Универзитет у Београду

Математички факултет

КЛАСИЧНЕ ГРУПЕ
И
»БОТАНИКА« ПОДГРУПА ИЗАБРАНИХ ЛИНЕАРНИХ ГРУПА

-Мастер рад-

ментор:
проф. др Зоран Петровић

студент:
Марко Пешовић

Београд, 2014.

ПРЕДГОВОР

Циљ овог рада је да се изложе и упореде класичне групе, одреде њихови специфични генератори и опишу све подгрупе изабраних коначних линеарних група.

Рад се састоји из два поглавља.

Прво поглавље је кратак преглед класичних група. Први део је посвећен линеарним и пројективним групама, њиховим генераторима и њиховим основним својствима. У другом делу су описане изометрија и сличност, те унитарна, ортогонална и симплектична група.

Друго поглавље приказује елементе и подгрупе линеарних група, њихове класе конјугација, централизаторе елемената и нормализаторе подгрупа. У овом делу су посматране линеарне групе $GL(2,2)$ и $GL(2,3)$, као и група $GL(3,2)$ којој су изоморфне све просте групе реда 168.

Садржај

Глава 1

КЛАСИЧНЕ ГРУПЕ

1.1 Линеарна група

Нека је $\mathbb{K}$ комутативно поље и $\mathbf{V}$ векторски простор над пољем скалара $\mathbb{K}$, димензије n.

Дефиниција 1. *Линеарна група $GL(\mathbf{V})$ је група $\mathbb{K}$-аутоморфизама векторског простора $\mathbf{V}$, над пољем $\mathbb{K}$, у односу на њихово множење.*

Ако је $e = [e_1, e_2, \dots, e_n]$ база простора $\mathbf{V}$ и $L : \mathbf{V} \to \mathbf{V}$ аутоморфизам простора $\mathbf{V}$, тада је и $[L(e_1), L(e_2), \dots, L(e_n)]$ база простора $\mathbf{V}$.

Специјано, сваки аутоморфизам L одређен је инверзибилном матрицом реда n над пољем скалара $\mathbb{K}$. Стога, јасно је да је $GL(\mathbf{V})$ изоморфно групи инверзибилних матрица реда n, над пољем $\mathbb{K}$, тј.

$$GL(\mathbf{V}) \cong GL(n, \mathbb{K}) = \{A \in M_n(\mathbb{K}) : \det(A) \in \mathbb{K}^*\}.$$

Дефиниција 2. *Специјална линеарна група $SL(\mathbf{V})$ је подгрупа групе $GL(\mathbf{V})$ изоморфна групи $SL(n, \mathbb{K})$, групи инверзибилних матрица реда n над пољем $\mathbb{K}$, чија је детерминанта једнака јединици, тј.*

$$SL(\mathbf{V}) \cong SL(n, \mathbb{K}) = \{A \in M_n(\mathbb{K}) : \det(A) = 1\}.$$

Посматрајмо пресликавање $L \in GL(\mathbf{V})$ које је одређено матрицом A у односу на базу e. Нека је $e' = [e'_1, e'_2, \dots, e'_n]$ друга база простора $\mathbf{V}$ и матрица P матрица преласка са базе e' на базу e. Тада матрици пресликавања $L \in GL(\mathbf{V})$, у односу на базу e, одговара матрица $P^{-1}AP$, у односу на базу e'. Приметимо, матрице A и $P^{-1}AP$ су конјуговане над $GL(n, \mathbb{K})$.

Дефиниција 3. *Пресликавања $L \in GL(\mathbf{V})$ и $L' \in GL(\mathbf{V})$ су конјугована акко су матрице, њима одређене, конјуговане над $GL(n, \mathbb{K})$.*

Ако је $f(X) = a_0 + a_1X + .. + a_mX^m$ произвољан полином из $\mathbb{K}[X]$, тада:

$$f(P^{-1}AP) = P^{-1}f(A)P.$$

Приметимо, $f(P^{-1}AP) = 0 \Leftrightarrow f(A) = 0$, па матрице $P^{-1}AP$ и A анулирају исте полиноме. Штавише:

Теорема 1. *Конјуговане матрице у $GL(n, \mathbb{K})$ имају исти минимални полином, исти траг и исту детерминанту.*

1.1.1 Дилатација

Теорема 2. *Нека је H хиперраван простора $\mathbf{V}$ и $L \in GL(\mathbf{V})$ пресликавање такво да је $L|_H = \mathrm{Id}_H$. Следећа четири услова су еквивалентна:*

1° $\det(L) = \lambda \neq 1$, *тј.* $L \notin SL(\mathbf{V})$,

2° *L има сопствену вредност $\lambda \neq 1$ и матрица пресликавања L је дијагонална,*

3° $D = \mathrm{Im}(L - \mathrm{Id}) \not\subset H$,

4° *за погодну базу, матрица пресликавања L је:*

$$\begin{bmatrix} 1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 \\ 0 & \dots & 0 & \lambda \end{bmatrix}, \quad \lambda \in \mathbb{K}^*, \quad \lambda \neq 1.$$

Доказ. Јасно је да важи $4^\circ \Rightarrow 1^\circ \Rightarrow 2^\circ$, остаје још да докажемо:

$2^\circ \Rightarrow 3^\circ$ Нека је x вектор који одговара сопственој вредности $\lambda \neq 1$, тј. $L(x) = \lambda x$. Пошто $L(x) - x = \lambda x - x = (\lambda - 1)x \neq 0$, то $x \notin H$. Тада $D = \mathrm{Im}(L - \mathrm{Id}) \not\subset H$ и важи $\dim(D) = 1$ и $D = \langle x \rangle$.

$3^\circ \Rightarrow 4^\circ$ Нека је $[e_1, e_2, \dots, e_{n-1}]$ база за H и $e_n \in D$, које га генерише. Како $e_n \notin H$, то $L(e_n) - e_n \neq 0$ и $L(e_n) - e_n \in D$, тј. $L(e_n) - e_n = \mu e_n$, за $\mu \neq 0$.
Коначно, $L(e_n) = (1 + \mu)e_n = \lambda e_n$, за $\lambda \neq 1$.

□

Дефиниција 4. *Уколико су испуњени услови Теореме 2. и један од четири еквивалентна исказа, кажемо да је L дилатација хиперрравни H по правој D са коефицијентом λ, где је $H = \mathrm{Ker}(L - \mathrm{Id})$ и $D = \mathrm{Im}(L - \mathrm{Id})$.*
Уколико је $\lambda = -1$ и $\mathbb{K}$ поље карактеристике различите од два, кажемо да је L рефлексија.

Став 1. *Две дилатације су конјуговане акко имају исти коефицијент.*

1.1.2 Трансвекција

Теорема 3. *Нека је H хиперраван простора $\mathbf{V}$ и $f \in \mathbf{V}^*$, линеарна форма простора $\mathbf{V}$ за коју важи $H = \mathrm{Kef}(f)$ и $f \neq 0$. Ако $L \in GL(\mathbf{V})$ и ако је $L \neq \mathrm{Id}$ и $L|_H = \mathrm{Id}_H$, следећих пет услова су еквивалентни:*

1° $\det(L) = 1$, *тј.* $L \in SL(\mathbf{V})$,

2° *матрица пресликавања L није дијагонална,*

3° $D = \mathrm{Im}(L - \mathrm{Id}) \subset H$,

4° $(\exists a \in H,\ a \neq 0)$ *такво да* $(\forall x \in \mathbf{V})$

$$L(x) = x + f(x)a,$$

5° *за погодну базу, матрица пресликавања L је:*

$$\begin{bmatrix} 1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 \\ 0 & \dots & 1 & 1 \end{bmatrix}.$$

Доказ. Јасно је да важи 5° $\Rightarrow$ 1° $\Rightarrow$ 2° $\Rightarrow$ 3°. Докажимо још:

3° $\Rightarrow$ 4° Посматрајмо $x_0 \in \mathbf{V}$, тд. $f(x_0) = 1$. Елемент $a = L(x_0) - x_0$ припада $D = \mathrm{Im}(L - \mathrm{Id}) \subset H$. Пошто $x_0 \notin H$, следи да $a \neq 0$. Специјално, за свако x важи $L(x) = x + f(x)a$.

4° $\Rightarrow$ 5° Нека је $[e_1, e_2, \dots, e_{n-1}]$ база за H и $e_{n-1} = a$. Приметимо да важи једнакост $L(e_i) = e_i$ $(\forall i \in \{1, \dots, n-1\})$.
Постоји $e_n \notin H$ такво да је $f(e_n) = 1$ и $[e_1, e_2, \dots, e_{n-1}, e_n]$ база простора $\mathbf{V}$. Стога, $L(e_n) = e_n + e_{n-1}$.

□

Дефиниција 5. *Уколико су испуњени услови Теореме 3. и један од пет еквивалентних исказа, кажемо да је L трансвекција хиперрравни H у правцу D, где је $D = \langle a \rangle$ и $D \subset H$.*

Приметимо да је свака трансфекција, у ознаци $\tau(f, a)$, одређена линеарном формом $f \in \mathbf{V}^*$, $f \neq 0$ и елементом $a \in \mathrm{Ker}(f)$, $a \neq 0$. Тада за свако $x \in \mathbf{V}$ важи:

$$\tau(f, a)(x) = x + f(x)a.$$

Став 2. *Нека је $f \in \mathbf{V}^*$, $f \neq 0$ и $a, b \in H = \mathrm{Ker}(f)$ и $a, b \neq 0$. Тада важи:*

$$\tau(f, a)\tau(f, b) = \tau(f, a + b).$$

$$\tau^{-1}(f, a) = \tau(f, -a).$$

Став 3. *Нека је τ трансфекција хиперравни H у правцу D и $L \in GL(\mathbf{V})$. Тада је $L\tau L^{-1}$ трансфекција хиперравни $L(H)$ у правцу $L(D)$. Прецизније, ако је $\tau = \tau(f, a)$ тада:*

$$L\tau L^{-1} = \tau(f \circ L^{-1}, L(a)).$$

Доказ. За произвољно $x \in V$ важи $\tau L^{-1}(x) = L^{-1}(x) + f(L^{-1}(x))a$ и

$$L\tau L^{-1}(x) = x + f(L^{-1}(x))L(a).$$

Пошто је $H = \mathrm{Ker}(f)$, то је $L(H) = \mathrm{Ker}(f \circ L^{-1})$. □

Став 4. *Две трансвекције су конјуговане над $GL(\mathbf{V})$.*

Став 5. *Две трансвекције су конјуговане над $SL(\mathbf{V})$, за $\dim(\mathbf{V}) > 2$.*

Доказ. Посматрајмо трансвекције τ и τ'. По претходном Ставу имамо да је $\tau = L\tau' L^{-1}$, за неко $L \in GL(\mathbf{V})$.
Постоји база таква да је матрица пресликавања τ:

$$\begin{bmatrix} 1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 \\ 0 & \dots & 1 & 1 \end{bmatrix}.$$

Нека је $\det(L) = \lambda$, тада постоји $G \in GL(\mathbf{V})$ такво да је $\det(G) = \lambda^{-1}$ и $G\tau G^{-1} = \tau$. Матрица пресликавања G је:

$$\begin{bmatrix} 1 & 0 & \dots & \dots & \dots & 0 \\ 0 & \ddots & \ddots & & & \vdots \\ \vdots & \ddots & 1 & \ddots & & \vdots \\ \vdots & & \ddots & \lambda & \ddots & \vdots \\ \vdots & & & \ddots & \lambda^{-1} & 0 \\ 0 & \dots & \dots & \dots & 0 & \lambda^{-1} \end{bmatrix}.$$

Приметимо, $\det(GL) = \det(G)\det(L) = \lambda^{-1}\lambda = 1$. Стога, $GL \in SL(V)$.
Коначно, $\tau = (GL)\tau'(GL)^{-1}$.

□

1.1.3 Центар линеарне групе

Став 6. *Нека је $L \in GL(\mathbf{V})$. Претпоставимо $(\forall x \in \mathbf{V})$ $(\exists \lambda \in \mathbb{K}^*)$ тд. $L(x) = \lambda x$. Тада је L хомотетија.*

Доказ. Потребно је доказати да $(\exists \lambda \in \mathbb{K}^*)$ $(\forall x \in \mathbf{V})$ $L(x) = \lambda x$.
Нека су x и y неколинеарни вектори за које важи $L(x) = \alpha x$ и $L(y) = \beta y$.

$$\mu(x + y) = L(x + y) = L(x) + L(y) = \alpha x + \beta y,$$

Коначно, $\mu = \alpha = \beta$. □

Теорема 4. *Центар Z, групе $GL(\mathbf{V})$, чине хомотетије са коефицијентом λ, за $\lambda \in \mathbb{K}^*$. Специјално, $Z \cong \mathbb{K}^*$.*

Доказ. Нека се $L \in GL(\mathbf{V})$ налази у центру Z. Тада,

$$(\forall L' \in GL(\mathbf{V})) \qquad LL' = L'L, \qquad \text{тј.} \qquad LL'L^{-1} = L'.$$

Специјално, за $L' = \tau$, имамо да је $L\tau L^{-1} = \tau$. Тада је $L\tau L^{-1}$ трансфекција у правцу $L(D)$, где је D правац трансфекције τ, то је и $L(D) = D$.
Пошто важи за све праве D, следи да је L хомотетија. □

Последица 1. *Ако је $h_\lambda \in GL(\mathbf{V})$ хомотетија са коефицијентом λ, тада:*

$$\det(h_\lambda) = \lambda^n,$$

где је n димензија простора $\mathbf{V}$.

