7 Matrične grupe

V tem razdelku bomo z $\mathbb{F}$ označevali poljuben končen obseg, z $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ množico obrnljivih elementov v $\mathbb{F}$, z $V = \mathbb{F}^n$ n-razsežni vektorski prostor n-teric nad obsegom $\mathbb{F}$ in z $\mathcal{M}(n, \mathbb{F})$ množico vseh $n \times n$ matrik z elementi iz obsega $\mathbb{F}$.

Nadalje, naj bo $I_n \in \mathcal{M}(n, \mathbb{F})$ *identična matrika* velikosti $n \times n$. Matrika $A \in \mathcal{M}(n, \mathbb{F})$ je *obrnljiva matrika* nantanko tedaj, ko zanjo obstaja matrika A^{-1}, ki zadošča enakosti $AA^{-1} = A^{-1}A = I_n$. Matrika je obrnljiva natanko tedaj, ko ima neničelno determinanto.

7.1 Linearni grupi $\mathrm{GL}(n, \mathbb{F})$ in $\mathrm{SL}(n, \mathbb{F})$

Označimo z

$$\begin{aligned} \mathrm{GL}(n, \mathbb{F}) &= \{A \in \mathcal{M}(n, \mathbb{F}) : \det(A) \neq 0\} \quad \text{in} \\ \mathrm{SL}(n, \mathbb{F}) &= \{A \in \mathcal{M}(n, \mathbb{F}) : \det(A) = 1\} \end{aligned}$$

množico matrik z neničelno determinanto (ki združuje natanko vse obrnljive matrike) in množico matrik z determinanto 1. Ker je determinantna multiplikativna funkcija, sta obe množici $\mathrm{GL}(n, \mathbb{F})$ in $\mathrm{SL}(n, \mathbb{F})$ zaprti za množenje in invertiranje. Ker vsebujeta enoto I_n in ker je množenje matrik asociativna operacija, sta $\mathrm{GL}(n, \mathbb{F})$ in $\mathrm{SL}(n, \mathbb{F})$ grupi za množenje.

Definition 7.1 *Grupi* $\mathrm{GL}(n, \mathbb{F})$ *rečemo* splošna linearna grupa*, grupi* $\mathrm{SL}(n, \mathbb{F})$ *pa* specialna linearna grupa*, stopnje* n *nad obsegom* $\mathbb{F}$*.*

Proposition 7.2 *Grupa* $\mathrm{SL}(n, \mathbb{F})$ *je podgrupa edinka grupe* $\mathrm{GL}(n, \mathbb{F})$ *in faktorstka grupa* $\mathrm{GL}(n, \mathbb{F})/\mathrm{SL}(n, \mathbb{F})$ *je izomorfna multiplikativni grupi* $\mathbb{F}^*$ *obrnljivih elementov obsega* $\mathbb{F}$*.*

Proof. Ker je determinanta multiplikativna funkcija, ki slika obrnljive matrike v neničlne elemente obsega $\mathbb{F}$, jo lahko razumemo kot surjektivni homomorfizem grup $\mathrm{GL}(n, \mathbb{F}) \to \mathbb{F}^*$. Jedro tega homorfizma je ravno grupa $\mathrm{SL}(n, \mathbb{F})$. Zato je $\mathrm{SL}(n, \mathbb{F})$ edinka v $\mathrm{GL}(n, \mathbb{F})$, zaradi "prvega izreka o izomorfizmu" pa je faktorska grupa $\mathrm{GL}(n, \mathbb{F})/\mathrm{SL}(n, \mathbb{F})$ izomorfna sliki homomorfizma det, ki je zaradi surjektivnosti enaka $\mathbb{F}^*$. ∎

7.2 Delovanje $\mathrm{GL}(n,\mathbb{F})$ na $\mathbb{F}^n$

Če na n-terico $\vec{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}^n$ pogledamo kot na matriko velikosti $1 \times n$ in jo z desne pomnožimo z matriko iz $\mathrm{GL}(n,\mathbb{F})$, dobimo za rezultat spet matriko velikosti $1 \times n$. Hitro se prepričamo, da predpis

$$\vec{x}^A = \vec{x}A, \qquad \vec{x} \in \mathbb{F}^n,\ A \in \mathrm{GL}(n,\mathbb{F}),$$

določa delovanje grupe $\mathrm{GL}(n,\mathbb{F})$ na množici $\mathbb{F}^n$.

EXERCISE. Preveri, da zgornji predpis res določa delovanje grupe. Natančneje, preveri, da je preslikava $\Phi\colon \mathrm{GL}(n,\mathbb{F}) \to \mathrm{Sym}(\mathbb{F}^n)$, ki vsaki matriki $A \in \mathrm{GL}(n,\mathbb{F})$ priredi permutacijo $\Phi_A\colon \mathbb{F}^n \to \mathbb{F}^n$, $\Phi_A\colon \vec{x} \to \vec{x}A$, homomorfizem grup.

Seveda delovanje $\mathrm{GL}(n,\mathbb{F})$ na $\mathbb{F}^n$ ni tranzitivno, saj vsaka matrika pribije n-terico $\vec{0} = (0, \ldots, 0)$. Ker za poljubna neničelna vektorja obstaja obrnljiva matrika, ki prvega preslika v drugega, deluje grupa $\mathrm{GL}(n,\mathbb{F})$ tranzitivno na množici $V^* = \mathbb{F}^n \setminus \{\vec{0}\}$. Še več, za vsak $m \leq n$, grupa $\mathrm{GL}(n,\mathbb{F})$ deluje tranzitivno na urejenih m-tericah linearno neodvisnih vektorjev iz $\mathbb{F}^n$. Ker bomo to dejstvo v nadaljevanju večkrat uporabljali, ga formulirajmo kot trditev.

