Afina in projektivna geometrija

Afina geometrija v splošnih vektorskih prostorih

(1) Poišči vse avtomorfizme obsegov $\mathbb{F}_p$, $\mathbb{Q}$ in $\mathbb{R}$.

Rešitev: Avtomorfizem obsega $\mathcal{O}$ je bijekcija $\phi : \mathcal{O} \to \mathcal{O}$, ki zadošča pogojema:

$$\phi(x+y) = \phi(x) + \phi(y),$$
$$\phi(xy) = \phi(x)\phi(y),$$

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

Avtomorfizmi obsega $\mathbb{F}_p$:

Obseg $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ 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

$$n = \underbrace{1 + 1 + \ldots + 1}_{n},$$

zato iz aditivnosti preslikave ϕ sledi

$$\phi(n) = \phi(\underbrace{1 + 1 + \ldots + 1}_{n}) = \underbrace{\phi(1) + \phi(1) + \ldots + \phi(1)}_{n} = \underbrace{1 + 1 + \ldots + 1}_{n} = n.$$

To pomeni, da je ϕ nujno identična preslikava, grupa avtomorfizmov obsega $\mathbb{F}_p$ pa vsebuje en sam element.

Avtomorfizmi obsega $\mathbb{Q}$:

Izberimo poljuben avtomorfizem ϕ obsega racionalnih števil. Podobno kot v prejšnjem primeru lahko pokažemo, da za vsak $n \in \mathbb{N}$ velja

$$\phi(n) = n.$$

V splošnem za vsak $q \in \mathbb{Q}$ velja $\phi(q) + \phi(-q) = \phi(q + (-q)) = \phi(0) = 0$, kar nam da enakost

$$\phi(-q) = -\phi(q).$$

Ker je ϕ identiteta na naravnih številih, mora biti po tej formuli identiteta tudi na vseh celih številih. Podoben sklep nam da

$$\phi(n)\phi\left(\frac{1}{n}\right) = \phi(1) = 1,$$

od koder sledi, da za vsak $n \in \mathbb{N}$ velja

$$\phi\left(\frac{1}{n}\right) = \frac{1}{n}.$$

Če je sedaj $q \in \mathbb{Q}$ poljubno racionalno število, ga lahko zapišemo v obliki $q = \frac{m}{n}$, kjer je $m \in \mathbb{Z}$ in $n \in \mathbb{N}$. Zaradi multiplikativnosti preslikave ϕ je potem

$$\phi(q) = \phi\left(\frac{m}{n}\right) = \phi(m)\phi\left(\frac{1}{n}\right) = m \cdot \frac{1}{n} = q.$$

Torej je tudi v primeru obsega $\mathbb{Q}$ edini avtomorfizem kar identična preslikava.

Avtomorfizmi obsega $\mathbb{R}$:

Na podoben način kot prej lahko pokažemo, da vsak avtomorfizem ϕ obsega $\mathbb{R}$ fiksira racionalna števila. Izberimo sedaj poljuben pozitiven $x \in \mathbb{R}$. Potem je

$$\phi(x) = \phi(\sqrt{x})\phi(\sqrt{x}) > 0.$$

Od tod sledi, da je preslikava ϕ monotona. Če je namreč $x > y$, je $x - y > 0$ in zato $\phi(x - y) = \phi(x) - \phi(y) > 0$. Pokažimo sedaj, da je $\phi(r) = r$ za vsak $r \in \mathbb{R}$. Če bi namreč za nek r veljalo $\phi(r) > r$, bi lahko našli $q \in \mathbb{Q}$, da bi veljalo

$$r < q < \phi(r).$$

Iz monotonosti ϕ pa po drugi strani sledi $\phi(r) < \phi(q) = q$, kar nas pripelje v protislovje. Podoben sklep deluje tudi, če bi bil $\phi(r) < r$.

Grupa avtomorfizmov obsega $\mathbb{R}$ vsebuje torej samo identično preslikavo.

Opomba: Primer obsega, ki ima netrivialne avtomorfizme, je obseg kompleksnih števil $\mathbb{C}$. Poleg identitete je zvezen avtomorfizem kompleksnih števil tudi kompleksno konjugiranje, obstaja pa še neskončno mnogo nezveznih avtomorfizmov. $\square$

(2) Naj bo $V = \mathbb{F}_p^n$ vektorski prostor dimenzije n nad obsegom $\mathbb{F}_p$.

(a) Poišči število linearnih premic v V.
(b) Poišči število afinih premic v V.
(c) Poišči število linearnih (semilinearnih endomorfizmov) V.
(d) Poišči število avtomorfizmov V.

