

Afina in projektivna geometrija

Afine transformacije

- (1) Naj bo Π ravnina v afinem prostoru $\mathbb{R}^3$, ki jo določajo točke $A(4, 6, -2)$, $B(-2, 0, 4)$ in $C(0, 4, 1)$ ter $\tau : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ afina transformacija, ki je podana s predpisom

$$\tau(x, y, z) = (x + 2y + z + 1, y - 2, x + 2z + 3).$$

Pokaži, da je $\tau(\Pi)$ ravnina v $\mathbb{R}^3$ in izračunaj njeno normalno enačbo.

Rešitev: Afina transformacija prostora $\mathbb{R}^n$ je bijekcija, ki poljubno trojico kolinearnih točk preslika v kolinearne točke. Po osnovnem izreku afine geometrije lahko vsako afino transformacijo $\tau : \mathbb{R}^n \rightarrow \mathbb{R}^n$ zapišemo v obliki

$$\tau(x) = Ax + a,$$

kjer je $A : \mathbb{R}^n \rightarrow \mathbb{R}^n$ obrnljiva linearna preslikava in $a \in \mathbb{R}^n$ neka točka.

Najprej bomo pokazali, da afine transformacije slikajo ravnine v ravnine. V ta namen predpostavimo, da je afina transformacija $\tau : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ dana s predpisom

$$\tau(\vec{x}) = A\vec{x} + \vec{a},$$

kjer je $A \in \mathbb{R}^{3 \times 3}$ obrnljiva matrika in $\vec{a} \in \mathbb{R}^3$. Nadalje naj bo ravnina Π podana v parametrični obliki

$$\vec{r}_T = \vec{r}_0 + t_1 \vec{s}_1 + t_2 \vec{s}_2,$$

kjer je $\vec{r}_0$ začetna točka in $\vec{s}_1$ ter $\vec{s}_2$ smerna vektorja Π . Potem je

$$\tau(\vec{r}_T) = A(\vec{r}_0 + t_1 \vec{s}_1 + t_2 \vec{s}_2) + \vec{a} = A\vec{r}_0 + \vec{a} + t_1 A\vec{s}_1 + t_2 A\vec{s}_2 = \tau(\vec{r}_0) + t_1 A\vec{s}_1 + t_2 A\vec{s}_2.$$

Vidimo, da je množica $\tau(\Pi)$ spet ravnina z začetno točko $\tau(\vec{r}_0)$ in s smernima vektorjema $A\vec{s}_1$ ter $A\vec{s}_2$.

V našem primeru lahko preslikavo τ zapišemo v obliki

$$\tau(x, y, z) = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 2 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} + \begin{bmatrix} 1 \\ -2 \\ 3 \end{bmatrix}.$$

Nadalje je $\vec{r}_0 = (4, 6, -2)$, $\vec{s}_1 = \overrightarrow{AB} = (-6, -6, 6)$ in $\vec{s}_2 = \overrightarrow{AC} = (-4, -2, 3)$. Od tod dobimo:

$$\begin{aligned} \tau(\vec{r}_0) &= (15, 4, 3), \\ A\vec{s}_1 &= (-12, -6, 6), \\ A\vec{s}_2 &= (-5, -2, 2). \end{aligned}$$

Normala na ravnino $\tau(\Pi)$ je vzporedna vektorju $(0, 1, 1)$, od koder dobimo normalno enačbo ravnine

$$y + z = 7.$$

Opomba: Podobno lahko pokažemo tudi, da afina transformacija preslika afin podprostor dimenzije k v afin podprostor dimenzije k . V splošnem linearni del afine transformacije pove, kako se transformirajo smerni vektorji afinega podprostora. Če smo v evklidskem prostoru in je afina transformacija izometrija, pa podoben sklep velja tudi za normalne smeri. $\square$

(2) V afini ravnini $\mathbb{R}^2$ sta dani premici $p : y = 1$ in $q : x = -2$.

(a) Pokaži, da preslikava $\tau : \mathbb{R}^2 \rightarrow \mathbb{R}^2$, ki je dana s predpisom $\tau(x, y) = (y - 3, x + 3)$, preslika p na q in q na p .

(b) Poišči vse afine transformacije $\tau : \mathbb{R}^2 \rightarrow \mathbb{R}^2$, ki preslikajo p na q in q na p .