PROPOSITION 7.3 *Za naravno število m, $m \leq n$, naj bo $\mathcal{B}_m$ množica vseh urejenih m-teric linearno neodvisnih vektorjev prostora $\mathbb{F}^n$. Tedaj velja naslednje:*

(i) *Grupa $\mathrm{GL}(n,\mathbb{F})$ deluje s predpisom $(\vec{x}_1, \ldots, \vec{x}_m)^A = (\vec{x}_1 A, \ldots, \vec{x}_m A)$ na $\mathcal{B}_m$ zvesto in tranzitivno. Če je $m = n$, je to delovanje regularno.*

(ii) *Delovanje podgrupe $\mathrm{SL}(n,\mathbb{F})$ na množici $\mathcal{B}_m$ je tranzitivno natanko tedaj, ko je $m < n$ ali $|\mathbb{F}| = 2$.*

PROOF. Dokažimo najprej (i). Zvestost delovanja sledi neposredno iz dejstva, da je linerna preslikava (kar množenje z matriko seveda je) natanko določena s slikami baznih vektorjev. Matrika, ki pribije vse neničelne vektorje, je zato ena sama, to je, identična matrika.

Dokažimo sedaj tranzitivnost delovanja grupe $\mathrm{GL}(n,\mathbb{F})$ na $\mathcal{B}_m$. Označimo z $\vec{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ i-ti standardni bazni vektor prostora V. Seveda je $(\vec{e}_1, \ldots, \vec{e}_m) \in \mathcal{B}_m$. Opazimo, da je za vsako matriko $A \in \mathrm{GL}(n,\mathbb{F})$ produkt $\vec{e}_i A$ enak i-ti vrstici matrike A.

Vzemimo poljubno m-terico $(\vec{x}_1, \ldots, \vec{x}_m) \in \mathcal{B}_m$ in dokažimo, da obstaja matrika $A \in \mathrm{GL}(n,\mathbb{F})$, za katero velja $\vec{e}_i A = \vec{x}_i$ za vsak $i \in \{1, \ldots, m\}$.

Dopolnimo m-terico $(\vec{x}_1,\ldots,\vec{x}_m)\in\mathcal{B}_m$ s primernimi vektorji $\vec{x}_{m+1},\ldots,\vec{x}_n\in\mathbb{F}^n$ do baze $(\vec{x}_1,\ldots,\vec{x}_n)$ prostora $\mathbb{F}^n$ in tvorimo matriko A, katere vrstice so, zaporedoma, ravno n-terice $\vec{x}_1,\ldots,\vec{x}_n$. Ker je matrika obrnljiva natanko tedaj, ko njene vrstice tvorijo linearno neodvisno množico, je $A\in\mathrm{GL}(n,\mathbb{F})$. Ker je prvih m vrstic matrike A enakih $\vec{x}_1,\ldots,\vec{x}_m$, pa velja tudi

$$(\vec{e}_1,\ldots,\vec{e}_m)^A=(\vec{e}_1A,\ldots,\vec{e}_mA)=(\vec{x}_1,\ldots,\vec{x}_m).$$

S tem smo dokazali tranzitivnost delovanja grupe $\mathrm{GL}(n,\mathbb{F})$ na $\mathcal{B}_m$.

Stabilizator elementa $(\vec{e}_1,\ldots,\vec{e}_m)$ pri tem delovanju tvorijo vse tiste matrike A, ki prvih m standardnih baznih vektorjev pribijejo. To pa so natanko tiste matrike, ki imajo prvih m vrstic enakih $\vec{e}_1,\ldots,\vec{e}_m$, se pravi matrike z bločno strukturo

$$\left[\begin{array}{c|c} I_m & 0 \\ \hline * & C \end{array}\right],\qquad C\in\mathrm{GL}(n-m,\mathbb{F}).$$

Če je $m=n$, ta stabilizator sestavlja le matrika I_n, zato je delovanje grupe $\mathrm{GL}(n,\mathbb{F})$ na $\mathcal{B}_n$ regularno. S tem je stavek (i) dokazan.

Dokazimo še stavek (ii). Če je $m<n$, potem imamo pri izbiri vektorjev $\vec{x}_{m+1},\ldots,\vec{x}_n$ v zgornjem postopku iskanja matrike A še nekaj svobode. Na primer, vsakega od teh vektorjev lahko pomnožimo s poljubnim neničelnim skalarjem. Če je determinanta dobljene matrike A zgoraj enaka λ za nek $\lambda\neq1$, potem lahko vektor $\vec{x}_{m+1}$ nadomestimo z vektorjem $\lambda^{-1}\vec{x}_{m+1}$ in tako dobimo matriko $A'\in\mathrm{SL}(n,\mathbb{F})$, ki, enako kot A, slika m-terico $(\vec{e}_1,\ldots,\vec{e}_m)$ v m-terico $(\vec{x}_1,\ldots,\vec{x}_m)$. Delovanje grupe $\mathrm{SL}(n,\mathbb{F})$ na $\mathcal{B}_m$ je v tem primeru torej tranzitivno.