Последица 2. *Центар групе $SL(\mathbf{V})$ је $Z \cap SL(\mathbf{V})$ и изоморфан је са:*

$$\{\lambda \in \mathbb{K} : \lambda^n = 1\}.$$

1.1.4 Генератори линеарне групе

Став 7. *Нека су* $x,\, y \in \mathbf{V} - \{0\}$. *Тада постоји трансвекција* τ *или производ трансвекција* $\tau\tau'$, *тако да важи* $\tau(x) = y$ *или* $\tau'\tau(x) = y$.

Доказ. Разматрајмо два случаја:

Случај када су вектори x и y неколинеарни.
Нека је $a = y - x$ и H хиперрраван која садржи a и не садржи x.
Изаберимо f тако да је $f(x) = 1$. Посматрајмо $\tau(x) = x + f(x)a$.
Приметимо да задата трансфекција задовољава услов $\tau(x) = y$.

Случај када су x и y колинеарни.
Постоји $z \in \mathbf{V}$, неколинеарно са x и са y. Тада постоје трансвекције τ и τ' такве да је $\tau(x) = z$ и $\tau'(z) = y$. Коначно, $\tau'\tau(x) = y$.

□

Став 8. *Нека је* $L \in GL(\mathbf{V})$ *и* $L \neq \mathrm{Id}$. *Следећа два услова су еквивалентна.*

1° τ *је трансфекција у правцу* D.

2° *за* $\tau|_D = \mathrm{Id}|_D$, *хомоморфизам индукован са* $\overline{\tau} : E/D \to E/D$ *је идентитет.*

Доказ. $1^\circ \Rightarrow 2^\circ$ Нека је $x = \overline{x} + D$ и $\tau(x) = \tau(\overline{x}) + D$.
Пошто $\tau(\overline{x}) - \overline{x} \in D$, то је дати хомоморфизам идентитет.

$2^\circ \Rightarrow 1^\circ$ Услов да је $\overline{\tau}(\overline{x}) = \overline{x}$ можемо записати:

$$(\forall x \in V) \qquad \tau(x) - x \in D.$$

Како је $\mathrm{Im}(\tau - \mathrm{Id}) \subset D$ и $\tau \neq \mathrm{Id}$, то је $\mathrm{Im}(\tau - \mathrm{Id}) = D$ и $\mathrm{Ker}(\tau - \mathrm{Id})$ је хиперраван која садржи праву D. Коначно, τ је трансфекција у правцу D.

□

Теорема 5. *Трансфекције генеришу специјалну линеарну групу* $SL(\mathbf{V})$.

Доказ. Нека је $x \in \mathbf{V}$ и $x \neq 0$. Применом Става 7. можемо добити пресликавање $\tau \in SL(\mathbf{V})$, које је трансфекција или производ две трансфекције, за које важи $\tau(x) = x$.
Означимо са D праву генерисану са x, а са $\overline{\tau} : \mathbf{V}/D \to \mathbf{V}/D$ аутоморфизам генерисан са τ. Покажимо да $\overline{\tau} \in SL(\mathbf{V}/D)$.
Нека је $\pi : \mathbf{V} \to \mathbf{V}/D$ канонска пројекција и $[x = e_1,\, e_2,\, ...,\, e_n]$ база простора $\mathbf{V}$. Тада је $[\tau(e_2),\, ...,\, \tau(e_n)]$ база за $\mathbf{V}/D$. Пошто је $\tau(e_1) = e_1$, то се из развоја детерминанте пресликавања τ добија да је $\det\overline{\tau} = 1$, тј. $\overline{\tau} \in SL(\mathbf{V}/D)$.
Јасно је да теорема важи за $\dim(\mathbf{V}) = 1$. Претпоставимо да важи за $r = \dim(\mathbf{V}/D)$ и докажимо да важи за $r + 1 = \dim(\mathbf{V})$.
Претпоставимо да је $\overline{\tau} = \overline{\tau_1}...\overline{\tau_r}$, где су $\overline{\tau_i} = \tau(\overline{f_i}, \overline{a_i})$ трансфекције у $\mathbf{V}/D$.
И нека су $a_i \in \mathbf{V}$ такви да $\pi(a_i) = \overline{a_i}$ и $f_i \in \mathbf{V}^*$ такви да $f_i = \overline{f_i} \circ \pi$.
Означимо са $\tau_i = \tau(f_i, a_i)$ и са $\tau' = \tau_1...\tau_r$. Јасно је да τ_i индукују $\overline{\tau_i}$.
Приметимо да је $f_i(x) = \overline{f_i} \circ \pi(x) = 0$ и $\tau_i(x) = x$.
Коначно, $\tau'(x) = \tau(x)$ и $\overline{\tau'} = \overline{\tau}$ и $\tau'^{-1}\tau$ је трансфекција (по Ставу 7.), одакле следи да је и τ трансфекција. □

Последица 3. *Трансфекције и дилатације генеришу линеарну групу* $GL(\mathbf{V})$.

Доказ. Изаберимо произвољно $L \in GL(\mathbf{V})$ и нека је $\det(L) = \lambda$. Тада постоји дилатација L' са коефицијентом λ^{-1}.
$L'L \in SL(\mathbf{V})$ и $L'L$ је генерисана трансфекцијама, одакле следи да је L генерисана трансфекцијама и дилатацијом. □

1.1.5 Аутоморфизми чији је траг једнак нули

Нека је $\mathbf{V}$ векторски простор над пољем $\mathbb{K}$, димензије $n > 1$. И нека је $e = [e_1, e_2, \dots, e_n]$ база простора $\mathbf{V}$. Аутоморфизме простора $\mathbf{V}$, чији је траг једнак нули, означимо са $\mathcal{N}$, тј.

$$\mathcal{N} = \{L \in GL(\mathbf{V}) : \operatorname{tr}(L) = 0\}.$$

Посматрајмо аутоморфизам L који је, у односу на базу e, одређен матрицом:

$$\begin{bmatrix} 0 & 0 & \dots & 0 & (-1)^{n+1}\lambda \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix}.$$

Приметимо да $L \in \mathcal{N}$ и да је $\det(L) = \lambda$. Специјално, важи следећи:

Став 9. *Нека је* $\lambda \in \mathbb{K}^*$. *Тада постоји* $L \in \mathcal{N}$ *тд.* $\det(L) = \lambda$.

Став 10. *Произвољна трансвекција простора* $\mathbf{V}$ *се може приказати као производ елемената из* $\mathcal{N}$.

Доказ. Нека је τ трансвекција простора $\mathbf{V}$. Постоји база e, за коју је матрица пресликавања τ:

$$T_n = \begin{bmatrix} 1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 \\ 0 & \dots & 1 & 1 \end{bmatrix} = \left[\begin{array}{c|c} E_{n-2} & 0 \\ \hline 0 & T_2 \end{array}\right], \quad T_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Уколико је $n = 2$, тада $T_2 = \begin{bmatrix} -1 & 0 \\ -1 & 1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$, што је и требало доказати.
За $n > 2$ уочимо пресликавања генерисана матрицама:

$$P_1 = \begin{bmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & \ddots & & \vdots & \vdots \\ \vdots & & 1 & 0 & 0 \\ 0 & \dots & 0 & 1 & 0 \end{bmatrix}, \quad P_2 = \begin{bmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ \vdots & \ddots & & \vdots & \vdots \\ 0 & \dots & 1 & 0 & \vdots \\ 0 & \dots & 1 & 1 & 0 \end{bmatrix}.$$

Лако се покаже да је $P_1 T_n = P_2$ и $P_1^{-1} = P_1^{\perp}$.
Стога, $T_n = P_1^{-1} P_2 = P_1^{\perp} P_2$, тј. матица T_n се може приказати као производ две матрице, чији је траг једнак нули. □

Теорема 6. *Сваки елемент групе $GL(\mathbf{V})$ се може приказати као производ елемената из $\mathcal{N}$.*

Доказ. Посматрајмо произвољно пресликавање $L \in GL(\mathbf{V})$. Тада постоји $L_1 \in \mathcal{N}$ тако да је $\det(L) = \det(L_1)$.
Уочимо $G = LL_1^{-1}$. Пошто је $\det(G) = 1$, то $G \in SL(\mathbf{V})$.
Пошто је $SL(\mathbf{V})$ генерисано трансфекцијама, а трансфекције су производ елемената из $\mathcal{N}$, то је и G производ елемената из $\mathcal{N}$.
Коначно, $L = L_1 G$, тј. L се може приказати као производ елемената из $\mathcal{N}$. □

1.1.6 Пројективна линеарна група

Дефиниција 6. *Количник групе $GL(\mathbf{V})$ по свом центру је пројективна линеарна група $PGL(\mathbf{V})$. Количник групе $SL(\mathbf{V})$ по свом центру је $PSL(\mathbf{V})$.*

Теорема 7. *Група $PSL(\mathbf{V})$ је проста, осим ако је:*

1° $\dim(\mathbf{V}) = 2$ *и* $\mathbb{K} = \mathbb{Z}_2$,

2° $\dim(\mathbf{V}) = 2$ *и* $\mathbb{K} = \mathbb{Z}_3$.

Доказ. Доказаћемо само случај када је $\dim(\mathbf{V}) = n > 2$.

Нека је $\overline{N}$ нормална подгрупа групе $PSL(V)$ и претпоставимо да $\overline{N}$ није неутрал. Одговарајућа подгрупа N из $SL(\mathbf{V})$ или садржи центар од $SL(\mathbf{V})$ и тај исти центар Z је нормалан у односу на N, или је $N = SL(\mathbf{V})$.
Како трансвекције генеришу $SL(\mathbf{V})$ и како су све међусобно конјуговане над $SL(\mathbf{V})$, довољно је да се докаже да је једна од њих у N.
Посматрајмо нетривијалан елемент $L \in N$. Тада пресликавање $G = L(\tau L^{-1}\tau^{-1}) \in N$, где је τ трансвекција хиперравни H и $L\tau L^{-1}$ трансфекција хиперравни $L(H)$.
Уколико је $L(H) = H$ и $G \neq \mathrm{Id}$, тада је $G = (L\tau L^{-1})\tau^{-1}$ трансфекција, као производ две такве. На тај начин смо изградили елемент из N који је инваријантан у односу на H.
Нека је $L \in N$ и $L \notin Z$. Пошто L није хомотетија, постоји $a \in \mathbf{V}$ такво да су $L(a)$ и a неколинеарни вектори.
Нека је τ трансвекција у правцу $\langle a \rangle$ и $G = L\tau L^{-1}\tau^{-1}$. И нека је H хиперраван H која садржи раван $\langle a, L(a) \rangle$.
Тада важи:

1° $G \in N$ и $G \neq \mathrm{Id}$,

2° $(\forall x \in \mathbf{V})\ G(x) - x \in H$,

3° $G(H) = H$.

Јасно је да је $G \in N$. Уколико је $G = \mathrm{Id}$, тада је $\tau = L\tau L^{-1}$, тј. трансвекције τ и $L\tau L^{-1}$ имају исти правац, одакле је $\langle a \rangle = \langle L(a) \rangle$, што је у контрадикцији са избором вектора a и $L(a)$.
Лако је уочити да је $G(x) - x \in \langle a, L(a) \rangle \subset H$ и $G(H) = H$.
Разматрајмо две могућности:

(I) Ако постоји трансвекција u хиперравни H која не комутира са G.

Тада $v = GuG^{-1}u^{-1} \in N$. Приметимо да је $v \neq \mathrm{Id}$ и како је производ трансвекције u^{-1}, хиперравни H, и GuG^{-1}, хиперравни $G(H) = H$, тада је v нетривијална трансвекција из N.

(II) Ако G комутира са свим трансвекцијама хиперравни H.

Нека је $f \in \mathbf{V}^*$ једначина хиперравни H и u трансвекција у односу на вектор $c \in H$, тј.
$$u(x) = x + f(x)c.$$
Како је $Gu = uG$, тада је за свако $x \in V$:
$$G(x) + f(x)G(c) = G(x) + f(G(x))c.$$
Пошто $G(x) - x \in H$, за $x \notin H$ важи $f(G(x)) = f(x) \neq 0$, па је $G(c) = c$.
Како важи за свако $c \in H$ и како је $G|_H = \mathrm{Id}|_H$ и $\det(G) = 1$, то је G једна трансвекција.

У оба случаја N садржи трансвекцију, стога је $N = SL(\mathbf{V})$, што је и требало доказати. □

1.1.7 Линеарне групе над коначним пољем

Нека је $\mathbb{F}_q$ поље са q елемената и $q = p^\alpha$, за прост p и $\alpha \in \mathbb{N}^*$.

Теорема 8. *Кардиналност линеарне и специјално линеарне групе над пољем $\mathbb{F}_q$ је:*

1° $|GL(n, \mathbb{F}_q)| = (q^n - 1)\ (q^n - q)\ ...\ (q^n - q^{n-2})\ (q^n - q^{n-1})$.

2° $|SL(n, \mathbb{F}_q)| = (q^n - 1)\ (q^n - q)\ ...\ (q^n - q^{n-2})\ q^{n-1}$.