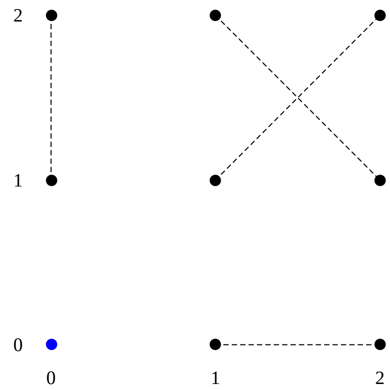
Rešitev: (a) Linearna premica v $\mathbb{F}_p^n$ je podprostor oblike

$$\mathcal{A} = \{\alpha s \mid \alpha \in \mathbb{F}_p\}$$

za nek $s \in \mathbb{F}_p^n$. Na vsaki takšni premici leži izhodišče in pa $p - 1$ neničelnih točk. Če bi točko s zamenjali z neko drugo neničelno točko na $\mathcal{A}$, bi dobili isto premico, a z drugo parametrizacijo. To pomeni, da vsaka točka $a \in \mathbb{F}_p^n$ natanko določa linearno premico in da po $p - 1$ neničelnih točk določa isto linearno premico. Ker je vseh neničelnih točk v $\mathbb{F}_p^n$ natanko $p^n - 1$, je

$$\text{število linearnih premic v } \mathbb{F}_p^n = \frac{p^n - 1}{p - 1}.$$

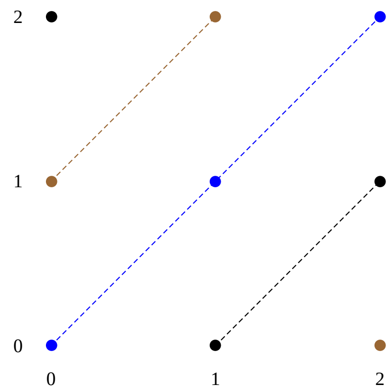
V afini ravnini $\mathbb{F}_3^2$ imamo tako na primer 4 linearne premice. Na vsaki izmed njih ležita dve neničelni točki.



(b) Afine premice dobimo s translacijami linearnih premic. Vsako linearno premico lahko premaknemo na p^n načinov, vendar pa nam po p translacij določa isto vzporednico. Za vsako smer imamo torej p^{n-1} vzporednic s to smerjo, od koder sledi

$$\text{število afinih premic v } \mathbb{F}_p^n = p^{n-1} \cdot \frac{p^n - 1}{p - 1}.$$

V afini ravnini $\mathbb{F}_3^2$ imamo v vsaki smeri 3 vzporednice. Ena izmed njih pa je linearna.



(c) Linearne endomorfizme vektorskega prostora $V = \mathbb{F}_p^n$ lahko identificiramo z matrikami velikosti $n \times n$ s koeficienti v obsegu $\mathbb{F}_p$. Vsaka takšna matrika ima n^2 koeficientov, za vsak koeficient pa imamo p možnosti. Torej je

$$\left|\mathrm{End}_{\mathbb{F}_p}(V)\right| = p^{n^2}.$$

Preslikava $M : V \to V$ 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:

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

Če je V vektorski prostor nad $\mathbb{F}_p$, $\mathbb{Q}$ ali $\mathbb{R}$, je edini avtomorfizem danega obsega identična preslikava, zato v teh primerih semilinearne preslikave sovpadajo z linearnimi. Torej je tudi v našem primeru število semilinearnih endomorfizmov prostora V enako številu linearnih endomorfizmov V.

(d) Linearni endomorfizem vektorskega prostora V je avtomorfizem prostora V, če je matrika, ki mu pripada, obrnljiva. To pa pomeni, da morajo biti njeni stolpci linearno neodvisni. Za prvi stolpec lahko izberemo poljuben neničelni vektor $v_1 \in \mathbb{F}_p^n$. Torej imamo na izbiro $p^n - 1$ možnosti. Drugi stolpec moramo izbrati tako, da ne bo ležal na premici, ki jo napenja v_1. Takšnih točk je $p^n - p$. Za izbiro tretjega stolpca so dobri vsi vektorji, ki ne ležijo v ravnini

$$A_2 = \{\alpha_1 v_1 + \alpha_2 v_2 \mid \alpha_1, \alpha_2 \in \mathbb{F}_p\}.$$

Takšnih vektorjev je $p^n - p^2$. Ta postopek sedaj ponavljamo, dokler ne pridemo do zadnjega stolpca. Na k-tem koraku imamo na voljo $p^n - p^{k-1}$ možnosti, število vseh avtomorfizmov vektorskega prostora V pa je enako

$$\left|\mathrm{Aut}_{\mathbb{F}_p}(V)\right| = (p^n - 1)(p^n - p)(p^n - p^2)\dots(p^n - p^{n-1}).$$

□

(3) Konstruiraj $p - 1$ paroma ortogonalnih latinskih kvadratov reda p, kjer je p praštevilo.