Če pa je $m=n$, potem je, kot smo videli zgoraj, delovanje grupe $\mathrm{GL}(n,\mathbb{F})$ na $\mathcal{B}_m$ regularno, in zato nobena prava podgrupa grupe $\mathrm{GL}(n,\mathbb{F})$ ne deluje na tej množici tranzitivno. Grupa $\mathrm{SL}(n,\mathbb{F})$ je zato na množici $\mathcal{B}_n$ tranzitivna le, če je $\mathrm{SL}(n,\mathbb{F})=\mathrm{GL}(n,\mathbb{F})$, kar pa se zgodi le, če je $|\mathbb{F}|=2$. ■

REMARK. Ker je množica $\{\vec{x}\}$, ki vsebuje en sam vektor, linearno neodvisna natanko tedaj, ko je $\vec{x}\neq\vec{0}$, lahko množico $\mathcal{B}_1$ iz zgornje trditve razumemo kot množico V^* neničelnih vektorjev iz $\mathbb{F}^n$. Zgornja trditev zato pravi, da je delovanje grup $\mathrm{SL}(n,\mathbb{F})$ in $\mathrm{GL}(n,\mathbb{F})$ na V^* vedno tranzitivno, razen v primeru $n=1$ in $|\mathbb{F}|\geq3$, ko je grupa $\mathrm{SL}(1,\mathbb{F})$ trivialna in zato ni tranzitivna na množici $\mathrm{PG}(1,\mathbb{F})$ moči $q-1>1$.

Ker je delovanje grupe $\mathrm{GL}(n,\mathbb{F})$ regularno na množici $\mathcal{B}_n$, je moč grupe $\mathrm{GL}(n,\mathbb{F})$ enaka moči množice $\mathcal{B}_n$. Enostaven premislek nam pove, da je

slednja enaka $(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$. Ker je $\mathrm{GL}(n,\mathbb{F})/\mathrm{SL}(n,\mathbb{F}) \cong \mathbb{F}^*$, je $|SL(n,\mathbb{F})| = \frac{1}{q-1}|\mathrm{GL}(n,\mathbb{F})|$. Od sledi naslednja trditev.

PROPOSITION 7.4 *Naj bo $\mathbb{F}$ končen obseg moči q. Tedaj velja*

$$|\mathrm{GL}(n,\mathbb{F})| = q^{\frac{n(n-1)}{2}} \prod_{k=1}^{n}(q^k-1), \qquad |\mathrm{SL}(n,\mathbb{F})| = q^{\frac{n(n-1)}{2}} \prod_{k=2}^{n}(q^k-1).$$

Oglejmo si še eno družino delovanj grupe $\mathrm{GL}(n,\mathbb{F})$. Za naravno število m, $m < n$, naj $\mathcal{L}_m = \mathcal{L}_m(n,\mathbb{F})$ označuje množico vseh m-razsežnih podprostorov prostora $\mathbb{F}^n$. Ker je za vsak $U \in \mathcal{L}_m$ in $A \in \mathrm{GL}(n,\mathbb{F})$ tudi množica $UA = \{\vec{x}A : \vec{x} \in U\}$ element $\mathcal{L}_m$, je s predpisom

$$U^A = UA, \qquad U \in \mathcal{L}_m, \quad A \in \mathrm{GL}(n,\mathbb{F})$$

določeno delovanje grupe $\mathrm{GL}(n,\mathbb{F})$ na množici $\mathcal{L}_m$.

Ker je vsak $U \in \mathcal{L}_m$ napet na neko m-terico $(\vec{x}_1,\ldots,\vec{x}_m) \in \mathcal{B}_m$ in ker vsak element $A \in \mathrm{GL}(n,\mathbb{F})$ slika linearne kombinacije vektorjev $\vec{x}_1,\ldots,\vec{x}_m$ v linearne kombinacije vektorjev $\vec{x}_1A,\ldots,\vec{x}_mA$, nam Trditev 7.3 pove naslednje:

COROLLARY 7.5 *Delovanji grup $\mathrm{GL}(n,\mathbb{F})$ in $\mathrm{SL}(n,\mathbb{F})$ na množici $\mathcal{L}_m(n,\mathbb{F})$ sta tranzitivni za vsako naravno število m, $m \le n$.*

7.3 Grupi ΓL in ΣL

Naj bo $q = p^d$ potenca praštevila p in $\mathbb{F} = \mathrm{GF}(q)$ obseg moči q. Znano je, da je grupa avtomorfizmov $\mathrm{Aut}(\mathbb{F})$ obsega $\mathbb{F}$ izomorfna ciklični grupi reda d in je generirana z avtomorfizmom, podanim s predpisom $x \mapsto x^p$. Delovanje grupe $\mathrm{Aut}(\mathbb{F})$ lahko po komponentah razširimo do delovanja na n-tericah $\mathbb{F}^n$.

Po drugi strani pa lahko grupo $\mathrm{Aut}(\mathbb{F})$ naravno vložimo tudi v grupo $\mathrm{Aut}(\mathrm{GL}(n,\mathbb{F}))$, pri čemer element $\sigma \in \mathrm{Aut}(\mathbb{F})$ identificiramo z avtomorfizmom $\vartheta(\sigma)$, podanim s predpisom

$$\vartheta(\sigma)\colon \begin{bmatrix} a_{1,1} & \ldots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \ldots & a_{n,n} \end{bmatrix} \mapsto \begin{bmatrix} a_{1,1}^\sigma & \ldots & a_{1,n}^\sigma \\ \vdots & \ddots & \vdots \\ a_{n,1}^\sigma & \ldots & a_{n,n}^\sigma \end{bmatrix}$$

Pri tem oznako ϑ navadno izpuščamo in namesto $A^{\vartheta(\sigma)}$ pišemo kar A^σ.