Доказ. Случај 1°. Претпоставимо да је $[e_1, e_2, \dots, e_n]$ канонска база за $\mathbb{F}_q^n$.
За $A \in GL(n, \mathbb{F}_q)$ имамо да је и $[Ae_1, Ae_2, \dots, Ae_n]$ база за $\mathbb{F}_q^n$. Специјално, постоји бијекција између за $GL(n, \mathbb{F}_q)$ и $\mathbb{F}_q^n$.
Изаберимо базу $[a_1, a_2, \dots, a_n]$. За a_1 бирамо произвољан ненула вектор који можемо изабрати на $q^n - 1$ начина. a_2 бирамо тако да не припада правој $\langle a_1 \rangle$. То можемо урадити на $q^n - q$ начина.
Ако су $a_1, a_2, \dots, a_i$ изабрани, a_{i+1} бирамо тако да не припада векторском потпростору генерисаном са $[a_1, a_2, \dots, a_i]$. За то постоји $q^n - q^i$ могућности.
Коначно, a_n можемо изабрати на $q^n - q^{n-1}$ начин.
Како $\mathbb{F}_q^*$ има $q - 1$ елемента, аналогним разматрањем добијамо тврђење за случај 2°. □

Став 11. *Кардиналност пројективних линеарних група над пољем $\mathbb{F}_q$ је:*

1° $|PGL(n, \mathbb{F}_q)| = |SL(n, \mathbb{F}_q)|$,

2° $|PSL(n, \mathbb{F}_q)| = \frac{|SL(n, \mathbb{F}_q)|}{d}$, *за* $d =$*НЗД*$(n, q-1)$.

1.2 Унитарна, ортогонална и симлектична група

1.2.1 Косо-линеарне форме

Посматрајмо комутативно поље $\mathbb{K}$ и аутоморфизам σ, поља $\mathbb{K}$. Уведимо ознаку:

$$\lambda^\sigma = \sigma(\lambda).$$

Аутоморфизам σ је инволуција ако је $\sigma^2 = \mathrm{Id}$.

Дефиниција 7. *Нека је $\mathbf{V}$ векторски простор над пољем $\mathbb{K}$. Пресликавање $f : \mathbf{V} \times \mathbf{V} \to \mathbb{K}$ називамо σ-косо-линеарна форма ако задовољава следећа два услова:*

1° *за фиксирано y, пресликавање $x \mapsto f(x,y)$ је линеарно,*

2° *за фиксирано x, пресликавање $y \mapsto f(x,y)$ је σ-полу-линеарно, тј.*

$$(\forall \lambda \in \mathbb{K}) \qquad f(x, \lambda y) = \lambda^\sigma f(x,y).$$

Специјално, уколико је $\sigma = \mathrm{Id}$ пресликавање f називамо билинеарно.

Приметимо да произвољаном елементу $y \in \mathbf{V}$ додељујемо линеарну форму $f_y(x) = f(x,y)$, над $\mathbf{V}$. Посматрајмо преликавање $\overline{f} : \mathbf{V} \to \mathbf{V}^*$, задато са:

$$\overline{f}(y) = f_y.$$

Дефиниција 8. *За пресликавање f кажемо да је недегенерисано ако је пресликавање $\overline{f}$ инјективно.*

Уведимо следеће појмове:

Дефиниција 9. *Нека је f косо-линеарна форма над $\mathbf{V}$.*

а) *Кажемо да је f рефлексивна ако за свако x, $y \in \mathbf{V}$ важи:*

$$f(x,y) = 0 \Leftrightarrow f(y,x) = 0.$$

б) *Кажемо да је f алтернирајућа акко за свако $x \in \mathbf{V}$ важи:*

$$f(x,x) = 0.$$

Дефиниција 10. *Нека је f билинеарна форма над $\mathbf{V}$.*

а) *Кажемо да је f симетрична ако за свако x, $y \in \mathbf{V}$ важи:*

$$f(x,y) = f(y,x).$$

б) *Кажемо да је f антисиметрична ако за свако x, $y \in \mathbf{V}$ важи:*

$$f(x,y) = -f(y,x).$$

Приметимо да су симетрична и антисиметрична форма рефлексивне.

Став 12. *Ако је f алтернирајућа форма и $f \neq 0$, тада важи:*

1° $\sigma = \mathrm{Id}$,

2° *f је антисиметрична.*

Доказ. За произвољно $x, y \in \mathbf{V}$ важи:

$$0 = f(x+y, x+y) = f(x,x) + f(x,y) + f(y,x) + f(y,y).$$

Коначно, $f(x,y) = -f(y,x)$, одале следа је f антисиметрична.
Нека су $x, y \in \mathbf{V}$ такви да $f(x,y) \neq 0$ и $\lambda \in \mathbb{K}$.

$$f(\lambda x, y) = \lambda f(x,y) = -\lambda f(y,x),$$

$$f(\lambda x, y) = -f(y, \lambda x) = -\lambda^\sigma f(y,x).$$

Коначно, $\lambda = \lambda^\sigma$, за све $\lambda \in \mathbb{K}$. Тада је $\sigma = \mathrm{Id}$. □

Дефиниција 11. *Нека је f σ-косо-линеарна форма и $\sigma \neq 0$. Кажемо да је f хермитска ако за свако x, $y \in \mathbf{V}$ важи:*

$$f(y,x) = f(x,y)^\sigma.$$

Теорема 9. *Нека је $\mathbf{V}$ векторски простор коначне димензије n. Ако је f σ-косо-линеарна, недегенерисана и рефлексивна форма, тада је σ инволуција, тј. $\sigma^2 = \mathrm{Id}$ и важи:*

а) *Ако $\sigma = \mathrm{Id}$, тада је f симетрична или антисиметрична,*

б) *Ако $\sigma \neq \mathrm{Id}$, тада постоји $\alpha \in \mathbb{K}$ такво да је αf хермитска.*

1.2.2 Ортогонални потпростори и изотропност

Дефиниција 12. *За x и $y \in \mathbf{V}$ кажемо да су ортогонални у односу на f ако је $f(x,y) = 0$, и пишемо $x \perp y$.*
Потпростори A и B су ортогонални ако $(\forall x \in A)$ $(\forall y \in B)$ $x \perp y$.

Дефиниција 13. *Нека је A потпростор векторског простора $\mathbf{V}$. Ортогонал $A^\perp$ потпростора A је потпростор задат са:*

$$A^\perp = \{x \in \mathbf{V} : (\forall a \in A)\ a \perp x\}.$$

Специјално, ако је $\dim(A) = p$ тада је $\dim(A^\perp) = n - p$, где је n димензија простора $\mathbf{V}$.

Посматрамо рефлексифну косо-линеарну форму f над простором $\mathbf{V}$, која је или симетрична, или хермитска, или алтернирајућа.

Дефиниција 14. *Нека је $x \in \mathbf{V}$ и $x \neq 0$. x је изотропан акко $f(x,x) = 0$.*

Дефиниција 15. *Потпростор $A \subset \mathbf{V}$ је изотропан ако је $A \cap A^\perp \neq 0$, тј. уколико постоји $x \in A$, такво да за свако $y \in A$ важи $f(x,y) = 0$.*

1.2.3 Изометрија

Дефиниција 16. *Аутоморфизам $L \in GL(\mathbf{V})$ је изометрија ако за свако x, $y \in \mathbf{V}$ важи:*

$$f(L(x), L(y)) = f(x, y).$$

Нека је $[e_1, e_2, \dots, e_n]$ база простора $\mathbf{V}$ и $L \in GL(\mathbf{V})$. L је изометрија акко за свако i и j важи:

$$f(L(e_i), L(e_j)) = f(e_i, e_j).$$

Став 13. *Изометрије чине подгрупу простора $GL(\mathbf{V})$.*

Дефиниција 17. *За подгрупу изометрија кажемо да је:*

а) *унитарна, уколико је f хермитска (ознака: $U(f)$).*

б) *ортогоналнана, уколико је f симетрична (ознака: $O(f)$).*

в) *симплектична, уколико је f алтернирајућа (ознака: $S_p(f)$).*

Дефиниција 18. *За групу кажемо да је класична ако је симплектична, унитарна или ортогонална.*

Дефиниција 19. *Специјана унитарна група $SU(f)$ је подгрупа коју чине изометрије унитарне групе $U(f)$, чија је детерминанта једнака јединици.*

1.2.4 Ортогонална група

Дефиниција 20. *Специјана ортогонална група $SO(f)$ је подгрупа коју чине изометрије ортогоналне групе $O(f)$, чија је детерминанта једнака јединици.*

Дефиниција 21. *Елементе специјалне ортогоналне групе називамо позитивне изометрије или ротације.*

Дефиниција 22. *Изометрије ортогоналне групе $O(f)$ чија је детерминанта једнака -1 називамо негативне изометрије.*

Нека је f симетрична форма и $[e_1, e_2, \dots, e_n]$ база простора $\mathbf{V}$. Ако је $L \in GL(\mathbf{V})$ и $L^2 = \mathrm{Id}$, тада постоје потпростори $\mathbf{V}^+$ и $\mathbf{V}^-$ тд:

1° $\mathbf{V} = \mathbf{V}^+ \oplus \mathbf{V}^-$,

2° $L_{\mathbf{V}^+} = \mathrm{Id}_{\mathbf{V}^+}$ и $L_{\mathbf{V}^-} = -\mathrm{Id}_{\mathbf{V}^-}$.

И нека је $[e_1, e_2, \dots, e_p]$ база за $\mathbf{V}^+$ и $[e_{p+1}, e_{p+2}, \dots, e_n]$ база за $\mathbf{V}^-$. Матрица пресликавања L дата је са:

$$\begin{bmatrix} 1 & 0 & \dots & \dots & \dots & 0 \\ 0 & \ddots & \ddots & & & \vdots \\ \vdots & \ddots & 1 & \ddots & & \vdots \\ \vdots & & \ddots & -1 & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ 0 & \dots & \cdots & \cdots & 0 & -1 \end{bmatrix}.$$

Дефиниција 23. *Горе описано пресликавање називамо симетрија, уколико је* $L \neq \mathrm{Id}$.

Приметимо, ако је $\dim(\mathbf{V}^-) = 1$, пресликавање L је рефлексија.

Став 14. *Нека је* $L \in \mathbf{V}$, $L^2 = \mathrm{Id}$ *и* $\mathbf{V}^+$ *и* $\mathbf{V}^-$ *горе описани потпростори.* L *је симетрија акко су* $\mathbf{V}^+$ *и* $\mathbf{V}^-$ *ортогонални.*
Специјално, $\mathbf{V}^+ = (\mathbf{V}^-)^\perp$ *и* $\mathbf{V}^- = (\mathbf{V}^+)^\perp$.

Доказ. Претпоставимо да је L изометрија. Нека су $x \in \mathbf{V}^+$ и $y \in \mathbf{V}^-$.

$$f(x,y) = f(L(x), L(y)) = f(x,-y) = f(-y,x) = -f(y,x) = -f(x,y),$$

одакле је $f(x,y) = 0$, па су потпростори $\mathbf{V}^+$ и $\mathbf{V}^-$ ортогонални.
Супротно, нека су $\mathbf{V}^+$ и $\mathbf{V}^-$ ортогонални и нека су x, $y \in \mathbf{V}$, за које важи разлагање:

$$x = x^+ + x^- \text{ и } y = y^+ + y^-, \text{ за } x^+,\, y^+ \in \mathbf{V}^+ \text{ и } x^-,\, y^- \in \mathbf{V}^-.$$

Дефинишимо:

$$L(x) = x^+ - x^- \text{ и } L(y) = y^+ - y^-.$$

Тада,

$$f(x,y) = f(x^+, y^+) + f(x^-, y^-) = f(L(x), L(y)).$$

Коначно, $L \in O(f)$. □

Последица 4. *Посматрајмо потпростор* $W \subset \mathbf{V}$ *који није изотропан. Тада постоји тачно једна симетрија* L *таква да* $W = \mathbf{V}^+(L)$.

Доказ. Дефинишимо L тако да $L|_W = -\mathrm{Id}_W$ и $L|_{W^\perp} = \mathrm{Id}_{W^\perp}$.
По претходном Ставу L је изометрија и важи $W = \mathbf{V}^+(L)$. □

Специјално, ако је L рефлексија тада је $\mathbf{V}^+(L)$ хиперраван, а $\mathbf{V}^-(L)$ права, тј. L је трансвекција у правцу $\mathbf{V}^-(L)$.

Може се доказати следећа:

Теорема 10. *Ортогонална група је генерисана рефлексијама.*

Дефиниција 24. *Нека су* f *и* f' *две косо-линеарне форме над простором* $\mathbf{V}$. *Кажемо да су еквивалентне ако постоји* $L \in GL(\mathbf{V})$ *тако да за свако* $x, y \in \mathbf{V}$ *важи:*

$$f'(x,y) = f(L(x), L(y)).$$

Из претходне дефиниције јасно је да:

$$G \in O(f') \Leftrightarrow LGL^{-1} \in O(f).$$

Теорема 11. *Ако су* f *и* f' *еквивалентне косо-линеарне форме, тада су* $O(f)$ *и* $O(f')$ *конјуговане над* $GL(\mathbf{V})$.

1.2.5 Сличност

Дефиниција 25. *Нека је f недегенерисана косо-линеарна форма над $\mathbf{V}$. И нека је хермитска, симетрична или алтернирајућа. За $L \in GL(\mathbf{V})$ кажемо да је сличност са коефицијентом $\mu \in \mathbb{K}^*$, ако за свако x, $y \in \mathbf{V}$ важи:*

$$f(L(x), L(y)) = \mu\ f(x, y).$$

У зависности од природе форме f, ознаке које користимо за сличност су $GU(f)$, $GO(f)$ и $GS_p(f)$.