Rešitev: Latinski kvadrat reda n je $n \times n$ matrika s koeficienti $\{1, 2, \dots, n\}$, katere vsaka vrstica in vsak stolpec vsebuje vseh n števil. Latinska kvadrata $A = (a_{ij})$ in $B = (b_{ij})$ sta ortogonalna, če sta enaki množici

$$\{(a_{ij}, b_{ij}) \mid i, j \in \{1, 2, \dots, n\}\} = \{(i, j) \mid i, j \in \{1, 2, \dots, n\}\}.$$

Poglejmo si pojem ortogonalnosti na primeru dveh latinskih kvadratov reda 3.

1	2	3
3	1	2
2	3	1

3	2	1
2	1	3
1	3	2

Če ta dva kvadrata zložimo skupaj, dobimo naslednjo matriko urejenih parov.

(1,3)	(2,2)	(3,1)
(3,2)	(1,1)	(2,3)
(2,1)	(3,3)	(1,2)

Dva latinska kvadrata sta potem ortogonalna natanko takrat, ko v tej matriki parov vsak urejeni par nastopa natanko enkrat.

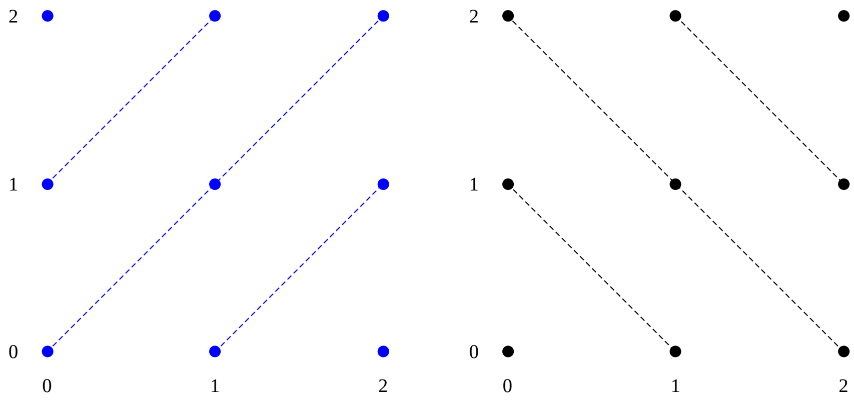
Pri konstrukciji ortogonalnih latinskih kvadratov reda p si bomo pomagali s končno afino ravnino $\mathbb{F}_p^2$. V tej afini ravnini imamo natanko $p + 1$ linearnih premic. Ena izmed teh je vodoravna, ena navpična, ostale pa so poševne. Pokazali bomo, da lahko vsaki poševni premici pridružimo nek latinski kvadrat tako, da bodo različne premice določale paroma ortogonalne latinske kvadrate.

Izberimo si torej neko poševno linearno premico $\mathcal{A}_1$. Ta premica določa družino vzporednic

$$\{\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_p\},$$

ki so paroma disjunktne, njihova unija pa je cela ravnina $\mathbb{F}_p^2$. Na vsaki premici je natanko p točk. Označimo sedaj mesta v kvadratu, ki ustrezajo točkam na premici $\mathcal{A}_i$, z i. Premica $\mathcal{A}_i$ seka vsako vodoravnico in vsako navpičnico natanko enkrat, zato bo število i nastopalo v vsaki vrstici in v vsakem stolpcu natanko enkrat. To pa pomeni, da smo s tem postopkom konstruirali latinski kvadrat.

Denimo sedaj, da je $\mathcal{B}_1 \neq \mathcal{A}_1$ neka druga poševna linearna premica ter $\{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_p\}$ njej pridružena družina vzporednic. Označimo z A in B prirejena latinska kvadrata. Za poljuben par (i,j) se premici $\mathcal{A}_i$ in $\mathcal{B}_j$ sekata v natanko eni točki. Torej matrika parov, ki jo dobimo z združitvijo latinskih kvadratov A in B, vsebuje vsak par (i,j) natanko enkrat, kar pa pomeni, da sta A in B ortogonalna.



