{1+p} uvek kvadrat, uslov (2) je zadovoljen. Ako je $p = 2$, biramo $x^{\theta} = x^2$ i bilo koji element b koji nije nula. Pretpostavimo da je moguće izabrati a tako da $x^3 + bx = a$ ima rešenje za svako a iz F. Ali tada preslikavanje $x \to x^3 + bx$ je $1 - 1$ i na što je nemoguće jer $x^3 + bx = 0$ ima dva rešenja $x = 0$ i $x = d$ gde je d jedinstven element iz F koji zadovoljava $d^2 = b$. ∎

3.5 Diksonov komutativni prsten sa deljenjem

Naš poslednji primer prstena sa deljenjem će biti komutativan ali ne i asocijativan. Konstrukcija će biti slična onoj koju smo uradili u prethodnom poglavlju, samo što će F biti konačno polje, D dvodimenzioni vektorski prostor nad F sa baznim elementima 1, λ i definišemo množenje u D.

Neka je $F = GF(p^n)$, gde je p prost neparan broj i $n > 1$ i neka je a bilo koji element iz F koji nije kvadrat. Ako je θ automorfizam u F dat sa $x^\theta = x^{p^r}$, $1 \leq r < n$, onda množenje u D definišemo

$$(x + \lambda y)(z + \lambda t) = (xz + ay^\theta t^\theta) + \lambda(yz + xt). \tag{38}$$

Teorema 3.4 *D je komutativni prsten sa deljenjem koji nikad nije asocijativan.*

Dokaz: Iz same definicije vidimo da je množenje u D komutativno. Da bismo dokazali da je D prsten sa deljenjem treba da pokažemo da nema nenula delitelje.

Ako desnu stranu jednačine (38) izjednačimo sa nula, imamo

$$xz + ay^\theta t^\theta = 0 \quad yz + xt = 0. \tag{39}$$

Ako je $z = 0$ onda je ili $t = 0$ ili $x = y = 0$, pa se možemo reći da je $z \neq 0$. Rešavajući prvu jednačinu iz (39) po x i ubacujući je u drugu, dobijamo $yz - ay^\theta t^{1+\theta} z^{-1} = 0$ što povlači

$$z^2 = ay^{\theta-1} t^{\theta+1} = ay^{p^r-1} t^{p^r+1}, \ y \neq 0. \tag{40}$$

Međutim, svaki faktor u (40) je kvadrat, osim a, pa z mora biti nula. Ovo je kontradikcija, pa je $y = 0$, a zatim je i x nula. Dakle, D je komutativni prsten sa deljenjem. Da bismo dokazali da nije asocijativan moramo prvo dokazati sledeću lemu. ∎

Skup F poistovećujemo sa $\{x + \lambda 0|, x \in F\}$.

Lema 3.5 F je srednji nukleus od D, i ako je K potpolje polja F sa elementima fiksiranim pomoću θ, K je desni i levi nukleus; takođe, K je nukleus i centar.
Dokaz: Ako izračunamo asocijator, dobijamo

$$[x + \lambda y, z + \lambda t, h + \lambda k] = at^\theta(y^\theta(h - h^\theta) + k^\theta(x^\theta - x)) + \lambda at^\theta(y^\theta k - yk^\theta). \tag{41}$$

Za $t = 0$ desna strana (41) postaje nula. Lema je dokazana pošto je K desni nukleus. Iz komutativnosti sledi da je K i levi nukleus, i kako $K \neq D$, D ne može biti polje. ∎

Literatura

[1] E. Artin, *Geometric algebra,* Princeton University, Princeton, New Jersey (1957)

[2] N. Bokan, S. Vukmirović,*Projektivna geometrija,* Matematički fakultet, Beograd (2004)

[3] G. Kalajdžić, *Algebra,* Matematički fakultet, Beograd (2008)

[4] D. Palman, *Projektivna geometrija,* Školska knjiga, Zagreb (1984)

[5] D. Hughes, F. Piper, *Projective planes,* Springer-Verlag, New Jork (1973)

[6] J. Stillwell, *The four pillars of geometry*, Springer-Verlag, New Jork (2005)