Приметимо, изометрија је сличност са коефицијентом један.

Став 15. *Хомотетија са коефицијентом λ је сличност са коефицијентом $\lambda\lambda^\sigma$.*

Доказ. Нека је $L \in GL(\mathbf{V})$ хомотетија са коефицијентом λ. Тада:

$$f(L(x), L(y)) = f(\lambda x, \lambda y) = \lambda\lambda^\sigma\ f(x, y).$$

Што је и требало доказати. □

Нека је f косо-линеарна форма. За базу $[e_1,\ e_2,\ \ldots\ , e_n]$ векторског простора $\mathbf{V}$ кажемо да је ортогонална у односу на f ако:

$$(\forall i, j)\ i \neq j \Rightarrow f(e_i, e_j) = 0.$$

Тада је матрица пресликавања f дијагонална матрица облика:

$$\begin{bmatrix} f(e_1, e_1) & 0 & \ldots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & f(e_n, e_n) \end{bmatrix}.$$

Став 16. *Нека је $\mathbf{V}$ векторски простор димензије n над пољем скалара $\mathbb{K}$ и f недегенерисана форма. Тада за $L \in GL(\mathbf{V})$ важи:*

$$L \in GO(f) \Leftrightarrow ((\forall x,\ y \in \mathbf{V})\ x \perp y \Rightarrow L(x) \perp L(y)).$$

Доказ. Случај $\Rightarrow$ је тривијалан.
Супротно, нека је $[e_1,\ e_2,\ \ldots\ , e_n]$ ортогонална база у односу на f. Тада је и $[e'_1,\ e'_2,\ \ldots\ , e'_n]$ ортогонална база, за $e'_i = L(e_i)$.
Како је f недегенерисана то је $f(e_i, e_i) \neq 0$ и $f(e'_i, e'_i) \neq 0$. Приметимо да је $f(e'_i, e'_i) = \mu_i\ f(e_i, e_i)$. Потребно је доказати да су μ_i-ови једнаки.
Приметимо да су вектори $e_i + e_j$ и $e_i + (-\frac{f(e_i,e_i)}{f(e_j,e_j)})e_j$ ортогонални:

$$f(e_i + e_j,\ e_i + (-\tfrac{f(e_i,e_i)}{f(e_j,e_j)})e_j) = f(e_i, e_i) - \tfrac{f(e_i,e_i)}{f(e_j,e_j)}\ f(e_j, e_j) = 0.$$

Тада су и вектори $e'_i + e'_j$ и $e'_i + (-\frac{f(e'_i,e'_i)}{f(e'_j,e'_j)})e'_j$ ортогонални, као и вектори $e'_i + e'_j$ и $e'_i + (-\frac{f(e_i,e_i)}{f(e_j,e_j)})e'_j$.
Приметимо,

$$\lambda = -\tfrac{f(e_i,e_i)}{f(e_j,e_j)} = -\tfrac{f(e'_i,e'_i)}{f(e'_j,e'_j)} = -\tfrac{\mu_i f(e_i,e_i)}{\mu_j f(e_j,e_j)} = \lambda\tfrac{\mu_i}{\mu_j}.$$

Коначно, $\mu_i = \mu_j$. □

Глава 2

»БОТАНИКА« ПОДГРУПА ИЗАБРАНИХ ЛИНЕАРНИХ ГРУПА

2.1 »Ботаника« групе $G = GL(2,2)$

Нека је $\mathbf{V}$ векторски простор над пољем $\mathbb{Z}_2$ и $e = [e_1, e_2]$ база простора $\mathbf{V}$. Посматрајмо све $\mathbb{Z}_2$-аутоморфизме простора $\mathbf{V}$ који су одређени инверзибилним матрицама реда два, над пољем $\mathbb{Z}_2$.

$$GL(2,2) = \{M \in M_2(\mathbb{Z}_2) : \det(M) \neq 0\} = \{M \in M_2(\mathbb{Z}_2) : \det(M) = 1\},$$

одакле следи:

$$GL(2,2) = SL(2,2).$$

2.1.1 Ред и класе конјугације групе G

Применом Теореме 8. добијамо:

$$|G| = (2^2 - 1)(2^2 - 2) = 6 = 2 \times 3.$$

Нека је $M \in G$ и није јединична. Карактеристични полином матрице M је:

$$\chi_M = X^2 - \operatorname{tr}(M)X + \det(M).$$

Специјално, кажемо да је M реда n ако M поништава полином $X^n - 1$. По Теореми 1. сличне матрице имају исти траг и исту детерминанту, па су карактеристични полиноми и класе конјугације:

- случај $\chi_M = X^2 + 1$,

$$\mathcal{C}_0 = \{M \in G \backslash \{E\} : \operatorname{tr}(M) = 0\}.$$

Пошто је $\chi_M = X^2 + 1$ исто што и $X^2 - 1$, то је ред матрице M два. Елементи ове класе конјугације су:

$$S_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, S_2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, S_3 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

- случај $\chi_M = X^2 - X + 1$,

$$\mathcal{C}_1 = \{M \in G : \mathrm{tr}(M) = 1\}.$$

Пошто $\chi_M = X^2 + X + 1$ дели $(X^2 + X + 1)(X - 1) = X^3 - 1$, то је ред матрице M три. Елементи ове класе конјугације су:

$$R_1 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, R_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

- случај $\chi_M = X + 1$,

$$\{E\}.$$

Како је $\chi_M = X + 1$ исто што и $X - 1$, то је ред матрице M један. Елемент ове класе конјугације је:

$$E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

2.1.2 Централизатори елемената групе G

Нека је $M \in G$. Централизатор елемента M је:

$$C(M) = \{A \in G : MA = AM\}, \quad |C(M)| = |G|/|\mathcal{C}(M)|.$$

- случај $M \in \mathcal{C}_0$:

$$|C(M)| = \frac{|G|}{|\mathcal{C}(M)|} = \frac{6}{3} = 2.$$

Како је M реда 2 и како $M, E \in C(M)$, то је

$$C(M) = \langle M \rangle.$$

- случај $M \in \mathcal{C}_1$:

$$|C(M)| = \frac{|G|}{|\mathcal{C}(M)|} = \frac{6}{2} = 3.$$

Одредимо централизатор елемента R_1.
Тражимо $A \in C(R_1)$ за које важи $AR_1 = R_1A$, тј.

$$\begin{bmatrix} a+b & a \\ c+d & c \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ a & b \end{bmatrix}.$$

Добијамо да је $C(R_1) = \{E, R_1, R_2\}$.
Аналогним разматрањем добијамо и $C(R_2) = \{E, R_1, R_2\}$.
Приметимо да важе следеће релације:

$$R_1^2 = R_2 \text{ и } R_2^2 = R_1.$$

Тада је лако уочити да важи:

$$C(R_1) = \langle R_1 \rangle \quad \text{и} \quad C(R_2) = \langle R_2 \rangle.$$

- случај $M = E$:

$$|C(E)| = \frac{|G|}{|\mathcal{C}(E)|} = \frac{6}{1} = 6.$$

Пошто је $|G| = 6$, то је:

$$C(E) = G.$$

Класе конј. $\mathcal{C}$	$\lvert\mathcal{C}\rvert$	Ред $M \in \mathcal{C}$	Центр. $C(M)$	$\lvert C(M)\rvert$
$\{E\}$	1	1	G	6
$\mathcal{C}_0$	3	2	$\langle M\rangle$	2
$\mathcal{C}_1$	2	3	$\langle M\rangle$	3

2.1.3 Подгрупе групе G и њихови нормализатори

Нека је W подгрупа групе G. Нормализатор од W је:

$$N(W) = \{A \in G : AW = WA\}.$$

Број подгрупа конјугованих са подгрупом W је $|G|/|N(W)|$.

Нетривијалне подгрупе групе G су:

- **Подгрупе реда два.**

Подгрупе реда два су генерисане елементима реда 2. Постоје 3 подгрупе:

$$\langle S_1\rangle, \quad \langle S_2\rangle \quad \text{и} \quad \langle S_3\rangle.$$

Елементи групе $\langle S_1\rangle$ су E и S_1. Приметимо,

$$N(\langle S_1\rangle) = C(\langle S_1\rangle) \cup \{A \in G : AS_1A^{-1} = E\}.$$

Пронађимо $A \in G$ такве да је $AS_1 = EA$, тј.

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

Како не постоје тражени елементи, то је

$$N(\langle S_1\rangle) = C(S_1) = \langle S_1\rangle.$$

Број конјугованих подгрупа са $\langle S_1\rangle$ је

$$\frac{|G|}{|N(\langle S_1\rangle)|} = \frac{6}{2} = 3.$$

Како су S_1, S_2 и S_3 конјуговане, то су и подргупе $\langle S_1\rangle$, $\langle S_2\rangle$ и $\langle S_3\rangle$ су међусобно конјуговане.

- **Подгрупе реда три.**

Подгрупе реда три су цикличне групе генерисане елементима реда 3. Постоји само једна подргрупа:

$$\langle R_1 \rangle = \langle R_2 \rangle.$$

Елементи подгрупе $\langle R_1 \rangle$ су E, R_1 и R_2.

$$N(\langle R_1 \rangle) = C(\langle R_1 \rangle) \cup \{A \in G : AR_1A^{-1} = R_2\},$$

Тражимо $A \in G$ такве да важи $AR_1 = R_2A$, тј.

$$\begin{bmatrix} a+b & a \\ c+d & c \end{bmatrix} = \begin{bmatrix} c & d \\ a+c & b+d \end{bmatrix}.$$

Пошто елементи S_1, S_2 и S_3 задовољавају тражену једнакост, то:

$$N(\langle R_1 \rangle) = \{E, R_1, R_2\} \cup \{S_1, S_2, S_3\} = G.$$

Како је нормализатор подгрупе сама група G, то је:

$$\langle R_1 \rangle \triangleleft G.$$

Лако је уочити да је центар групе G јединична матрица E, па је:

$$PGL(2,2) = GL(2,2) = SL(2,2) = PSL(2,2).$$

Приметимо, R_1 је реда 3, S_1 је реда 2 и важи:

$$S_1R_1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = R_1^{-1}S_1.$$

Коначно, $G = \langle R_1, S_1 \rangle$ и $G \cong \mathbf{D}_3$.

Подгр.	Ред подгр.	Тип	Бр. кл. конј.	Норм.	Ред норм.
$\langle E \rangle$	1	циклична	1	G	6
$\langle S \rangle$	2	циклична	3	$\langle S \rangle$	2
$\langle R \rangle$	3	циклична	1	G	6
G	6	$\mathbf{D}_3$	1	G	6
			Укупно: 6		

2.2 »Ботаника« групе $G = GL(2,3)$

Нека је $\mathbf{V}$ векторски простор над пољем $\mathbb{Z}_3$ и $e = [e_1, e_2]$ база простора $\mathbf{V}$. Посматрајмо све $\mathbb{Z}_3$-аутоморфизме простора $\mathbf{V}$ који су одређени инверзибилним матрицама реда два, над пољем $\mathbb{Z}_3$. И нека је:

$$H = SL(2,3) = \{M \in G : \det(M) = 1\}.$$

2.2.1 Ред и класе конјугације групе G

Применом Теореме 8. добијамо:

$$|G| = (3^2 - 1)(3^2 - 3) = 48 = 2^4 \times 3,$$

$$|H| = (3^2 - 1)3^1 = 24 = 2^3 \times 3.$$

Нека је $M \in G$, која није скаларна. Карактеристични полином матрице M означимо са:

$$\chi_{\mathrm{tr}(M),\det(M)} = X^2 - \mathrm{tr}(M)X + \det(M).$$

Специјално, кажемо да је M реда n ако M поништава полином $X^n - 1$.
Како сличне матрице имају исти траг и исту детерминанту, то су карактеристични полиноми и класе конјугације:

- случај $\chi_{-1,1} = X^2 + X + 1$,

$$\mathcal{C}_{-1,1} = \{M \in G\backslash\{E\} : \mathrm{tr}(M) = -1 \wedge \det(M) = 1\}.$$

Како $\chi_{-1,1} = X^2 + X + 1$ дели $(X^2 + X + 1)(X - 1) = X^3 - 1$, то је ред матрице $M \in \mathcal{C}_{-1,1}$ три. Елементи ове класе конјугације су:

$$T_1 = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix},\ T_2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

$$T_3 = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix},\ T_4 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},\ T_5 = \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix},$$

$$T_6 = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix},\ T_7 = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix},\ T_8 = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}.$$

Приметимо да је:

$$T^{-1} = T^2.$$

Важе још и следеће једнкости:

$$\begin{array}{lll} T_3 = T_1^T, & T_5 = T_1^{-1}, & T_7 = T_1^{-1,T}, \\ T_4 = T_2^T, & T_6 = T_2^{-1}, & T_8 = T_2^{-1,T}. \end{array}$$