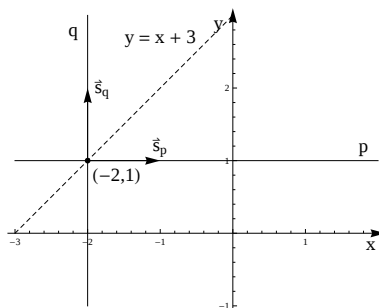
Rešitev: (a) Smerna vektorja premic sta $\vec{s}_p = (1, 0)$ in $\vec{s}_q = (0, 1)$. Ker leži točka $(-2, 1)$ na obeh premicah, lahko izberemo naslednji parametrizaciji premic p in q :

$$\begin{aligned} p : \vec{r} &= (-2, 1) + t(1, 0) = (-2 + t, 1), \\ q : \vec{r} &= (-2, 1) + s(0, 1) = (-2, 1 + s). \end{aligned}$$

Od tod dobimo:

$$\begin{aligned} \tau(-2 + t, 1) &= (-2, 1 + t), \\ \tau(-2, 1 + s) &= (-2 + s, 1), \end{aligned}$$

kar pomeni, da τ preslika p na q in q na p . Geometrično lahko transformacijo τ opišemo kot zrcaljenje čez premico $y = x + 3$.



(b) Išče afine transformacije ravnine $\mathbb{R}^2$, ki preslikajo p na q in obratno. Vsaka takšna preslikava je oblike

$$\tau(\vec{x}) = A\vec{x} + \vec{a},$$

kjer je A obrnljiva matrika velikosti 2×2 in $\vec{a} \in \mathbb{R}^2$. Bolj podrobno lahko zapišemo

$$\tau(x, y) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} e \\ f \end{bmatrix}$$

za neke $a, b, c, d, e, f \in \mathbb{R}$.

Če hočemo, da bo preslikava τ preslikala premico p na q , premico q pa na p , mora veljati:

$$\begin{aligned} A\vec{s}_p &\parallel \vec{s}_q, \\ A\vec{s}_q &\parallel \vec{s}_p. \end{aligned}$$

Pogoj vzporednosti $A\vec{s}_p \parallel \vec{s}_q$ lahko zapišemo v obliki $A\vec{s}_p = \alpha\vec{s}_q$ oziroma

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \alpha \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Ta sistem ima rešitev $a = 0$ in $c = \alpha$. Podobno iz pogoja $A\vec{s}_q \parallel \vec{s}_p$ sledi

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \beta \begin{bmatrix} 1 \\ 0 \end{bmatrix},$$

oziroma $b = \beta$ in $d = 0$. Oboje skupaj nam pove, da mora biti matrika A oblike

$$A = \begin{bmatrix} 0 & b \\ c & 0 \end{bmatrix}$$

za neka neničelna $b, c \in \mathbb{R}$. Za določitev vektorja $\vec{a}$ bomo sedaj uporabili še dejstvo, da se premici p in q sekata v točki $(-2, 1)$. Iz pogoja naloge potem sledi, da je $(-2, 1)$ fiksna točka preslikave τ oziroma $\tau(-2, 1) = (-2, 1)$. Od tod dobimo

$$\tau(-2, 1) = \begin{bmatrix} 0 & b \\ c & 0 \end{bmatrix} \begin{bmatrix} -2 \\ 1 \end{bmatrix} + \begin{bmatrix} e \\ f \end{bmatrix} = \begin{bmatrix} b + e \\ -2c + f \end{bmatrix} = \begin{bmatrix} -2 \\ 1 \end{bmatrix},$$

kar nam da $e = -2 - b$ in $f = 1 + 2c$. Vsaka afina transformacija ravnine $\mathbb{R}^2$, ki preslika p na q in q na p je torej oblike

$$\tau(x, y) = \begin{bmatrix} 0 & b \\ c & 0 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} -2 - b \\ 1 + 2c \end{bmatrix} = \begin{bmatrix} 0 & b \\ c & 0 \end{bmatrix} \begin{bmatrix} x + 2 \\ y - 1 \end{bmatrix} + \begin{bmatrix} -2 \\ 1 \end{bmatrix} = (by - 2 - b, cx + 1 + 2c)$$

za neka neničelna realna parametra b in c .