$\square$

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

(a) Pokaži, da preslikava $\tau : \mathbb{R}^2 \to \mathbb{R}^2$, 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 $\tau : \mathbb{R}^2 \to \mathbb{R}^2$, ki preslikajo p na q in q na p.

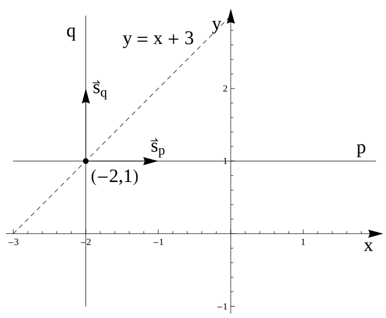
Rešitev: (a) Smerna vektorja premic sta $\vec{s}_p = (1,0)$ in $\vec{s}_q = (0,1)$. Ker leži točka $(-2,1)$ na obeh premicah, lahko izberemo naslednji parametrizaciji premic p in q:

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

Od tod dobimo:

$$\tau(-2+t, 1) = (-2, 1+t),$$
$$\tau(-2, 1+s) = (-2+s, 1),$$

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) Bijekcija vektorskega prostora V nad obsegom $\mathcal{O}$ je afina transformacija, če se poljubna trojica kolinearnih točk preslika v kolinearne točke. Po osnovnem izreku afine geometrije lahko vsako afino transformacijo $\tau : V \to V$ zapišemo v obliki

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

kjer je $A : V \to V$ obrnljiva semilinearna preslikava in $b \in V$ neka točka. V primeru, ko je V vektorski prostor nad obsegom $\mathbb{F}_p$, $\mathbb{Q}$ ali $\mathbb{R}$, je vsaka semilinearna preslikava avtomatično linearna, zato so v teh primerih afine transformacije ravno kompozicije obrnljivih linearnih preslikav in translacij.

V našem primeru iščemo afine transformacije ravnine $\mathbb{R}^2$, ki preslikajo p na q in obratno. Vsaka takšna preslikava je oblike

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

kjer je A obrnljiva matrika velikosti 2×2 in $\vec{b} \in \mathbb{R}^2$. Izberimo sedaj poljubno premico l v ravnini in jo zapišimo v obliki

$$l : \vec{r} = \vec{r}_0 + t\vec{s}.$$

Ker je τ afina transformacija, je potem tudi $\tau(l)$ premica s parametrizacijo

$$\tau(l) : \tau(\vec{r}) = \tau(\vec{r}_0 + t\vec{s}) = A(\vec{r}_0 + t\vec{s}) + \vec{b} = (A\vec{r}_0 + \vec{b}) + tA\vec{s}.$$

Premica $\tau(l)$ ima torej smerni vektor $A\vec{s}$. Če hočemo, da bo preslikava τ preslikala premico p na q, premico q pa na p, mora veljati:

$$A\vec{s}_p \parallel \vec{s}_q,$$
$$A\vec{s}_q \parallel \vec{s}_p.$$

Pišimo sedaj

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

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

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 $\vec{b}$ 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:

- zrcaljenja čez premico $y = x + 3$,
- raztegov s središčema v točki $(-2, 1)$. V navpični smeri raztegujemo za faktor c, v vodoravni smeri pa za faktor b.

$\square$

(5) Karakteriziraj dilatacije afine ravnine $\mathbb{R}^2$.

Rešitev: Afina transformacija $\tau : \mathbb{R}^2 \to \mathbb{R}^2$ je dilatacija, če za vsako premico $p \subset \mathbb{R}^2$ velja $p \parallel \tau(p)$. Kot poljubno afino transformacijo lahko tudi vsako dilatacijo zapišemo v obliki

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

kjer je A obrnljiva matrika velikosti 2×2 in $\vec{b} \in \mathbb{R}^2$. Zanimalo nas bo, kakšna mora biti matrika A, da bo preslikava τ dilatacija. Če hočemo, da bo za vsako premico p veljalo $p \parallel \tau(p)$, mora veljati

$$\vec{s} \parallel A\vec{s}$$

za vsak $\vec{s}$. To pomeni, da je vsak vektor lastni vektor matrike A, od koder pa sledi, da je matrika A oblike

$$A = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}$$

za nek $\lambda \in \mathbb{R} \setminus \{0\}$. Ta matrika predstavlja razteg s središčem v koordinatnem izhodišču za faktor λ. Dilatacije so torej preslikave oblike

$$\tau(\vec{x}) = \lambda\vec{x} + \vec{b}.$$

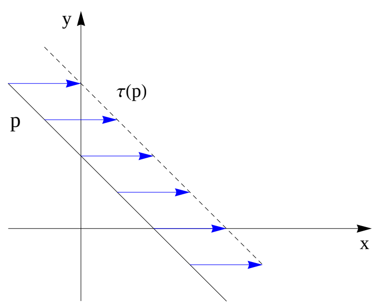
Ločimo dva tipa dilatacij.