- случај $\chi_{0,1} = X^2 + 1$,

$$\mathcal{C}_{0,1} = \{M \in G : \mathrm{tr}(M) = 0 \wedge \det(M) = 1\}.$$

Како $\chi_{0,1} = X^2 + 1$ дели $(X^2 + 1)(X^2 - 1) = X^4 - 1$, то је ред матрице $M \in \mathcal{C}_{0,1}$ четири. Елементи ове класе конјугације су:

$$Q_1 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},\ Q_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},\ Q_3 = \begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix},$$

$$Q_4 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},\ Q_5 = \begin{bmatrix} -1 & -1 \\ -1 & 1 \end{bmatrix},\ Q_6 = \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}.$$

Приметимо,

$$Q^{-1} = -Q \text{ и } Q^2 = -E,$$

и важе следеће једнакости:

$$Q_4 = Q_1^{-1}, \;\; Q_5 = Q_2^{-1}, \;\; Q_6 = Q_3^{-1}.$$

- случај $\chi_{1,1} = X^2 - X + 1$,

$$\mathcal{C}_{1,1} = \{M \in G \backslash \{-E\} : \mathrm{tr}(M) = 1 \wedge \det(M) = 1\}.$$

Како $\chi_{1,1} = X^2 - X + 1 = (X+1)^2$ дели $(X+1)^2(X^2-X+1)^2 = X^6 - 1$, то је ред матрице $M \in \mathcal{C}_{1,1}$ шест. Елементи ове класе конјугације су:

$$S_1 = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}, S_2 = \begin{bmatrix} -1 & -1 \\ 0 & -1 \end{bmatrix}, S_3 = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix},$$

$$S_4 = \begin{bmatrix} -1 & 0 \\ -1 & -1 \end{bmatrix}, S_5 = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}, S_6 = \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix},$$

$$S_7 = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}, S_8 = \begin{bmatrix} -1 & 0 \\ 1 & -1 \end{bmatrix}.$$

Приметимо,

$$S = -T,$$

и још важи:

$$\begin{aligned} S_1^5 = S_1^{-1} = S_5, \quad S_2^5 = S_2^{-1} = S_6, \\ S_3^5 = S_3^{-1} = S_7, \quad S_4^5 = S_4^{-1} = S_8. \end{aligned}$$

- случај $\chi_{-1,-1} = X^2 + X - 1$,

$$\mathcal{C}_{-1,-1} = \{M \in G : \mathrm{tr}(M) = -1 \wedge \det(M) = -1\}.$$

Како $\chi_{-1,-1} = X^2 + X - 1$ дели $(X^2 + X - 1)(X^2 - X - 1) = X^4 + 1$ што дели $(X^4 + 1)(X^4 - 1) = X^8 - 1$, то је ред матрице $M \in \mathcal{C}_{-1,-1}$ осам. Елементи ове класе конјугације су:

$$F_1 = \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix}, F_2 = \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix}, F_3 = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix},$$

$$F_4 = \begin{bmatrix} -1 & -1 \\ -1 & 0 \end{bmatrix}, F_5 = \begin{bmatrix} 0 & -1 \\ -1 & -1 \end{bmatrix}, F_6 = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}.$$

- случај $\chi_{0,-1} = X^2 - 1$,

$$\mathcal{C}_{0,-1} = \{M \in G : \mathrm{tr}(M) = 0 \wedge \det(M) = -1\}.$$

Како је $\chi_{0,-1} = X^2 - 1$, то је ред матрице $M \in \mathcal{C}_{0,-1}$ два. Елементи ове класе конјугације су:

$$D_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, D_2 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, D_3 = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix},$$

$$D_4 = \begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix}, D_5 = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, D_6 = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix},$$

$$D_7 = \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix}, D_8 = \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}, D_9 = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix},$$

$$D_{10} = \begin{bmatrix} 1 & 0 \\ -1 & -1 \end{bmatrix}, D_{11} = \begin{bmatrix} -1 & 0 \\ -1 & 1 \end{bmatrix}, D_{12} = \begin{bmatrix} -1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Приметимо,

$$\begin{gathered} D_5 = -D_1, \quad D_7 = -D_3, \\ D_6 = -D_2, \quad D_8 = -D_4. \end{gathered}$$

И још важи:

$$\begin{gathered} D_9 = D_3^T, \quad D_{11} = -D_3^T, \\ D_{10} = D_4^T, \quad D_{12} = -D_4^T. \end{gathered}$$

- случај $\chi_{1,-1} = X^2 - X - 1$,

$$\mathcal{C}_{1,-1} = \{M \in G : \operatorname{tr}(M) = 1 \wedge \det(M) = -1\}.$$

Како $\chi_{1,-1} = X^2 - X - 1$ дели $(X^2 - X - 1)(X^2 + X - 1) = X^4 + 1$ што дели $(X^4 + 1)(X^4 - 1) = X^8 + 1$, то је ред матрице $M \in \mathcal{C}_{1,-1}$ осам. Елементи ове класе конјугације су:

$$B_1 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, B_2 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, B_3 = \begin{bmatrix} -1 & -1 \\ 1 & -1 \end{bmatrix},$$

$$B_4 = \begin{bmatrix} 0 & -1 \\ -1 & 1 \end{bmatrix}, B_5 = \begin{bmatrix} 1 & -1 \\ -1 & 0 \end{bmatrix}, B_6 = \begin{bmatrix} -1 & 1 \\ -1 & -1 \end{bmatrix}.$$

Приметимо да је $B = F^{-1}$, и важе следеће једнакости:

$$\begin{gathered} B_1^3 = B_5, \quad B_1^5 = F_5, \quad B_1^7 = F_1, \\ B_2^3 = B_4, \quad B_2^5 = F_4, \quad B_2^7 = F_2, \\ B_3^3 = B_6, \quad B_3^5 = F_6, \quad B_3^7 = F_3. \end{gathered}$$

- случај $\chi = X + 1$,

$$\{-E\}.$$

Како $\chi = X + 1$ дели $(X+1)(X-1) = X^2 - 1$, то је ред матрице $-E$ два.

- случај $\chi_E = X - 1$,

$$\{E\}.$$

Ред матрице E је 1.

2.2.2 Централизатори елемената групе G

Нека је $M \in G$. Централизатор елемента M је:

$$C(M) = \{A \in G : PA = AP\} \wedge |C(M)| = |G|/|\mathcal{C}(M)|.$$

- случај $M \in \mathcal{C}_{-1,1}$:

$$|C(M)| = |G|/|\mathcal{C}(M)| = 48/8 = 6.$$

Како је M реда 3 и како $M, -E \in C(M)$, то је $C(M) = \langle M, -E \rangle$, циклична група реда шест генерисана са $-M$, тј.:

$$C(M) = \langle -M \rangle.$$

- случај $M \in \mathcal{C}_{0,1}$:

$$|C(M)| = |G|/|\mathcal{C}(M)| = 48/6 = 8.$$

Како је M реда 4 и $\langle M \rangle = \{E, -E, M, -M\}$, то $\langle M \rangle \subseteq C(M)$.
Приметимо, $(M - E)M = M(M - E)$, одакле је $M - E \in C(M)$.
Нека је $X^2 + aX + b$ карактеристични полином за $M - E$. Тада:

$$(M^2 - 2M + E) + a(M - E) + bE = M^2 + (a - 2)M + (1 + b - a)E = 0.$$

Пошто $M \in \mathcal{C}_{0,1}$, то је $M^2 + E = 0$ одакле следи да је $a = -1$ и $b = -1$. Карактеристични полином за $M - E$ је $X^2 - X - 1$.
Из $\det(M - E) = -1$ и $\mathrm{tr}(M - E) = 1$ имамо да $M - E \in \mathcal{C}_{1,-1}$, те је ред матрице $M - E$ једнак осам. Тада,

$$C(M) = \langle M - E \rangle.$$

- случај $M \in \mathcal{C}_{1,1}$:

$$|C(M)| = |G|/|\mathcal{C}(M)| = 48/8 = 6.$$

Како је M реда 6, то је:

$$C(M) = \langle M \rangle.$$

- случај $M \in \mathcal{C}_{-1,-1}$:

$$|C(M)| = |G|/|\mathcal{C}(M)| = 48/6 = 8.$$

Како је M реда 8, то је:

$$C(M) = \langle M \rangle.$$

- случај $M \in \mathcal{C}_{0,-1}$:

$$|C(M)| = |G|/|\mathcal{C}(M)| = 48/12 = 4.$$

Како је M реда 2 и како $M, -E \in C(M)$, то је $\langle M, -E \rangle$ циклична група реда 4. Тада,

$$C(M) = \langle M, -E \rangle.$$

- случај $M \in \mathcal{C}_{1,-1}$:

$$|C(M)| = |G|/|\mathcal{C}(M)| = 48/6 = 8.$$

Како је M реда 8, то је:

$$C(M) = \langle M \rangle.$$

- случај $M = -E$:

$$|C(-E)| = |G|/|\mathcal{C}(-E)| = 48/1 = 48.$$

Тада,

$$C(-E) = G.$$

- случај $M = E$:

$$|C(E)| = |G|/|\mathcal{C}(E)| = 48/1 = 48.$$

Тада,

$$C(E) = G.$$

Класе конј. $\mathcal{C}$	$\lvert\mathcal{C}\rvert$	Ред $M \in \mathcal{C}$	Центр. $C(M)$	$\lvert C(M)\rvert$
$\{E\}$	1	1	G	48
$\{-E\}$	1	2	G	48
$\mathcal{C}_{0,-1}$	12	2	$\langle M, -E\rangle$	4
$\mathcal{C}_{-1,1}$	8	3	$\langle -M\rangle$	6
$\mathcal{C}_{0,1}$	6	4	$\langle M - E\rangle$	8
$\mathcal{C}_{1,1}$	8	6	$\langle M\rangle$	6
$\mathcal{C}_{-1,-1}$	6	8	$\langle M\rangle$	8
$\mathcal{C}_{1,-1}$	6	8	$\langle M\rangle$	8

2.2.3 Подгрупе групе G и њихови нормализатори

Нека је W подгрупа групе G. Нормализатор од W у G је:

$$N_G(W) = \{A \in G : AW = WA\}.$$

Аналогно, нормализатор од W у H је:

$$N_G(H) = \{A \in H : AW = WA\}.$$

Број подгрупа конјугованих са подгрупом W је $|G|/|N_G(W)|$. Специјално, ако је W подргрупа од G, тада или $W \subseteq H$, или су елементи из W равномерно распоређени у H и $G \setminus H$.

Нетривијалне подгрупе групе G су:

- **Подгрупе реда два.**

Подгрупе реда два су генерисане елементима реда 2. Постоји 13 подгрупа:

$$\langle -E\rangle \text{ и подгрупе облика } \langle D\rangle, \text{ за } D \in \mathcal{C}_{0,-1}.$$

Нормализатор од $\langle -E\rangle$ је цела група G, одакле следи да је:

$$\langle -E\rangle \lhd G.$$

Посматрајмо нормализатор подгрупе $\langle D\rangle$:

$$N_G(\langle D\rangle) = C(D) = \langle D, -E\rangle.$$

Број конјугованих подгрупа подгрупе $\langle D\rangle$ је:

$$|G|/|N_G(\langle D\rangle)| = 48/4 = 12.$$

Како су $D \in \mathcal{C}_{0,-1}$ међусобно конјуговане, то су и подгрупе, њима генерисане, конјуговане.

- **Подгрупе реда три.**

Подгрупе реда три су цикличне подгрупе генерисане елементима реда 3. Постоје 4 подгрупе:

$$\langle T_1\rangle, \quad \langle T_2\rangle, \quad \langle T_3\rangle \quad \text{и} \quad \langle T_4\rangle.$$

Елементи подгрупе $\langle T_1\rangle$ су E, T_1 и $T_1^2 = T_5$.

$$N_G(\langle T_1\rangle) = C(\langle T_1\rangle) \cup \{A \in G : AT_1A^{-1} = T_5\}.$$

Тражимо $A \in G$ такве да важи $AT_1 = T_5A$, тј.

$$\begin{bmatrix} b & -a-b \\ d & -c-d \end{bmatrix} = \begin{bmatrix} c-a & d-b \\ -a & -b \end{bmatrix}.$$

Елементи који задовољавају тражену једнакост су D_1, D_4 и D_9. Стога,

$$N_G(\langle T_1\rangle) = \langle -T_1\rangle \cup \{D_1, -D_1, D_4, -D_4, D_9, -D_9\}.$$

Приметимо да је $T_1D_1 = -D_9$ и $T_1^2D_1 = D_4$.
Тада нормализатор подгрупе $\langle T_1\rangle$ можемо записати као: $N_G(\langle T_1\rangle)$ скуп:

$$\{E, -E, T_1, -T_1, T_1^2, -T_1^2, D_1, -D_1, T_1D_1, -T_1D_1, T_1^2D_1, -T_1^2D_1\},$$

$$N_G(\langle T_1\rangle) = \langle -T_1, D_1\rangle.$$

Аналогно,

$$N_G(\langle T_2\rangle) = \langle -T_2\rangle \cup \{D_2, -D_2, D_3, -D_3, D_4, -D_4\} = \langle -T_2, D_2\rangle.$$

$$N_G(\langle T_3\rangle) = \langle -T_3\rangle \cup \{D_1, -D_1, D_3, -D_3, D_{10}, -D_{10}\} = \langle -T_3, D_1\rangle.$$

$$N_G(\langle T_4\rangle) = \langle -T_4\rangle \cup \{D_2, -D_2, D_9, -D_9, D_{10}, -D_{10}\} = \langle -T_4, D_2\rangle.$$

Број конјугованих подгрупа подгрупе $\langle T\rangle$ је

$$|G|/|N_G(\langle T\rangle)| = 48/12 = 4.$$

Како су T_1, T_2, T_3 и T_4 конјуговане, то су и подгрупе, њима генерисане, конјуговане.