To nam omogoča definirati polpremi produkt

$$\Gamma\mathrm{L}(n,\mathbb{F}) := \mathrm{GL}(n,\mathbb{F}) \rtimes_{\vartheta} \mathrm{Aut}(\mathbb{F}),$$

ki mu pravimo *splošna gama linearna grupa*.

V enakosti $(\vec{x}A)^{\sigma} = \vec{x}^{\sigma}A^{\sigma}$, ki velja za poljuben element $\vec{x} \in \mathbb{F}^n$, poljubno matriko $A \in \mathrm{GL}(n,\mathbb{F})$ in poljuben avtomorfizem $\sigma \in \mathrm{Aut}(\mathbb{F})$, brž prepoznamo pogoj iz leme 3.3. Tako delovanji grup $\mathrm{GL}(n,\mathbb{F})$ in $\mathrm{Aut}(\mathbb{F})$ na množici $\mathbb{F}^n$ inducirata naravno delovanje grupe $\Gamma\mathrm{L}(n,\mathbb{F})$ na $\mathbb{F}^n$.

Ker velja $\det(A^{\sigma}) = \det(A)^{\sigma}$ za vsako matriko A in $\sigma \in \mathrm{Aut}(\mathbb{F})$, je podgrupa $\mathrm{SL}(n,\mathbb{F})$ invariantna za delovanje grupe $\mathrm{Aut}(\mathbb{F})$. Podrupi $\mathrm{SL}(n,\mathbb{F})$ in $\mathrm{Aut}(\mathbb{F})$ grupe $\Gamma\mathrm{L}(n,\mathbb{F})$ zato generirata podgrupo

$$\Sigma\mathrm{L}(n,\mathbb{F}) := \langle \mathrm{SL}(n,\mathbb{F}), \mathrm{Aut}(\mathbb{F}) \rangle \cong \mathrm{SL}(n,\mathbb{F}) \rtimes \mathrm{Aut}(\mathbb{F}),$$

ki ji pravimo *specialna sigma linearna grupa*.

7.4 Afina grupa $\mathrm{AGL}(n,\mathbb{F})$

Naj bo $\mathbb{F} = \mathrm{GF}(q)$ polje karakteristike p in moči $q = p^d$ in naj bo K aditivna grupa vektorskega prostora $\mathbb{F}^n$. Ker je množenje s poljubno matriko iz $\mathrm{GL}(n,\mathbb{F})$ aditivna preslikava na $\mathbb{F}^n$, lahko grupo $\mathrm{GL}(n,\mathbb{F})$ razumemo kot podgrupo grupe $\mathrm{Aut}(K)$. Zato lahko tvorimo polpremi produkt

$$\mathrm{AGL}(n,\mathbb{F}) := K \rtimes_{\mathrm{id}} \mathrm{GL}(n,\mathbb{F}),$$

ki jo imenujemo *afina grupa* prostora $\mathbb{F}^n$. Kot polpremi produkt grupa $\mathrm{AGL}(n,\mathbb{F})$ s predpisom

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

deluje na množici $K = \mathbb{F}^n$.

Ker stabilizator $\mathrm{GL}(n,\mathbb{F})$ točke $\vec{0} \in \mathbb{F}^n$ deluje tranzitivno na množici $\mathbb{F}^n \setminus \{\vec{0}\}$, v primeru, ko je $q = 2$ pa celo 2-tranzitivno, lahko zaključimo naslednje:

Proposition 7.6 *Grupa* $\mathrm{AGL}(n,\mathbb{F})$ *deluje na prostoru* $\mathbb{F}^n$ 2*-tranzitivno, če pa je* $\mathbb{F}$ *obseg moči* 2*, pa celo* 3*-tranzitivno.*

7.5 Projektivni grupi $\mathrm{PGL}(n,\mathbb{F})$ in $\mathrm{PSL}(n,\mathbb{F})$

V nadaljevanju poglavja bomo predpostavljali, da je $n \geq 2$. V Trditvi 7.3 smo dokazali, da je delovanje grupe $\mathrm{GL}(n,\mathbb{F})$ na množici $V^* = \mathbb{F}^n \setminus \{\vec{0}\}$ tranzitivno. V tem razdelku bomo dokazali, da je to delovanje neprimitivno in se ukvarjali z delovanjem na najdenem sistemu neprimitivnosti.

Za $\vec{x} \in \mathbb{F}^n \setminus \{\vec{0}\}$ naj bo $\mathbb{F}^*\vec{x} = \{\lambda\vec{x} : \lambda \in \mathbb{F}^*\}$ *prebodena premica* skozi vektor $\vec{x}$.

DEFINITION 7.7 *Množico* $\{\mathbb{F}^*\vec{x} : \vec{x} \in \mathbb{F}^n \setminus \{\vec{0}\}\}$ *vseh prebodenih premic prostora* $\mathbb{F}^n$ *imenujemo* projektivni prostor *razsežnosti* $n-1$ *nad obsegom* $\mathbb{F}$ *in ga označimo s* $\mathrm{PG}(n-1,\mathbb{F})$.

Z $\mathbb{F}^*I_n$ označimo grupo $\{\lambda I_n : \lambda \in \mathbb{F}^*\}$ neničelnih skalarnih matrik. Grupa $\mathbb{F}^*I_n$ je očitno edinka grupe $\mathrm{GL}(n,\mathbb{F})$ in leži v njenem centru.

PROPOSITION 7.8 *Množica* $\mathrm{PG}(n-1,\mathbb{F})$ *je sistem neprimitivnosti za delovanje grupe* $\mathrm{GL}(n,\mathbb{F})$ *na* $\mathbb{F}^n \setminus \{\vec{0}\}$. *Jedro delovanja grupe* $\mathrm{GL}(n,\mathbb{F})$ *na* $\mathrm{PG}(n-1,\mathbb{F})$ *je podgrupa* $\mathbb{F}^*I_n$.