1. Translacije:

Translacije so preslikave oblike

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

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

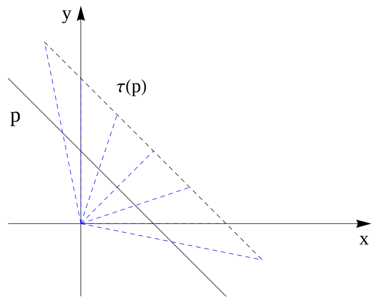


2. Središčni raztegi:

Središčni raztegi so preslikave oblike

$$\tau(\vec{x}) = \lambda\vec{x} + \vec{b}$$

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



□

(6) Preslikava $F\colon \mathbb{R}_2[x] \to \mathbb{R}_2[x]$ je dana s predpisom

$$(Fp)(x) = x \cdot p'(x) + p(1) + x + 1$$

za poljuben $p \in \mathbb{R}_2[x]$.

(a) Zapiši predpis za preslikavo F v koordinatah na $\mathbb{R}_2[x]$, ki jih določa baza $\{x^2, x, 1\}$, in pokaži, da je F afina transformacija.

(b) Naj bo $\mathcal{A} = \{p \in \mathbb{R}_2[x] \,|\, p(0) = 1,\ p(1) = 1\}$. Pokaži, da je $\mathcal{A}$ afin podprostor v $\mathbb{R}_2[x]$ in nato zapiši njegovo sliko v obliki $F(\mathcal{A}) = a + U$, kjer je $a \in \mathbb{R}_2[x]$ in $U \subset \mathbb{R}_2[x]$ nek linearni podprostor.

Rešitev: (a) Vektorski prostor $\mathbb{R}_2[x]$ realnih polinomov stopnje največ dva je izomorfen prostoru $\mathbb{R}^3$. Pri tej nalogi bomo uporabili eksplicitni izomorfizem $\phi : \mathbb{R}_2[x] \to \mathbb{R}^3$, ki je določen s predpisom

$$\phi(ax^2 + bx + c) = (a, b, c).$$

Preslikava F preslika polinom $p(x) = ax^2 + bx + c$ v polinom

$$\begin{aligned}(Fp)(x) &= x \cdot p'(x) + p(1) + x + 1,\\ &= x(2ax + b) + a + b + c + x + 1,\\ &= 2ax^2 + (b+1)x + (a+b+c+1).\end{aligned}$$

V koordinatah, ki jih določa baza $\{x^2, x, 1\}$, lahko F zapišemo v obliki

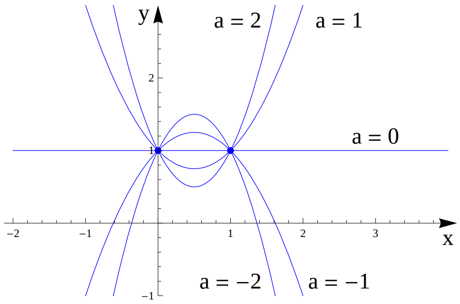
$$F(a, b, c) = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} a \\ b \\ c \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}.$$

Preslikava F je kompozicija obrnljive linearne preslikave in pa translacije, zato je afina transformacija.

(b) Polinomi v množici $\mathcal{A} = \{p \in \mathbb{R}_2[x] \,|\, p(0) = 1,\, p(1) = 1\}$ zadoščajo pogojema $c = 1$ in $a + b + c = 1$. Poljuben polinom $p \in \mathcal{A}$ je torej oblike $p(x) = ax^2 - ax + 1$, zato lahko zapišemo

$$\mathcal{A} = 1 + \mathrm{Lin}\{x^2 - x\},$$

od koder sledi, da je $\mathcal{A}$ afin podprostor v $\mathbb{R}_2[x]$. Prostor $\mathcal{A}$ je enodimenzionalen in sestoji iz vseh kvadratnih polinomov, ki potekajo skozi točki $(0, 1)$ in $(1, 1)$.



Iz enakosti

$$F(a, -a, 1) = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} a \\ -a \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 2a \\ -a + 1 \\ 2 \end{bmatrix} = a \begin{bmatrix} 2 \\ -1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}$$

sledi, da je $F(\mathcal{A}) = a + U$, kjer je

$$a = x + 2,$$
$$U = \mathrm{Lin}\{2x^2 - x\}.$$

$\square$