- **Подгрупе реда четири.**

  - **Цикличне подгрупе реда четири.**

    Цикличне подгрупе реда четири генерисане су елементима реда 4. Постоје 3 подгрупе:

$$\langle Q_1\rangle, \quad \langle Q_2\rangle \quad \text{и} \quad \langle Q_3\rangle.$$

Елементи подгрупе $\langle Q_1\rangle$ су E, Q_1, $Q_1^2 = -E$ и $Q_1^3 = -Q_1$.

$$N_G(\langle Q_1\rangle) = C(\langle Q_1\rangle) \cup \{A \in G : AQ_1A^{-1} = -Q_1\}.$$

Тражимо $A \in G$ такве да важи $AQ_1 = -Q_1A$, тј.

$$\begin{bmatrix} b & -a \\ d & -c \end{bmatrix} = \begin{bmatrix} c & d \\ -a & -b \end{bmatrix}.$$

Елементи који задовољавају тражену једнакост су D_1, D_2, D_5, D_6, Q_2, Q_3, Q_5 и Q_6.

$$N_G(\langle Q_1\rangle) = \langle Q_1 - E\rangle \cup \{D_1, D_2, -D_1, -D_2, Q_2, Q_3, -Q_2, -Q_3\}.$$

Приметимо,

$$\begin{gathered} (Q_1-E)D_1 = -Q_2, \quad (Q_1-E)^2D_1 = -D_2, \quad (Q_1-E)^3D_1 = Q_3, \\ (Q_1-E)^4D_1 = -D_1, \quad (Q_1-E)^5D_1 = Q_2, \quad (Q_1-E)^6D_1 = D_2, \\ (Q_1-E)^7D_1 = -Q_3. \end{gathered}$$

Коначно,

$$N_G(\langle Q_1\rangle) = \langle Q_1 - E, D_1\rangle.$$

Аналогно се доказује:

$$N_G(\langle Q_2\rangle) = \langle Q_2 - E, D_3\rangle, \quad N_G(\langle Q_3\rangle) = \langle Q_3 - E, D_4\rangle.$$

Број конјугованих подгрупа подгрупе $\langle Q\rangle$ је:

$$|G|/|N_G(\langle Q\rangle)| = 48/16 = 3.$$

Како су Q_1, Q_2 и Q_3 конјуговане, то су и подгрупе, њима генерисане, конјуговане.

•• Нециклични подгрупе реда четири.

Нецикличне подгрупе реда четири су изоморфне Клајновој групи и облика су $\{E, -E, D, -D\}$, где $D \in \mathcal{C}_{0,-1}$. Постоји 6 подргупа:

$$\begin{gathered} \langle -E, D_1\rangle, \quad \langle -E, D_2\rangle, \quad \langle -E, D_2\rangle, \\ \langle -E, D_4\rangle, \quad \langle -E, D_9\rangle, \quad \langle -E, D_{10}\rangle. \end{gathered}$$

$$N_G(\langle -E, D_1\rangle) = C(\langle D_1\rangle) \cup \{A \in G : AD_1A^{-1} = -D_1\}.$$

Тражимо $A \in G$ такве да важи $AD_1 = -D_1A$, тј.

$$\begin{bmatrix} b & a \\ d & c \end{bmatrix} = \begin{bmatrix} -c & -d \\ -a & -b \end{bmatrix}.$$

Елементи који задовољавају тражену једнакост су D_2, $-D_2$, Q_1 и $-Q_1$.

$$N_G(\langle -E, D_1\rangle) = \langle D_1\rangle \cup \{D_2, -D_2, Q_1, -Q_1\}.$$

Приметимо, $D_1Q_1 = D_2$. Коначно,

$$N_G(\langle -E, D_1\rangle) = \langle D_1, Q_1\rangle.$$

Аналогно,

$$N_G(\langle -E, D_2\rangle) = \langle D_2, Q_1\rangle,\quad N_G(\langle -E, D_3\rangle) = \langle D_3, Q_2\rangle,$$

$$N_G(\langle -E, D_4\rangle) = \langle D_4, Q_3\rangle,\quad N_G(\langle -E, D_9\rangle) = \langle D_9, Q_2\rangle,$$
$$N_G(\langle -E, D_{10}\rangle) = \langle D_{10}, Q_3\rangle.$$

Број конјугованих подгрупа подгрупе $\langle -E_2, D\rangle$ је:

$$|G|/|N_G(\langle -E, D\rangle)| = 48/8 = 6.$$

Како су D-ови међусобно конјуговани, то су и подгрупе, њима генерисане, конјуговане.

- **Подгрупе реда шест.**

•• Цикличне подгрупе реда шест.

Цикличне подгрупе реда шест су генерисане елементима реда 6. Постоје четири подгрупе:

$$\langle S_1\rangle,\quad \langle S_2\rangle,\quad \langle S_3\rangle \quad \text{и} \quad \langle S_4\rangle.$$

Приметимо да је $S^2 = T$ реда 3. Тада је $\langle S^2\rangle$ подгрупа групе $\langle S\rangle$. Специјално, $N_G(\langle S\rangle) \subseteq N_G(\langle S^2\rangle)$.
Како су генератори подгрупа конјуговани, то је:

$$|N_G(\langle S\rangle)| = 48/4 = 12.$$

Из $|N_G(\langle S^2\rangle)| = 12$ следи да је:

$$N_G(\langle S\rangle) = N_G(\langle S^2\rangle).$$

•• Нецикличне подгрупе реда шест.

Нецикличне подгрупе реда шест су облика $\langle T, D\rangle$, где је $\langle T\rangle$ подгрупа реда 3 и D елемент реда 2 тд. $DTD^{-1} = T^{-1}$.
Уочимо да $D \in N_G(\langle T\rangle)$.
Посматрајмо T_1. Услов $AT_1A^{-1} = T_1^{-1} = T_5$ задовољавају елементи D_1, D_4 и D_9.
Приметимо да важи $T_1D_1 = -D_9$ и $T_1^2D_1 = D_4$.
Аналогно, $T_1(-D_1) = D_9$ и $T_1^2(-D_1) = -D_4$.
Тада су:

$$\langle T_1, D_1\rangle = \langle T_1\rangle \cup \{D_1,\ T_1D_1 = D_{11},\ T_1^2D_1 = D_4\},$$

$$\langle T_1, -D_1\rangle = \langle T_1\rangle \cup \{D_5,\ T_1(-D_1) = D_{11},\ T_1^2(-D_1) = D_8\}$$

подгрупе реда 6 које одговарају $\langle T_1\rangle$. Сличним разматрањем добијамо:

$$\langle T_2, D_2\rangle = \langle T_2\rangle \cup \{D_2, D_3, D_4\},\ \langle T_2, -D_2\rangle = \langle T_2\rangle \cup \{D_6, D_7, D_8\},$$

$$\langle T_3, D_1\rangle = \langle T_3\rangle \cup \{D_1, D_7, D_{10}\},\ \langle T_3, -D_1\rangle = \langle T_3\rangle \cup \{D_5, D_3, D_{12}\},$$

$$\langle T_4, D_2\rangle = \langle T_4\rangle \cup \{D_2, D_9, D_{10}\},\ \langle T_4, -D_2\rangle = \langle T_4\rangle \cup \{D_6, D_{11}, D_{12}\}.$$

Како је $\langle T\rangle$ подгрупа групе $\langle T, D\rangle$, то $N_G(\langle T, D\rangle) \subseteq N_G(\langle T\rangle)$.
Из $|N_G(\langle T\rangle)|/|\langle T, D\rangle| = 12/6 = 2$ следи да је:

$$\langle T, D\rangle \triangleleft N_G(\langle T\rangle).$$

Тада је $N_G(\langle T, D\rangle) \supseteq N_G(\langle T\rangle)$.
Коначно,

$$N_G(\langle T, D\rangle) = N_G(\langle T\rangle).$$

Број конјугованих подгрупа подгрупе $\langle T, D\rangle$ је:

$$|G|/|N_G(\langle T, D\rangle)| = 48/12 = 4.$$

Како имамо 8 нецикличних подгрупа реда шест, то постоје 2 класе конјугације такве да свака класа садржи 4 подгрупе.

Посматрајмо подгрупе $\langle T, D\rangle$ и $\langle T, -D\rangle$. Тражимо $M \in G$ такво да $M^{-1}\langle T, D\rangle M = \langle T, -D\rangle$. Како је $\langle T\rangle$ јединствена подгрупа реда 3 за групе $\langle T, D\rangle$ и $\langle T, -D\rangle$, тада

$$M \in N_G(\langle T\rangle) = N_G(\langle T, D\rangle).$$

Стога, $M^{-1}\langle T, D\rangle M = \langle T, D\rangle = \langle T, -D\rangle$, што је контрадикција.

Како су D_1 и $-D_1$ конјуговане, то је $\langle T_1, D_1\rangle$ конјугована са најмање једном од подгрупа $\langle T_1, -D_1\rangle$ и $\langle T_3, D_1\rangle$. Пошто $\langle T_1, D_1\rangle$ и $\langle T_1, -D_1\rangle$ нису конјуговане, то су подгрупе $\langle T_1, D_1\rangle$ и $\langle T_3, D_1\rangle$ конјуговане.

Како су T_1 и T_2 конјуговане, то је $\langle T_1, D_1\rangle$ конјугована са најмање једном од подгрупа $\langle T_2, D_2\rangle$ и $\langle T_2, -D_2\rangle$. Нађимо $P \in G$ такво да важи $PT_1P^{-1} = T_2$, тј.

$$PT_1 = \begin{bmatrix} b & -a-b \\ d & -c-d \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ c & d \end{bmatrix} = T_2P.$$

Елементи који задовољавају тражени услов су F_2, F_6, B_4, T_4, D_{10} и D_{12}.
Приметимо да важи $F_2D_1F_2^{-1} = D_8 \in \langle T_2, -D_2\rangle$, то су $\langle T_1, D_1\rangle$ и $\langle T_2, -D_2\rangle$ конјуговане.

Пошто су D_2 и $-D_2$ конјуговане, то је $\langle T_4, D_2\rangle$ конјугована са $\langle T_2, -D_2\rangle$.

Коначно, класе конјугације су:

$$\{\langle T_1, D_1\rangle, \langle T_2, -D_2\rangle, \langle T_3, -D_1\rangle, \langle T_4, D_2\rangle\},$$

$$\{\langle T_1, -D_1\rangle, \langle T_2, D_2\rangle, \langle T_3, D_1\rangle, \langle T_4, -D_2\rangle\}.$$

- **Подгрупе реда дванаест.**

Нека је Δ подгрупа реда $12 = 2^2 \times 3$. Тада је $\Delta \subseteq H = SL(2,3)$ или су елементи равномерно распоређени у H и у $G\backslash H$.

•• **случај $\Delta \subseteq H = SL(2,3)$.**

Како је $|H|/|\Delta| = 24/12 = 2$, то је $\Delta \triangleleft H$, тј.

$$(\forall h \in H)(\forall \delta \in \Delta)\ \ h\delta h^{-1} \in \Delta.$$

Како Δ садржи једну 3-Силовљеву подгрупу, то су и елементи те подгрупе уједно и елементи подгрупе Δ. Приметимо да су елементи из 3-Силовљеве подгрупе конјуговани само са самим собом, јер елеметни реда 2 нису у H.

Осталих 9 елемената се налазе у у 2-Силовљевој подгрупи. Пошто су сви конјуговани са H, то је 2-Силовљева подгрупа нормална у H.

Постоји само једна 2-Силовљева група генерисана елементом Q, реда 4. Она је циклична и важи $|N_H(Q)| = 8$, што је у контрадицкији са $|N_H(Q)| = |H| = 12$. Коначно, не постоји подгрупа реда 12 садржана у H.

•• **случај када су елементи равномерно распоређени у H и у $G\backslash H$.**

Нека је $\Delta_H = \Delta \cap H$ циклична подгрупа групе H реда 6. Тада је $|N_G(\Delta_H)| = 12$.
Како је $|\Delta|/|\Delta_H| = 12/6 = 2$, то је $\Delta_H \triangleleft \Delta$ и $\Delta \subseteq N_G(\Delta_H)$. Стога,

$$N_G(\Delta_H) = \Delta.$$

Како је Δ_H циклична група реда 6, то је $N_G(\Delta_H) = N_G(\langle T\rangle)$, где је $\langle T\rangle$ 3-Силовљева подгрупа групе Δ_H.
Коначно, постоје 4 подгрупе реда дванаест облика:

$\langle -T, D\rangle$, где је T реда 3, D реда 2 и $TD = DT^{-1}$ и $(-T)D = D(-T)^{-1}$.

Тражене подгрупе су:

$$\langle -T_1, D_1\rangle, \quad \langle -T_2, D_2\rangle,$$
$$\langle -T_3, D_1\rangle, \quad \langle -T_4, D_2\rangle.$$

Група Δ је изоморфна групи D_6.

Пошто је $\Delta_H \subseteq \Delta$, тада $N_G(\Delta) \subseteq N_G(\Delta_H) = \Delta$. Стога, $N_G(\Delta) = \Delta$.
Број конјугованих подгрупа подгрупе Δ је:

$$|G|/|N_G(\Delta)| = 48/12 = 4.$$

те су све подргупе реда 12 конјуговане.