PROOF. Označimo $G = \mathrm{GL}(n,\mathbb{F})$, $\mathcal{P} = \mathrm{PG}(n-1,\mathbb{F})$ in $V^* = \mathbb{F} \setminus \{\vec{0}\}$. Ker je $\mathbb{F}^*I_n$ edinka grupe G, je množica njenih orbit, ki je ravno množica $\mathcal{P}$, sistem neprimitivnosti za delovanje grupe G.

Naj bo K jedro delovanja grupe G na $\mathcal{P}$. Seveda je $\mathbb{F}^*I_n \leq K$. Dokažimo še vsebovanost v obratni smeri. Če je $A \in K$, potem za vsak $\vec{x} \in V^*$ obstaja $\lambda_{\vec{x}} \in \mathbb{F}^*$, da je $\vec{x}A = \lambda_{\vec{x}}\vec{x}$. Ker to velja tudi za standardne bazne vektorje, sledi, da je matrika A diagonalna. Ker je tudi $(1,\ldots,1)A = \lambda(1,\ldots,1)$ za neki $\lambda \in \mathbb{F}^*$, je matrika A skalarna. ∎

DEFINITION 7.9 *Faktorski grupi* $\mathrm{GL}(n,\mathbb{F})/\mathbb{F}^*I_n$ *pravimo* projektivna splošna linearna grupa *in jo označimo s* $\mathrm{PGL}(n,\mathbb{F})$, *ali tudi s* $\mathrm{PGL}_n(q)$, *kjer je* q *moč obsega* $\mathbb{F}$.

Oglejmo si elemente faktorske grupe nekoliko natančneje in se dogovorimo, kako jih bomo označevali. Formalno gledano so elementi faktorske grupe $\mathrm{PGL}(n,\mathbb{F}) = \mathrm{GL}(n,\mathbb{F})/\mathbb{F}^*I_n$ odseki grupe $\mathbb{F}^*I_n$ v $\mathrm{GL}(n,\mathbb{F})$, torej množice

$$\mathbb{F}^*I_nA = \{\lambda A : \lambda \in \mathbb{F}^*\}, \qquad A \in \mathrm{GL}(n,\mathbb{F}).$$

Da bomo ločili med matrikami iz $\mathrm{GL}(n,\mathbb{F})$ in ustreznimi elementi iz grupe $\mathrm{PGL}(n,\mathbb{F})$, bomo odsek $\mathbb{F}^* I_n A$, ki ga določa matrika

$$A = \begin{bmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{bmatrix}$$

označili s simbolom

$$[A] = \left[\!\!\left[\begin{array}{ccc} a_{1,1} & \dots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{array} \right]\!\!\right]. \qquad (*)$$

Ker dve matriki $A, B \in \mathrm{GL}(n,\mathbb{F})$ ležita v istem odseku (in zatorej določata isti element grupe $\mathrm{PGL}(n,\mathbb{F})$) natanko tedaj, ko je ena skalarni večkratnik druge), lahko iz elementov $a_{i,j}$ zapisa $(*)$ brez škode pokrajšamo katerikoli neničelni skalar $\lambda \in \mathbb{F}^*$.

Podobno kot elemente grupe $\mathrm{PGL}(n,\mathbb{F})$ bomo označevali tudi točke prostora $\mathrm{PG}(n-1,\mathbb{F})$. Za $\vec{x} = (x_1, x_2, \dots, x_n) \in \mathbb{F}^n$ bomo element $\mathbb{F}^*\vec{x} \in \mathrm{PG}(n-1,\mathbb{F})$ označili s simbolom $[[x_1, x_2, \dots, x_n]]$. Seveda je $[\vec{x}] = [\vec{y}]$ natanko tedaj, ko je $\vec{x}$ skalarni večkratnik vektorja $\vec{y}$.

Če elemente grupe $\mathrm{PGL}(n,\mathbb{F})$ predstavimo z matrikami, potem množenje v $\mathrm{PGL}(n,\mathbb{F})$ poteka po običajnem postopku za množenje matrik, le da smemo na katerem koli koraku iz matrike pokrajšati neničelni skalarni faktor.

EXAMPLE. Naj bo $\mathbb{F} = \mathbb{Z}_3$ in $n = 2$. Tedaj je

$$\left[\!\!\left[\begin{array}{cc} 0 & 1 \\ 2 & 1 \end{array} \right]\!\!\right] \left[\!\!\left[\begin{array}{cc} 1 & 2 \\ 0 & 1 \end{array} \right]\!\!\right] = \left[\!\!\left[\begin{array}{cc} 0 & 1 \\ 2 & 2 \end{array} \right]\!\!\right] = \left[\!\!\left[\begin{array}{cc} 0 & 2 \\ 1 & 1 \end{array} \right]\!\!\right] \quad \text{in}$$

$$[[1,2]] \left[\!\!\left[\begin{array}{cc} 0 & 1 \\ 1 & 1 \end{array} \right]\!\!\right] = [[2,0]] = [[1,0]].$$

Podobno:

$$\left[\!\!\left[\begin{array}{cc} 1 & 2 \\ 1 & 1 \end{array} \right]\!\!\right] \left[\!\!\left[\begin{array}{cc} 1 & 1 \\ 2 & 1 \end{array} \right]\!\!\right] = \left[\!\!\left[\begin{array}{cc} 2 & 0 \\ 0 & 2 \end{array} \right]\!\!\right] = \left[\!\!\left[\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right]\!\!\right],$$

ali povedano drugače,

$$\left[\!\!\left[\begin{array}{cc} 1 & 2 \\ 1 & 1 \end{array} \right]\!\!\right]^{-1} = \left[\!\!\left[\begin{array}{cc} 1 & 1 \\ 2 & 1 \end{array} \right]\!\!\right].$$

■

Na koncu še preštejemo elemente množice $\mathrm{PG}(n-1,\mathbb{F})$. Ker je to množica blokov moči $q-1$ na množici $\mathbb{F}^n \setminus \{0\}$ moči $q^n - 1$, velja naslednja trditev.