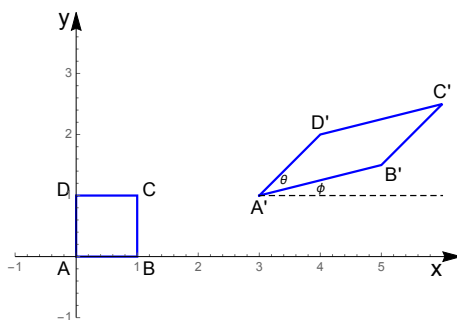
Geometrično lahko takšno preslikavo interpretiramo kot kompozicijo:

- raztega s središčem v točki $(-2, 1)$ za faktor c v vodoravni smeri in za faktor b v navpični smeri,
- zrcaljenja čez premico $y = x + 3$.

□

- (3) Naj bosta $ABCD$ enotski kvadrat in $A'B'C'D'$ pozitivno orientiran paralelogram v $\mathbb{R}^2$. Pokaži, da obstaja natanko ena afina transformacija, ki kvadrat preslika na paralelogram.

Rešitev: Označimo $A = (0, 0)$, $B = (1, 0)$, $C = (1, 1)$ in $D = (0, 1)$.



Pozitivno orientiran paralelogram $A'B'C'D'$ lahko parametriziramo na dva načina:

- (1) S koordinatami oglišč A' , B' in D' ,
- (2) s koordinatama oglišča A' , dolžinama stranic $|A'B'|$ in $|A'D'|$ ter kotoma ϕ in θ .

V vsakem primeru potrebujemo za opis paralelograma 6 parametrov, naš cilj pa je, da spoznamo, v kakšni zvezi so ti parametri s parametri afine transformacije.

Iščemo torej vse afine transformacije $\tau : \mathbb{R}^2 \rightarrow \mathbb{R}^2$, ki zadoščajo pogojem $\tau(A) = A'$, $\tau(B) = B'$, $\tau(C) = C'$ in $\tau(D) = D'$. Preslikava τ je oblike

$$\tau(x, y) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} e \\ f \end{bmatrix},$$

kjer so $a, b, c, d, e, f \in \mathbb{R}$.

(1) Iz pogoja $\tau(A) = A'$, dobimo

$$A' = \tau(0, 0) = \begin{bmatrix} e \\ f \end{bmatrix}.$$

(2) Iz pogojev $\tau(B) = B'$ in $\tau(C) = C'$ pa sledi:

$$\begin{aligned} \overrightarrow{A'B'} &= \tau(B) - \tau(A) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} a \\ c \end{bmatrix}, \\ \overrightarrow{A'D'} &= \tau(D) - \tau(A) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} b \\ d \end{bmatrix}. \end{aligned}$$

Vidimo, da so koeficienti afine transformacije natanko določeni s koordinatami točk A' , B' in D' , kar pomeni, da obstaja kvečjemu ena afina transformacija τ , ki zadošča pogojem naloge. Ker so točke A' , B' in D' nekolinearne, je matrika v predpisu τ obrnljiva in zato dani predpis res določa iskano afino transformacijo.

Geometrijski opis elementov grupe $GL^+(2, \mathbb{R})$:

Grupo vseh obrnljivih matrik velikosti 2×2 , ki ohranjajo orientacijo, označimo z

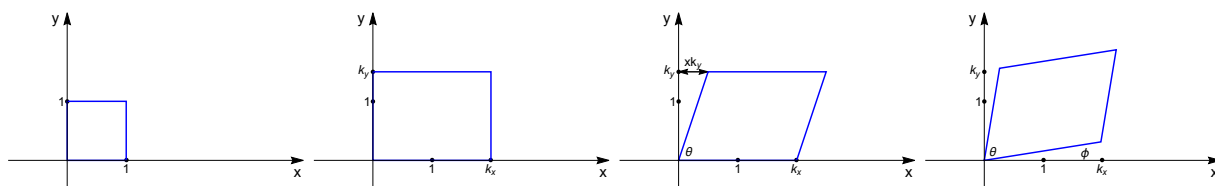
$$GL^+(2, \mathbb{R}) = \{A \in \mathbb{R}^{2 \times 2} \mid \det(A) > 0\}.$$

Ni težko pokazati, da lahko vsako takšno matriko enolično faktoriziramo v obliki

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} \cos \phi & -\sin \phi \\ \sin \phi & \cos \phi \end{bmatrix} \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} k_x & 0 \\ 0 & k_y \end{bmatrix},$$

kjer so $\phi \in [0, 2\pi)$, $x \in \mathbb{R}$ in $k_x, k_y \in (0, \infty)$. Geometrijsko lahko torej poljubno matriko A s pozitivno determinanto opišemo kot kompozicijo:

- raztegov za faktorja k_x in k_y v vodoravni oziroma navpični smeri,
- strižne deformacije s koeficientom x ,
- rotacije za kot ϕ .