• **Подгрупе реда двадесет четири.**

Нека је L подгрупа реда 24. Тада је $L \subseteq H = SL(2,3)$ или су елементи равномерно распоређени у H и у $G\backslash H$.

•• **случај $L \subseteq H = SL(2,3)$.**

Како је $|L| = 12 = |H|$, то је $L = H = SL(2,3)$.

•• **случај када су елементи равномерно распоређени у H и у $G \backslash H$.**

Нека је $L_H = L \cap H$ и $|L_H| = 12$. Како не постоји подгрупа реда 12 групе H, то не постоји подгрупа L реда 24 таква да су елементи су равномерно распоређени у H и у $G \backslash H$.

• **Подгрупе реда шеснаест.**

Нека је K подгрупа реда $16 = 2^4$. Како је $|G| = 2^4 \times 3$, то је K 2-Силовљева подгрупа групе G. По Силовљевој теореми, број подгрупа реда 16 је 1 или 3.

Уколико постоји тачно једна подгрупа реда 16, тада она садржи све елементе чији ред дели 8. Како у G/H постоји 24 елемента који су реда 2 или 8, то је у контрадикцији са претпоставком да постоји тачно једна подгрупа. Стога, постоје 3 подгрупе реда шеснаест.

Претпоставимо да је K' једна од њих. Пошто 16 не дели 24, то K' садржи бар један елемент из H. Стога, 8 елемената су у $K' \cap H$, а 8 ван H. Тада је $K' \cap H$ подгрупа реда 8, и у њој су елементи чији ред дели 8. Приметимо да су то елементи из класа $\{E\}$, $\{-E\}$ и $\mathcal{C}_{0,1}$. Тада $K' \cap H$ не зависи од избора подгрупе K'. Те елементе означимо са K.

$$K = \{E,\ -E,\ Q_1,\ Q_2,\ Q_3,\ -Q_1,\ -Q_2,\ -Q_3\}.$$

Како је $H \triangleleft G$, то је конјугација подгрупе од H такође подгрупа у H. Како K' има јединствену подгрупу реда 8, то $K \triangleleft G$.
Бар једна 2-Силовљева група садржи елемент реда 8. Нека је K' таква. Како циклична група садржи 4 елемента реда 8, то је преосталих 4 елемента реда 2. Пошто су 2-Силовљеве подгрупе конјуговане, то је:

$$|N_G(K')| = |G|/3 = 48/3 = 16 = |K'|.$$

И коначно,

$$N_G(K') = K'.$$

Како су подгрупе реда 16 генерисане са K и елементом реда 8, то су оне облика:

$$\langle K, B_1\rangle, \quad \langle K, B_2\rangle, \quad \text{и} \quad \langle K, B_3\rangle.$$

• **Подгрупе реда осам.**

Нека је I подгрупа реда 8. Тада је $I \subseteq H = SL(2,3)$ или су елементи равномерно распоређени у H и у $G \backslash H$.

•• **случај $I \subseteq H = SL(2,3)$.**

Уколико је $I \subseteq H$, по претходном разлагању

$$I = K.$$

Како K има елементе реда 2 и нема елемент реда 8, то је:

$$I \cong \mathbb{H}_8.$$

•• **случај када су елементи равномерно распоређени у H и у $G \backslash H$.**

••• **случај када $I \cap (G \setminus H)$ садржи елемент реда 8.**

Како I садржи елемент реда 8, то је I циклична и постоји подгрупа K' реда 16 таква да I јединa подгрупа од K'. Постоје 3 подгрупе реда 8:

$$\langle B_1 \rangle, \quad \langle B_3 \rangle, \quad \text{и} \quad \langle B_3 \rangle.$$

Пошто су B_1, B_2 и B_3 конјуговане, то су и подгрупе њима генерисане конјуговане и

$$|N_G(I)| = |G|/3 = 48/3 = 16 = |K'|,$$

одакле закључујемо:

$$N_G(I) = K'.$$

••• **случај када $I \cap (G \setminus H)$ не садржи елемент реда 8.**

I садржи 4 елемента реда 2 из подгрупе K. Специјално, $I \cap H$ је подгрупа, реда 4, од K, и једини елемент реда два у K је $-E$. Стога, I садржи $-E$.
Нека $D \in I \cap (G \setminus H)$. Како је:

$$|I|/|\langle -E, D \rangle| = 8/4 = 2,$$

то је подгрупа $\langle -E, D \rangle$ је нормалана у I и

$$N_G(\langle -E, D \rangle) \supseteq I.$$

Како је $|N_G(\langle -E, D \rangle)| = 8$, то је $N_G(\langle -E, D \rangle) = I$.
Приметимо, постоји $Q \in G$такво да

$$N_G(\langle -E, D \rangle) = \langle Q, D \rangle = I.$$

И још, $DQD^{-1} = Q^{-1} = -Q$. Коначно, $I \cong \mathbf{D}_4$. Тражене подгрупе су:

$$\langle D_1, Q_1 \rangle, \quad \langle D_3, Q_2 \rangle, \quad \text{и} \quad \langle D_4, Q_3 \rangle.$$

$|N_G(I)| = |G|/3 = 48/3 = 16 = |K'| \Rightarrow N_G(I) = K'$, где је K' подгрупа чија је једина подгрупа реда осам I.

Лако је уочити да је центар групе G подгрупа $\langle -E \rangle$, па је:

$$|PGL(2,3)| = \frac{|G|}{|Z|} = \frac{48}{2} = 24 \quad \text{и} \quad |PSL(2,3)| = \frac{|H|}{|Z|} = \frac{24}{2} = 12.$$

Може се доказати и да је:

$$PGL(2,3) \cong \sigma_4 \text{ и } PSL(2,3) \cong \mathfrak{U}_4.$$

Подгр.	Ред подр.	Тип	Бр. кл. конј.	Норм.	Ред норм.
$\langle E \rangle$	1	циклична	1	G	48
$\langle -E \rangle$	2	циклична	1	G	48
$\langle D \rangle$	2	циклична	12	$\langle -E, D \rangle$	4
$\langle T \rangle$	3	циклична	4	$\langle -T, D \rangle$	12
$\langle Q \rangle$	4	циклична	3	$\langle Q - E, Q' \rangle$	16
$\langle -E, D \rangle$	4	$\mathbf{V}_4$	6	$\langle D, Q \rangle$	8
$\langle -T \rangle$	6	циклична	4	$\langle -T, D \rangle$	12
$\langle T, D \rangle$	6	σ_3	4	$\langle -T, D \rangle$	12
$\langle T, D \rangle$	6	σ_3	4	$\langle -T, D \rangle$	12
K	8	$\mathbb{H}_8$	1	G	48
$\langle B \rangle$	8	циклична	3	$\langle K, B \rangle$	16
$\langle Q, D \rangle$	8	$\mathbf{D}_4$	3	$\langle K, B \rangle$	16
$\langle -T, D \rangle$	12	$\mathbf{D}_6$	4	$\langle -T, D \rangle$	12
$\langle K, B \rangle$	16	$\mathbb{H}_8 \times \mathbb{Z}_2$	3	$\langle K, B \rangle$	16
H	24	$SL(2, \mathbb{Z}_3)$	1	G	48
G	48	$GL(2, \mathbb{Z}_3)$	1	G	48
			Укупно: 55		

2.3 »Ботаника« групе $G = GL(3,2)$

Нека је $\mathbf{V}$ векторски простор над пољем $\mathbb{Z}_2$ и $e = [e_1, e_2, e_3]$ база простора $\mathbf{V}$. Посматрајмо све $\mathbb{Z}_2$-аутоморфизме простора $\mathbf{V}$ који су одређени инверзибилним матрицама реда три, над пољем $\mathbb{Z}_2$. Приметимо,

$$GL(3,2) = \{M : \det(M) \neq 0\} = \{M : \det(M) = 1\} = SL(3,2).$$

2.3.1 Ред и класе конјугације групе G

Применом Теореме 8. добијамо:

$$|G| = (2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 168 = 2^3 \times 3 \times 7.$$

Нека је $M \in G$ и M није јединична. Карактеристични полином матрице M је:

$$\chi_M = X^3 - \operatorname{tr}(M)X^2 + aX + \det(M).$$

Специјално, кажемо да је M реда n ако M поништава полином $X^n - 1$. По Теореми 1. сличне матрице имају исти траг и исту детерминанту, па су карактеристични полиноми и класе конјугације:

- случај $\chi_1 = X^3 + X^2 + X + 1$,

$$\mathcal{C}_1 = \{M \in G \backslash \{E\} : \chi_1(M) = 0\}.$$

Како $\chi_1 = (X^2+1)(X+1) = (X+1)^3$ дели $(X+1)^4 = X^4 - 1$, то је ред матрице $M \in \mathcal{C}_1$ четири. Представник класе конјугације је:

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Класа садржи 42 елемента.

- случај $\chi_2 = X^3 + X^2 + 1$,

$$\mathcal{C}_2 = \{M \in G : \chi_2(M) = 0\}.$$

Како $\chi_2 = X^3 + X^2 + 1$ дели $(X^3 + X^2 + 1)^2(X+1) = X^7 - 1$, то је ред матрице $M \in \mathcal{C}_2$ седам. Представник класе конјугације је:

$$B = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Класа садржи 24 елемента.

- случај $\chi_3 = X^3 + X + 1$,

$$\mathcal{C}_3 = \{M \in G : \chi_3(M) = 0\}.$$

Како $\chi_3 = X^3 + X + 1$ дели $(X^3 + X + 1)^2(X+1) = X^7 - 1$, то је ред матрице $M \in \mathcal{C}_3$ седам. Представник класе конјугације је:

$$C = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Класа садржи 24 елемента.

- случај $\chi_4 = X^2 + X + 1$,

$$\mathcal{C}_4 = \{M \in G : \chi_4(M) = 0\}.$$

Како $\chi_4 = X^2 + X + 1$ дели $(X^2 + X + 1)(X+1) = X^3 - 1$, то је ред матрице $M \in \mathcal{C}_4$ три. Представник класе конјугације је:

$$D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

Класа садржи 56 елемената.

- случај $\chi_5 = X^2 + 1$,

$$\mathcal{C}_5 = \{M \in G \backslash \{E\} : \chi_5(M) = 0\}.$$

Ред матрице $M \in \mathcal{C}_5$ је два. Представник класе конјугације је:

$$F = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Класа садржи 21 елемент.

- случај $\chi_5 = X + 1$,

$$\mathcal{C}_6 = \{E\}.$$

Ред матрице је један. Елемент класе конјугације је:

$$E = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

2.3.2 Централизатори елемената групе G

Нека је $M \in G$. Централизатор елемента M је:

$$C(M) = \{N \in G : PN = NP\}, \quad |C(M)| = |G|/|\mathcal{C}(M)|.$$

- случај $M \in \mathcal{C}_1$:

$$|C(M)| = |G|/|\mathcal{C}(M)| = 168/42 = 4.$$

Како је M реда 4, то је

$$C(M) = \langle M \rangle.$$

- случај $M \in \mathcal{C}_2$:

$$|C(M)| = |G|/|\mathcal{C}(M)| = 168/24 = 7.$$

Како је M реда 7, то је

$$C(M) = \langle M \rangle.$$

- случај $M \in \mathcal{C}_3$:

$$|C(M)| = |G|/|\mathcal{C}(M)| = 168/24 = 7.$$

Како је M реда 7, то је

$$C(M) = \langle M \rangle.$$

- случај $M \in \mathcal{C}_4$:

$$|C(M)| = |G|/|\mathcal{C}(M)| = 168/56 = 3.$$

Како је M реда 3, то је

$$C(M) = \langle M \rangle.$$

- случај $M \in \mathcal{C}_5$:
$$|C(M)| = |G|/|\mathcal{C}(M)| = 168/21 = 8.$$

  Тражећи елементе Q, који задовољавају $QM = MQ$, добијамо:

$$C(M) = \{E,\ N,\ N^2,\ N^3,\ L,\ NL,\ N^2L,\ N^3L\},$$

  где је $N \in \mathcal{C}_1$ такав да је $N^2 = M$ и $L \in \mathcal{C}_5 \backslash \{M\}$ тд. $LM = ML$. Коначно,
$$C(M) = \langle M, L\rangle.$$

- случај $M \in \mathcal{C}_6$:
$$|C(M)| = |G|/|\mathcal{C}(M)| = 168/1 = 168.$$

  Коначно,
$$C(M) = G.$$

Класе конј. $\mathcal{C}$	$\lvert\mathcal{C}\rvert$	Ред $M \in \mathcal{C}$	Центр. $C(M)$	$\lvert C(M)\rvert$
$\{E\}$	1	1	G	168
$\mathcal{C}_5$	21	2	$\langle N, L\rangle$	8
$\mathcal{C}_4$	56	3	$\langle M\rangle$	3
$\mathcal{C}_1$	42	4	$\langle M\rangle$	4
$\mathcal{C}_2$	24	7	$\langle M\rangle$	7
$\mathcal{C}_3$	24	7	$\langle M\rangle$	7

2.3.3 Подгрупе групе G и њихови нормализатори

Нека је W подгрупа групе G. Нормализатор од W у G је:

$$N_G(W) = \{P \in G : PW = WP\}.$$

Број подгрупа конјугованих са подгрупом W је $|G|/|N_G(W)|$.