PROPOSITION 7.10 *Naj bo $\mathbb{F}$ obseg moči q. Tedaj je*

$$|\mathrm{PG}(n-1,\mathbb{F})| = \frac{q^n-1}{q-1} = q^{n-1}+q^{n-2}+\ldots+1.$$

7.6 Delovanje $\mathrm{PGL}(n,\mathbb{F})$ na $\mathrm{PG}(n-1,\mathbb{F})$

Ker delujeta grupi $\mathrm{GL}(n,\mathbb{F})$ in $\mathrm{SL}(n,\mathbb{F})$ tranzitivno na prostoru $V^* = \mathbb{F}^n \setminus \{\vec{0}\}$, delujeta tranzitivno tudi na sistemu neprimitivnosti $\mathrm{PG}(n-1,\mathbb{F})$. Zato sta na množici $\mathrm{PG}(n-1,\mathbb{F})$ tranzitivni tudi grupi $\mathrm{PGL}(n,\mathbb{F})$ in $\mathrm{PSL}(n,\mathbb{F})$. V nadaljevanju bomo dokazali, da delujeta celo 2-tranzitivno. Ampak najprej raziščimo strukturo stabilizatorjev. Označimo $(\mathbb{F}^*)^{[n]} = \{\lambda^n : \lambda \in \mathbb{F}\}$. Opazimo, da je $(\mathbb{F}^*)^{[n]}$ podgrupa grupe $\mathbb{F}^*$ reda $\frac{q-1}{\gcd(q-1,n)}$.

PROPOSITION 7.11 *Naj bo $\omega = [[1,0,\ldots,0]] \in \mathrm{PG}(n-1,\mathbb{F})$. Tedaj je*

$$\begin{aligned}
\mathrm{PGL}(n,\mathbb{F})_\omega &= \Big\{ \left[\!\!\left[\begin{array}{c|c} 1 & 0 \\ \hline \vec{a}^t & B \end{array} \right]\!\!\right] : \vec{a} \in \mathbb{F}^{n-1}, B \in \mathrm{GL}(n-1,\mathbb{F}) \Big\}, \\
\mathrm{PSL}(n,\mathbb{F})_\omega &= \Big\{ \left[\!\!\left[\begin{array}{c|c} 1 & 0 \\ \hline \vec{a}^t & B \end{array} \right]\!\!\right] : \vec{a} \in \mathbb{F}^{n-1}, B \in \mathrm{GL}(n-1,\mathbb{F}), \det(B) \in (\mathbb{F}^*)^{[n]} \Big\}.
\end{aligned}$$

Kot abstraktna grupa je $\mathrm{PGL}(n,\mathbb{F})_\omega$ izomorfna afini grupi $\mathrm{AGL}(n-1,\mathbb{F})$.

PROOF. Element $[A] \in \mathrm{PGL}(n,\mathbb{F})$ pribije točko ω, če in samo če A preslika prvi standardni bazni vektor $\vec{e}_1$ v $\lambda\vec{e}_1$ za neki $\lambda \in \mathbb{F}^*$, torej natanko tedaj, ko je prva vrstica matrike A enaka $[\lambda,0,\ldots,0]$ za $\lambda \neq 0$. Prvi del trditve zdaj enostavno sledi, če upoštevamo $[A] = [\lambda^{-1}A]$.

Spomnimo se, da je $\mathrm{AGL}(n,\mathbb{F}) \cong \mathbb{F}^n \rtimes \mathrm{GL}(n,\mathbb{F})$ in definirajmo preslikavo

$$\Phi\colon \mathrm{PGL}(n,\mathbb{F})_\omega \to \mathbb{F}^n \rtimes \mathrm{GL}(n,\mathbb{F}), \qquad \Phi\colon \left[\!\!\left[\begin{array}{c|c} 1 & 0 \\ \hline \vec{a}^t & B \end{array} \right]\!\!\right] \mapsto (\vec{a}, B^{-t}),$$

kjer smo z B^{-t} označili inverz transponiranke B^t. Dobra definiranost in injektivnost preslikave sledi iz dejstva, da ima vsak odsek $[A] \in \mathrm{PGL}(n,\mathbb{F})_\omega$ natanko enega predstavnika z enico v levem zgornjem kotu. Ker je surjektivnost preslikave očitna, sledi, da je Φ dobro definirana bijektivna preslikava.