Med parametri afine transformacije in parametri v razcepu veljajo zveze:

$$\begin{aligned} (a, c) &= k_x(\cos \phi, \sin \phi), \\ \operatorname{ctg} \theta &= x, \\ \sqrt{b^2 + d^2} &= k_y \sqrt{1 + x^2}. \end{aligned}$$

□

(4) Opiši podobnostne transformacije evklidske ravnine $\mathbb{R}^2$.

Rešitev: Afina transformacija $\tau : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ je *podobnostna transformacija*, če ohranja kote med premicami. Podobnostne transformacije ohranjajo obliko likov, ne pa nujno tudi njihove velikosti.

Kot poljubno afino transformacijo lahko tudi vsako podobnostno transformacijo zapišemo v obliki

$$\tau(\vec{x}) = A\vec{x} + \vec{a},$$

kjer je $A \in \mathbb{R}^{2 \times 2}$ obrnljiva matrika in $\vec{a} \in \mathbb{R}^2$. Na smeri premic vpliva samo matrika A , pogoj iz definicije pa lahko zapišemo v obliki enakosti

$$\angle(\vec{s}_1, \vec{s}_2) = \angle(A\vec{s}_1, A\vec{s}_2),$$

ki mora veljati za vse neničelne smerne vektorje.

Če vstavimo $\vec{s}_1 = (1, 0)$ in $\vec{s}_2 = (0, 1)$, vidimo, da morata biti stolpca (a, c) in (b, d) matrike A pravokotna. Ker morata biti trikotnika z oglišči $(0, 0)$, $(1, 0)$ in $(0, 1)$ ter $(0, 0)$, (a, c) in (b, d) podobna, pa mora veljati še, da sta vektorja (a, c) in (b, d) enako dolga. Oba pogoja skupaj nam povesta, da je $(b, d) = \pm(-c, a)$, matrika A pa je torej lahko oblike

$$A = \begin{bmatrix} a & -c \\ c & a \end{bmatrix} \text{ ali } A = \begin{bmatrix} a & c \\ c & -a \end{bmatrix}.$$

Če označimo $k = \sqrt{a^2 + c^2}$, lahko to zapišemo tudi v obliki

$$A = k \begin{bmatrix} \frac{a}{k} & -\frac{c}{k} \\ \frac{c}{k} & \frac{a}{k} \end{bmatrix} \text{ ali } A = k \begin{bmatrix} \frac{a}{k} & \frac{c}{k} \\ \frac{c}{k} & -\frac{a}{k} \end{bmatrix},$$

kar pomeni, da je A večkratnik ortogonalne matrike. Vsaka podobnostna transformacija evklidske ravnine ima torej predpis

$$\tau(\vec{x}) = kQ\vec{x} + \vec{a},$$

kjer je $k > 0$ in Q ortogonalna matrika. Torej lahko vsako podobnostno transformacijo zapišemo kot kompozicijo linearne izometrije, središčnega raztega in translacije.

O podobnostnih transformacijah lahko govorimo v afinih prostorih nad obsegi s skalarnim produktom. V splošnih afinih prostorih pa lahko definiramo pojem dilatacije. Afina transformacija $\tau : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ je *dilatacija*, če za vsako premico $p \subset \mathbb{R}^2$ velja $p \parallel \tau(p)$. Dilatacije so preslikave oblike

$$\tau(\vec{x}) = k\vec{x} + \vec{a}$$

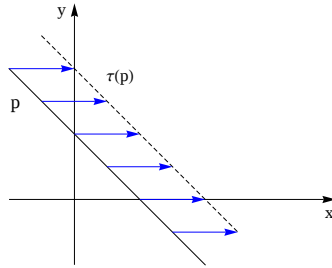
za $k \neq 0$. Ločimo dva tipa dilatacij.