Ker je $\Phi([I_n]) = (\vec{0}, I_{n-1})$, zadošča preveriti, da Φ slika produkt v produkt. Računajmo!

$$\Phi\Big(\left[\!\!\left[\begin{array}{c|c} 1 & 0 \\ \hline \vec{b}^t & B \end{array} \right]\!\!\right] \left[\!\!\left[\begin{array}{c|c} 1 & 0 \\ \hline \vec{c}^t & C \end{array} \right]\!\!\right]\Big) = \Phi\Big(\left[\!\!\left[\begin{array}{c|c} 1 & 0 \\ \hline (\vec{b}+\vec{c}B^t)^t & BC \end{array} \right]\!\!\right]\Big) = (\vec{b}+\vec{c}B^t, (BC)^{-t}).$$

Po drugi stani je

$$\Phi\Big(\Big[\!\Big[\begin{array}{c|c} 1 & 0 \\ \hline \vec{b}^t & B \end{array}\Big]\!\Big]\Big)\,\Phi\Big(\Big[\!\Big[\begin{array}{c|c} 1 & 0 \\ \hline \vec{c}^t & C \end{array}\Big]\!\Big]\Big) = (\vec{b}, B^{-t})(\vec{c}, C^{-t}) = (\vec{b} + \vec{c}B^t, B^{-t}C^{-t}).$$

Ker smo obakrat dobili isti rezultat, je Φ res homomorfizem grup. ∎

PROPOSITION 7.12 *Naj bo $\mathbb{F}$ končen obseg in $n \geq 2$. Grupi $\mathrm{PGL}(n,\mathbb{F})$ in $\mathrm{PSL}(n,\mathbb{F})$ delujeta na množici $\mathrm{PG}(n-1,\mathbb{F})$ 2-tranzitivno. Če je $n = 2$, deluje $\mathrm{PGL}(2,\mathbb{F})$ na projektivni premici $\mathrm{PG}(1,\mathbb{F})$ celo 3-tranzitivno.*

PROOF. Dokažimo najprej da deluje grupa $\mathrm{PSL}(n,\mathbb{F})$ (in s tem tudi $\mathrm{PGL}(n,\mathbb{F})$) 2-tranzitivno. Ker že vemo, da je delovanje tranzitivno, je dovolj dokazati, da je delovanje stabilizatorja $\mathrm{PSL}(n,\mathbb{F})_\omega$ tranzitivno na množici $\mathrm{PG}(n-1,\mathbb{F}) \setminus \{\omega\}$. V ta namen vzemimo poljuben $[\vec{x}] = [[x_1,\ldots,x_n]] \in \mathrm{PG}(n-1,\mathbb{F}) \setminus \{\omega\}$ in poiščimo element stabilizatorja $\mathrm{PSL}(n,\mathbb{F})_\omega$, ki $[\vec{e}_2] = [[0,1,\ldots,0]]$ preslika v $[\vec{x}]$. Dopolnimo vektor $\vec{x}' = (x_2,\ldots,x_n)$ do baze $\vec{x}', \vec{x}'_3, \ldots, \vec{x}'_n$ prostora $\mathbb{F}^{n-1}$, izračunamo determinanto α matrike, katere vrstice so zaporedoma $\vec{x}', \vec{x}'_3, \ldots, \vec{x}'_n$, in tvorimo matriko

$$M = \left[\!\!\left[\begin{array}{c|c} 1 & 0 \\ \hline \alpha^{-1}x_1, & \alpha^{-1}\vec{x}' \\ 0 & \vec{x}'_3 \\ \vdots & \vdots \\ 0 & \vec{x}'_n \end{array}\right]\!\!\right].$$

Tedaj je $[\vec{e}_2]^M = [\vec{e}_2 M] = [[\lambda^{-1}\vec{x}_1, \ldots, \lambda^{-1}x_n]] = \vec{x}$ in ker je $\det(\lambda^{-1}A) = 1$, je $M \in \mathrm{PSL}(n,\mathbb{F})_\omega$. S tem smo dokazali, da deluje $\mathrm{PSL}(n,\mathbb{F})$ na $\mathrm{PG}(n-1,\mathbb{F})$ 2-tranzitivno.

Naj bo sedaj $n = 2$ in opazujmo delovanje grupe $\mathrm{PGL}(2,\mathbb{F})$ na projektivni premici $\mathrm{PG}(1,\mathbb{F})$. Ker že vemo, da je to delovanje 2-tranzitivno, je dovolj dokazati, da stabilizator $\mathrm{PGL}(2,\mathbb{F})_{\omega,\gamma}$ elementov $\omega = [\vec{e}_1]$ in $\gamma = [\vec{e}_2]$ deluje tranzitivno na $\mathrm{PG}(1,\mathbb{F}) \setminus \{\omega,\gamma\}$.

Vzemimo poljuben element $[[x_1,x_2]] \in \mathrm{PG}(1,\mathbb{F}) \setminus \{\omega,\gamma\}$ in dokažimo, da obstaja $[A] \in \mathrm{PGL}(2,\mathbb{F})_{\omega,\gamma}$, ki preslika $[\vec{e}] = [[1,1]]$ v $[[x_1,x_2]]$. Ker je $[[x_1,x_2]] \neq [[1,0]],[[0,1]]$, lahko predpostavimo, da sta oba x_1 in x_2 neničelna. Definirajmo

$$M = \left[\!\!\left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & x_1^{-1}x_2 \end{array}\right]\!\!\right].$$

Očitno M pribije tako ω kot γ, hkrati pa preslika $[[1,1]]$ v $[[1, x_1^{-1}x_2]] = [[x_1, x_2]]$. ∎

7.7 Projektivne geometrije

Spomnimo se, da za vsak $m \leq n$ grupi $\mathrm{GL}(n,\mathbb{F})$ in $\mathrm{SL}(n,\mathbb{F})$ delujeta tudi na množici $\mathcal{L}_m$ m-razsežnih podprostorov prostora $\mathbb{F}^n$. Ta delovanja so, kot pravi Posledici 7.5, tranzitivna.