1. Translacije:

Translacije so preslikave oblike

$$\tau(\vec{x}) = \vec{x} + \vec{a}$$

za nek $\vec{a} \in \mathbb{R}^2$. V tem primeru je $k = 1$.

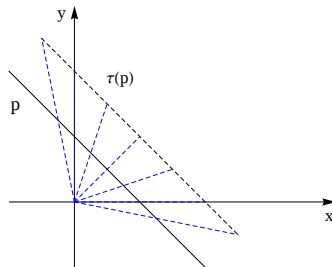


2. Središčni raztegi:

Središčni raztegi so preslikave oblike

$$\tau(\vec{x}) = k\vec{x} + \vec{a}$$

za $k \notin \{0, 1\}$. V tem primeru gre za razteg s središčem v točki $\frac{1}{1-k}\vec{a}$ in za faktor k .



□

(5) Pokaži, da v vsaki afini ravnini nad poljem velja Menelajev izrek.

Rešitev: Menelajev izrek je bil v osnovni verziji dokazan v evklidski ravnini, mi pa si bomo pogledali dokaz, ki temelji na dilatacijah in deluje v poljubni afini ravnini.

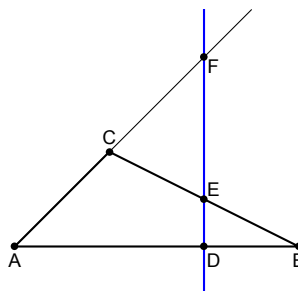
Menelajev izrek: Naj bo ABC trikotnik v $\mathbb{F}^2$ in D , E in F od oglišč različne točke na nosilkah stranic trikotnika. Potem so točke D , E in F kolinearne natanko takrat, ko velja

$$\frac{\overrightarrow{DA}}{\overrightarrow{DB}} \frac{\overrightarrow{EB}}{\overrightarrow{EC}} \frac{\overrightarrow{FC}}{\overrightarrow{FA}} = 1.$$

Pri tem je na primer za tri različne kolinearne točke A , B in D kvocient usmerjenih daljic definiran s pogojem

$$\frac{\overrightarrow{DA}}{\overrightarrow{DB}} = k \in \mathbb{F} \iff \overrightarrow{DA} = k\overrightarrow{DB}.$$

Poglejmo najprej skico.



Označimo sedaj $k_D = \frac{\overrightarrow{DB}}{\overrightarrow{DA}}$, $k_E = \frac{\overrightarrow{EC}}{\overrightarrow{EB}}$, $k_F = \frac{\overrightarrow{FA}}{\overrightarrow{FB}}$ in definirajmo središčne raztege τ_D , τ_E in τ_F afine ravnine $\mathbb{F}^2$ s predpisi:

$$\begin{aligned}\tau_D(x) &= k_D(x - D) + D, \\ \tau_E(x) &= k_E(x - E) + E, \\ \tau_F(x) &= k_F(x - F) + F.\end{aligned}$$

Ker tvorijo dilatacije grupo, je tudi afina transformacija $\tau : \mathbb{F}^2 \rightarrow \mathbb{F}^2$ s predpisom

$$\tau = \tau_F \circ \tau_E \circ \tau_D$$

dilatacija. Koeficiente središčnih raztegov smo izbrali tako, da velja $\tau_D(A) = B$, $\tau_E(B) = C$ in $\tau_F(C) = A$ in da je posledično A fiksna točka dilatacije τ . Od tod sledi, da je τ bodisi identiteta, ali pa središčni razteg s središčem v točki A .

($\Rightarrow$) Recimo, da so točke D , E in F kolinearne in naj bo p premica, ki vsebuje te tri točke. Ker so τ_D , τ_E in τ_F središčni raztegi s središči na p , velja $\tau_D(p) = \tau_E(p) = \tau_F(p) = p$ in posledično tudi $\tau(p) = p$. Ker premica p ne vsebuje točke A , jo vsak središčni razteg s središčem v A preslika na njej disjunktno vzporedno premico. Torej mora biti τ identiteta. Poglejmo sedaj formulo za kompozicijo dilatacij. Če je $\tau_1(x) = k_1x + a_1$ in $\tau_2(x) = k_2x + a_2$, je

$$\tau_2(\tau_1(x)) = \tau_2(k_1x + a_1) = k_2k_1x + k_2a_1 + a_2.$$

Vidimo, da se pri kompoziciji dilatacij faktorji raztegov množijo. V našem primeru tako iz dejstva, da je τ identiteta, sledi, da je $k_F k_E k_D = 1$, od koder pa sledi enakost

$$\frac{\overrightarrow{DA}}{\overrightarrow{DB}} \frac{\overrightarrow{EB}}{\overrightarrow{EC}} \frac{\overrightarrow{FC}}{\overrightarrow{FA}} = 1.$$

($\Leftarrow$) Recimo sedaj, da velja $\frac{\overrightarrow{DA}}{\overrightarrow{DB}} \frac{\overrightarrow{EB}}{\overrightarrow{EC}} \frac{\overrightarrow{FC}}{\overrightarrow{FA}} = 1$. Kot prvo od tod sledi, da je $k_F k_E k_D = 1$, kar pa pomeni, da je τ identiteta. Označimo s p premico skozi točki D in E . Ker sta τ_D in τ_E središčna raztega s središčema na p , je $\tau_D(p) = \tau_E(p) = p$. Poleg tega je tudi $\tau(p) = p$ in posledično $\tau_F(p) = p$. Središčni razteg ohranja natanko tiste premice, ki vsebujejo središče raztega. V našem primeru od tod sledi, da je $F \in p$, torej so D , E in F kolinearne. $\square$

- (6) (a) Izračunaj, koliko je afinih transformacij afinih ravnin $\mathbb{F}_p^2$, kjer je p praštevilo.
(b) Izračunaj, koliko je afinih transformacij afine ravnine $\text{GF}(4)^2$.

Rešitev: V primeru, ko je V vektorski prostor nad obsegom $\mathcal{O}$, je po osnovnem izreku afine geometrije vsaka afina transformacija $\tau : V \rightarrow V$ oblike

$$\tau(x) = Mx + a,$$

kjer je $M : V \rightarrow V$ obrnljiva semilinearna preslikava in $a \in V$ neka točka. V primeru, ko je V vektorski prostor nad obsegom $\mathbb{R}$, je vsaka semilinearna preslikava avtomatično linearna, zato so v teh primerih afine transformacije ravno kompozicije obrnljivih linearnih preslikav in translacij. Preslikava $M : V \rightarrow V$ iz vektorskega prostora V nad $\mathcal{O}$ nazaj vase je semilinearna, če obstaja tak avtomorfizem ϕ obsega $\mathcal{O}$, da za vsaka $x, y \in V$ in za vsak $\alpha \in \mathcal{O}$ velja:

$$\begin{aligned}M(x + y) &= M(x) + M(y) && \text{aditivnost,} \\ M(\alpha x) &= \phi(\alpha)M(x) && \text{seminhomogenost.}\end{aligned}$$

Za opis vseh afinih transformacij moramo torej klasificirati vse avtomorfizme obsega $\mathcal{O}$. Spomnimo se, da je avtomorfizem obsega $\mathcal{O}$ bijekcija $\phi : \mathcal{O} \rightarrow \mathcal{O}$, ki zadošča pogojem:

$$\begin{aligned}\phi(x + y) &= \phi(x) + \phi(y), \\ \phi(xy) &= \phi(x)\phi(y),\end{aligned}$$

za vsaka $x, y \in \mathcal{O}$. Od tod avtomatično sledi $\phi(0) = 0$ in $\phi(1) = 1$.

(a) Najprej si pogledajmo primer obsega $\mathbb{F}_p$. Obseg $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ je končen obseg praštevilske moči p . Seštevanje in množenje definiramo po modulu p . Enota za seštevanje je 0, enota za množenje pa 1. Za poljuben avtomorfizem obsega $\mathbb{F}_p$ je torej $\phi(0) = 0$ in $\phi(1) = 1$. Izberimo sedaj poljuben $n \in \mathbb{F}_p$, $1 < n < p$. Potem lahko pišemo

$$n = \underbrace{1 + 1 + \dots + 1}_n,$$

zato iz aditivnosti preslikave ϕ sledi

$$\phi(n) = \phi(\underbrace{1 + 1 + \dots + 1}_n) = \underbrace{\phi(1) + \phi(1) + \dots + \phi(1)}_n = \underbrace{1 + 1 + \dots + 1}_n = n.$$

To pomeni, da je ϕ nujno identična preslikava, grupa avtomorfizmov obsega $\mathbb{F}_p$ pa vsebuje en sam element. Vsaka afina transformacija $\mathbb{F}_p^2$ je torej oblike

$$\tau(x) = Ax + a,$$

kjer je A obrnljiva matrika s koeficienti v $\mathbb{F}_p$ in $a \in \mathbb{F}_p^2$.