Za podprostor $U \in \mathcal{L}_m$ označimo $[U] = \{[\vec{x}] : \vec{x} \in U\}$ in definirajmo množico $(m-1)$-razsežnih *projektivnih podprostorov* projektivnega prostora $\mathrm{GF}(n-1,\mathbb{F})$

$$P\mathcal{L}_m = \{[U] : U \in \mathcal{L}_m\}.$$

Opazimo, da je preslikava $U \mapsto [U]$, bijekcija med $\mathcal{L}_m$ in $P\mathcal{L}_m$, zato je

$$|P\mathcal{L}_m| = |\mathcal{L}_m|.$$

Na množici $P\mathcal{L}_m$ definirajmo delovanje grupe $\mathrm{PGL}(n,\mathbb{F})$ s predpisom

$$[U]^{[A]} = [U^A]$$

za vsak $[A] \in \mathrm{PGL}(n,\mathbb{F})$. Prepričajmo se najprej, da je ta definicija dobra, (tj., da velja $[U^A] = [U^B]$, kadarkoli je $[A] = [B]$). Res, če je $[A] = [B]$, potem je $B = \lambda A$ za neki $\lambda \in \mathbb{F}^*$, in zato $[U^B] = [U^{\lambda A}] = [(\lambda U)^A] = [U^A]$.

Ker grupi $\mathrm{GL}(,\mathbb{F})$ in $\mathrm{SL}(n,\mathbb{F})$ delujeta na množica $\mathcal{L}_m$ tranzitivno, sta tranzitivni tudi delovanji grup $\mathrm{PGL}(n,\mathbb{F})$ in $\mathrm{PGL}(n,\mathbb{F})$ na $\mathcal{L}_m$ za vsak $m \leq n$.

Predpostavimo sedaj, da je $2 \leq m \leq n-1$ in definirajmo na množici $\mathrm{PG}(n-1,\mathbb{F})$ incidenčno strukturo, katere točke so elementi množice $\mathrm{PG}(n-1,\mathbb{F})$, bloki elementi množice $\mathcal{L}_m$, incidenca pa običajna relacija vsebovanosti. Dobljeno incidenčno strukturo označimo s $\mathrm{PG}_{m-1}(n-1,\mathbb{F})$ in jo imenujemo *projektivna geometrija* projektivne razsežnosti $n-1$ in stopnje $m-1$.

Ker grupa $\mathrm{PGL}(n,\mathbb{F})$ deluje tako na točkah kot na blokih te strukture in pri tem ohranja relacijo vsebovanosti, je $\mathrm{PGL}(n,\mathbb{F})$ podgrupa grupe avtomorfizmov dobljene incidenčne strukture. Iz povedanega sledi naslednje:

PROPOSITION 7.13 *Grupa avtomorfizmov projektivne geometrije* $\mathrm{PGL}(n,\mathbb{F})$ *vsebuje podgrupo* $G \cong \mathrm{PGL}(n,\mathbb{F})$, *ki deluje na točkah* 2*-tranzitivno, na blokih pa tranzitivno.*

Oglejmo si primer $n = 3$ in $m = 2$ nekoliko podrobneje. V tem primeru rečemo projektivni geometriji $\mathrm{PG}_1(2, \mathbb{F})$ tudi *projektivna ravnina nad obsegom* $\mathbb{F}$. Blokom te geometrije rečemo tudi *premice* projektivne ravnine.

Ker je premica projektivne ravnine slika dvorazsežnega podprostora prostora $\mathbb{F}^3$ pri preslikavi $U \mapsto [U]$, je natanko določena z enačbo $a_1x_1+a_2x_2+a_3x_3 = 0$. Pri tem seveda velja, da dve trojki (a_1, a_2, a_3) in (a'_1, a'_2, a_3) določata isto projektivno premico če in samo če se razlikujeta za neničelni skalarni faktor. To nam omogoča, da definiramo preslikavo

$$\tau\colon \mathrm{PG}(2, \mathbb{F}) \to P\mathcal{L}_2, \quad [[a_1, a_2, a_3]] \mapsto \{[[x_1, x_2, x_3]] : a_1x_1+a_2x_2+a_3x_3 = 0\}.$$

Opazimo, da je preslikava τ bijektivna.

PROPOSITION 7.14 *Projektivna ravnina* $\mathrm{PG}_1(2, \mathbb{F})$ *nad obsegom* $\mathbb{F}$ *moči* q *vsebuje* $q^2 + q + 1$ *točk in enako število premic. Vsaka točka je vsebovana v* $q + 1$ *premicah in vsaka premica vsebuje* $q + 1$ *točk. Vsaki dve premici se sekata v natanko eni točki in za vsaki dve točki obstaja natanko ena premica, ki ju obe vsebuje.*

PROOF. Trditev o številu točk projektivne ravnine smo dokazali že s trditvijo 7.10. Vemo tudi, da je premic v projektivni ravnini ravno toliko kot točk.

Vzemimo točko $\omega = [[1, 0, 0]]$ projektivne ravnine in premislimo na koliko premicah leži. Ker je $a_1 \cdot 1 + a_2 \cdot 0 + a_3 \cdot 0 = 0$ natank tedaj, ko je $a_1 = 0$, je takšnih premic natanko toliko, kot je elementov $[[a_1, a_2, a_3]] \in \mathrm{PG}(2, \mathbb{F})$ s prvo komponento ničelno. Takšen, kjer je tudi $a_2 = 0$, je en sam. Če pa je $a_2 \neq 0$, pa lahko predpostavimo, da je $a_2 = 1$ in a_3 poljuben element iz $\mathbb{F}$. Slednjih je torej q, skupaj $q + 1$.

∎