Matrika A je obrnljiva natanko tedaj, ko sta njena stolpca linearno neodvisna. Za prvi stolpec lahko izberemo poljuben neničelni vektor $v_1 \in \mathbb{F}_p^2$, kar pomeni, da imamo na izbiro $p^2 - 1$ možnosti. Drugi stolpec moramo izbrati tako, da ne bo ležal na premici, ki jo napenja v_1 . Takšnih točk je $p^2 - p$. Število obrnljivih matrik je torej $(p^2 - 1)(p^2 - p)$. Ker imamo za izbiro elementa a na voljo p^2 možnosti, je število vseh afinih transformacij afine ravnine $\mathbb{F}_p^2$ enako

$$p^2(p^2 - 1)(p^2 - p).$$

(b) Teorija obsegov nam pove, da je vsak končen obseg ene izmed naslednjih dveh oblik:

- Obseg $\mathbb{F}_p$ ostankov pri deljenju s praštevilom p s p elementi,
- Galoisov obseg $\text{GF}(p^n)$ s p^n elementi, kjer je p praštevilo in $n > 1$ naravno število.

Ker obsege ostankov $\mathbb{F}_p$ že dobro poznamo, si bomo v nadaljevanju pogledali konstrukcijo Galoisovih obsegov. Galoisov obseg $\text{GF}(p^n)$ konstruiramo na naslednji način:

- Izberemo nerazcepen polinom stopnje n v kolobarju $\mathbb{F}_p[x]$.
- Elementi $\text{GF}(p^n)$ so polinomi stopnje največ $n-1$ v $\mathbb{F}_p[x]$, ki jih lahko interpretiramo tudi kot ostanke pri deljenju s polinomom $p(x)$.
- Seštevanje je definirano kot seštevanje polinomov.
- Produkt dveh polinomov dobimo tako, da najprej izračunamo njun produkt v $\mathbb{F}_p[x]$, nato pa vzamemo ostanek pri deljenju s polinomom $p(x)$.

V našem primeru je

$$\text{GF}(2^2) = \{0, 1, x, 1 + x\}$$

operaciji seštevanja in množenja pa lahko predstavimo s tabelama:

+	0	1	x	$1+x$	·	0	1	x	$1+x$
0	0	1	x	$1+x$	0	0	0	0	0
1	1	0	$1+x$	x	1	0	1	x	$1+x$
x	x	$1+x$	0	1	x	0	x	$1+x$	1
$1+x$	$1+x$	x	1	0	$1+x$	0	$1+x$	1	x

Množica vseh elementov obsega $\text{GF}(4)$ tvori grupo za seštevanje, ki je izomorfna grupi $\mathbb{Z}_2 \times \mathbb{Z}_2$, grupa obrnljivih elementov obsega $\text{GF}(4)$ pa je izomorfna grupi $\mathbb{Z}_3$.

Preverimo lahko, da ima obseg $\text{GF}(4)$ poleg identičnega še netrivialni avtomorfizem ϕ , ki je definiran s predpisom:

$$\phi(0) = 0, \phi(1) = 1, \phi(x) = 1+x, \phi(1+x) = x.$$

Vsaka semilinearna preslikava

$$M : \text{GF}(4)^2 \rightarrow \text{GF}(4)^2$$

je sedaj ene izmed naslednjih dveh oblik:

$$M(x_1, x_2) = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix},$$

$$M(x_1, x_2) = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix} \begin{bmatrix} \phi(x_1) \\ \phi(x_2) \end{bmatrix},$$

kjer je ϕ netrivialni avtomorfizem obsega $\text{GF}(4)$. Število obrnljivih semilinearnih preslikav je torej $2 \cdot (4^2 - 1) \cdot (4^2 - 4) = 360$, vseh afinih transformacij afine ravnine $\text{GF}(4)^2$ pa je

$$360 \cdot 16 = 5760.$$

□