Нетривијалне подгрупе групе G су:

- **Подгрупе реда два.**

  Подгрупе реда два су генерисане елементима реда 2. Постоји 21 подгрупа и облика су:

$$\langle F\rangle,\ \text{за } F \in \mathcal{C}_5.$$

  Нормализатор од $\langle F\rangle$ је централизатор елемента F:

$$N_G(\langle F\rangle) = \langle N, L\rangle,$$

  где је $N \in \mathcal{C}_1$ такав да је $N^2 = F$ и $L \in \mathcal{C}_5 \backslash \{F\}$ такав да је $LF = FL$. Број конјугованих подгрупа подгрупе $\langle F\rangle$ је:

$$|G|/|N_G(\langle F\rangle)| = 168/8 = 21.$$

  Како су $F \in \mathcal{C}_5$ међусобно конјуговане, то су и подгрупе, њима генерисане, конјуговане.

- **Подгрупе реда три.**

Подгрупе реда три су генерисане елементима реда три. Како постоји 56 елемената реда три, то постоји 28 подгрупа реда три и облика су:

$$\langle D\rangle, \text{ за } D \in \mathcal{C}_4.$$

Нормализатор од $\langle D\rangle$ је:

$$N_G(\langle D\rangle) = C(D) \cup \{N \in G : NDN^{-1} = D^2\}.$$

Елементи који задовољавају једнакост $NDN^{-1} = D^2$ су F, DF и D^2F, где је F елемент реда два.
Коначно,

$$N_G(\langle D\rangle) = \langle D, F\rangle.$$

Број конјугованих подгрупа подгрупе $\langle D\rangle$ је:

$$|G|/|N_G(\langle D\rangle)| = 168/6 = 28.$$

Како су $D \in \mathcal{C}_4$ међусобно конјуговане, то су и подгрупе, њима генерисане, конјуговане.

- **Подгрупе реда четири.**

  - **Цикличне подгрупе реда четири.**

Цикличне подгрупе реда четири генерисане су елементима реда 4. Како постоје 42 елемента реда четири, то постоји 21 подгрупа реда четири и облика су:

$$\langle A\rangle, \text{ за } A \in \mathcal{C}_1.$$

Нормализатор од $\langle A\rangle$ је:

$$N_G(\langle A\rangle) = C(A) \cup \{N \in G : NAN^{-1} = A^3\}.$$

Елементи који задовољавају једнакост $NAN^{-1} = A^3$ су елементи F, AF, A^2F и A^3F, где је F елемент реда два.
Коначно,

$$N_G(\langle A\rangle) = \langle A, F\rangle.$$

Број конјугованих подгрупа подгрупе $\langle A\rangle$ је:

$$|G|/|N_G(\langle A\rangle)| = 168/8 = 21.$$

Како су $A \in \mathcal{C}_1$ међусобно конјуговане, то су и подгрупе, њима генерисане, конјуговане.

  - **Нецикличне подгрупе реда четири.**

Нецикличне подгрупе реда четири су изоморфне Клајновој групи и облика су:

$$\langle a, b : a^2 = b^2 = (ab)^2 = 1\rangle.$$

Нека је F елеменат реда 2. Тражимо елементе $N \in \mathcal{C}_5$ који задовољавају $(FN)^2 = E$. Тражени елементи су: F_1', F_1'', F_2' и F_2''. Приметимо да важе следеће једнакости:

$$FF_1' = F_1'',\ FF_1'' = F_1' \text{ и } F_1'F_1'' = F_1''F_1',$$

$$FF_2' = F_2'',\ FF_2'' = F_2' \text{ и } F_2'F_2'' = F_2''F_2'.$$

Произвољној матрици $F \in \mathcal{C}_5$ можемо придружити две нецикличне подгрупе реда четири:

$$\langle E, F, F_1', F_1'' \rangle \text{ и } \langle E, F, F_2', F_2'' \rangle.$$

Коначно, постоји $\frac{21\times 2}{3} = 14$ подгрупа.
Рачунањем добијамо да је $|N_G(\langle E, F, F_1', F_1'' \rangle)| = |N_G(\langle E, F, F_2', F_2'' \rangle)| = 24$, те је:

$$|G|/|N_G(\langle E, F, F_1', F_1'' \rangle)| = |G|/|N_G(\langle E, F, F_2', F_2'' \rangle)| = 168/24 = 7.$$

Како постоји 14 подгрупа и како се у једној класи конјугације налази 7 погрупа реда четири, то постоје две класе конјугације.

- **Подгрупе реда шест.**

Подгрупе реда шест су облика:

$$\langle a, b : a^3 = b^2 = 1 \wedge a^2b = ba \rangle.$$

Нека је D елеменат реда 3. Тражимо елементе $N \in \mathcal{C}_5$ који задовољавају $D^2N = ND$. Тражени елементи су: F, DF и D^2F.
Произвољној матрици $D \in \mathcal{C}_4$ можемо придружити тачно једну подгрупу реда шест, те постоји 28 подгрупа и облика су:

$$\langle D, F \rangle, \text{ за } D \in \mathcal{C}_4 \text{ и } F \in \mathcal{C}_5.$$

Како подгрупи $\langle D, F \rangle$, реда шест, одговара тачно једна подгрупа $\langle D \rangle$, реда три, следи да $N_G(\langle D, F \rangle) \subset N_G(\langle D \rangle)$. Пошто је $|N_G(\langle D \rangle)| = 6$ и $\langle D, F \rangle \subset N_G(\langle D, F \rangle)$, то је:

$$|N_G(\langle D, F \rangle)| = 6$$

и

$$N_G(\langle D, F \rangle) = \langle D, F \rangle.$$

Пошто је:

$$|G|/|N_G(\langle D, F \rangle)| = 168/6 = 28,$$

следи да су све подгрупе реда шест међусобно конјуговане.

- **Подгрупе реда седам.**

Подгрупе реда седам су цикличне групе генерисане елементима реда 7.
Како је $|\mathcal{C}_2| = 24$, то постоји $\frac{24}{6} = 4$ подгрупе реда седам и облика су:

$$\langle B \rangle, \text{ за } B \in \mathcal{C}_2.$$

Како је $|\mathcal{C}_3| = 24$, то постоји $\frac{24}{6} = 4$ подгрупе реда седам и облика су:

$$\langle C \rangle, \text{ за } C \in \mathcal{C}_3.$$

Рачунањем добијамо да је $|N_G(\langle B \rangle)| = |N_G(\langle C \rangle)| = 21$.
Број конјугованих подгрупа реда седам је:

$$|G|/|N_G(\langle B \rangle)| = |G|/|N_G(\langle C \rangle)| = 168/21 = 8.$$

Приметимо, све подгрупе реда седам су међусобно конјуговане.

- **Подгрупе реда осам.**

Подгрупе реда осам су облика:

$$\langle a, b : a^4 = b^2 = 1 \land a^3 b = ba \rangle.$$

Нека је A елеменат реда 4. Тражимо елементе $N \in \mathcal{C}_5$ који задовољавају $A^3 N = NA$. Тражени елементи су: F, AF, AF^2 и $A^3 F$.
Произвољној матрици $A \in \mathcal{C}_1$ можемо придружити тачно једну подгрупу реда осам, те постоји 21 подгрупа и облика су:

$$\langle A, F \rangle, \text{ за } A \in \mathcal{C}_1 \text{ и } F \in \mathcal{C}_5.$$

Како подгрупи $\langle A, F \rangle$, реда осам, одговара тачно једна подгрупа $\langle A \rangle$, реда четири, следи да $N_G(\langle A, F \rangle) \subset N_G(\langle A \rangle)$. Пошто је $|N_G(\langle A \rangle)| = 8$ и $\langle A, F \rangle \subset N_G(\langle A, F \rangle)$, то је:

$$|N_G(\langle A, F \rangle)| = 8,$$

те је:

$$N_G(\langle A, F \rangle) = \langle A, F \rangle.$$

Пошто је

$$|G|/|N_G(\langle A, F \rangle)| = 168/8 = 21,$$

следи да су све подгрупе реда осам међусобно конјуговане.

Може се доказати да две нецикличне подгрупе реда четири, садржане у подгрупи реда осам, нису конјуговане.

- **Подгрупе реда дванаест.**

Подгрупе реда дванаест су облика:

$$\langle a, b, c : a^2 = b^2 = c^3 = 1 \land ab = ba \land ca = bc \land cb = abc \rangle.$$

Посматрајмо нецикличне подгрупе реда четири. Наиме, оне садрже елементе реда два који комутирају. Нека $F', F'' \in \mathcal{C}_5$ комутирају. Тражимо елемент $N \in \mathcal{C}_4$ такав да важи:

$$NF' = F''N \text{ и } NF'' = F'F''N.$$

Приметимо да четири елемента задовољавају тражени услов: D, $F'D$, $F''D$ и $F'F''D$.
Пошто подгрупа реда дванаест садржи један елемент реда 1, три елемента реда 2 и осам реда 3, то свакој нецикличној подгрупи реда четири одговара тачно једна подгрупа реда 12.
Постоји 14 подгрупа реда дванаест и облика су:

$$\langle F', F'', D\rangle, \text{ за } F', F'' \in \mathcal{C}_5 \text{ и } D \in \mathcal{C}_4.$$

Како подгрупи $\langle F', F'', D\rangle$ одговара тачно једна подгрупа $\langle F, F''\rangle$, следи да $N_G(\langle F', F'', D\rangle) \subset N_G(\langle F', F''\rangle)$.
Пошто је $|N_G(\langle F', F''\rangle)| = 24$ и $\langle F', F'', D\rangle \subset N_G(\langle F', F'', D\rangle)$, то је:

$$|N_G(\langle F', F'', D\rangle)| = 24,$$

те је:

$$|G|/|N_G(\langle F', F'', D\rangle)| = 168/24 = 7.$$

Стога, како постоји 14 подгрупа и како се у једној класи конјугације налази 7 погрупа реда дванаест, то постоје две класе конјугације.

- **Подгрупе реда двадесет један.**

Подгрупе реда двадесет један су облика:

$$\langle a, b : a^3 = b^7 = 1 \wedge ab = b^4 a\rangle.$$

Нека је $B \in \mathcal{C}_2$. Тражимо елементе $N \in \mathcal{C}_4$ такве да важи $NB = B^4 N$.
Елементи који задовољавају тражени услов су D, BD, B^2D, B^3D, B^4D, B^5D и B^6D. Коначно, произвољној подгрупи реда седам можемо придружити тачно једну подгрупу реда двадесет један.
Постоје четири подгрупе и облика су:

$$\langle B, D\rangle, \text{ за } B \in \mathcal{C}_2 \text{ и } D \in \mathcal{C}_4.$$

Аналогно, постоје још четири подгрупе:

$$\langle C, D\rangle, \text{ за } C \in \mathcal{C}_3 \text{ и } D \in \mathcal{C}_4.$$

Како подгрупи $\langle B, D\rangle$ одговара тачно једна подгрупа $\langle B\rangle$, реда седам, следи да $N_G(\langle B, D\rangle) \subset N_G(\langle B\rangle)$.
Пошто је $|N_G(\langle B\rangle)| = 21$ и $\langle B, D\rangle \subset N_G(\langle B, D\rangle)$, то је:

$$|N_G(\langle B, D\rangle)| = 21,$$

стога:

$$N_G(\langle B, D\rangle) = \langle B, D\rangle.$$

Аналогно се добија и:

$$|N_G(\langle C, D\rangle)| = 21$$

и

$$N_G(\langle C, D\rangle) = \langle C, D\rangle.$$

Број конјугованих подгрупа реда двадесет један је:

$$|G|/|N_G(\langle B, D\rangle)| = |G|/|N_G(\langle C, D\rangle)| = 168/21 = 8.$$

Приметимо, све подгрупе су међусобно конјуговане.

- **Подгрупе реда двадесет четири.**

  Приметимо да је нормализатор нецикличних подгрупа реда четири и подгрупа реда дванаест група реда двадесет четири.
  Нека су F', F'' и $F'F''$ елементи нецикличне групе реда четири. Како сваком елементу одговарају по две подгрупе, уочимо и преостале подгрупе ових елемената:

  $$\langle F', F_1' \rangle,\ \langle F'', F_1'' \rangle \text{ и } \langle F'F'', F \rangle.$$

  У нормализатору подгрупе $\langle F', F'' \rangle$ се налазе и елементи ове три подгрупе реда четири. Тада постоји и елемент реда три $D \in \mathcal{C}_4$ такав да је:

  $$\langle D, F', F'', F \rangle, \text{ за } D \in \mathcal{C}_4 \text{ и } F', F'', F \in \mathcal{C}_5,$$

  подгрупа реда двадесет четири и уједно нормализатор подргупа $\langle F', F'' \rangle$ и $\langle D, F', F'' \rangle$.
  Пошто се свакој нецикличној подгрупи реда четири на јединствен начин додељује тачно једна подгрупа реда двадесет четири, то постоји 14 подгрупа реда двадесет четири.
  Из $|N_G(\langle D, F', F'', F \rangle)| = 24$, следи да је:

  $$N_G(\langle D, F', F'', F \rangle = \langle D, F', F'', F \rangle.$$

  Број конјугованих подгрупа реда двадесет четири је:

  $$|G|/|N_G(\langle D, F', F'', F \rangle)| = 168/24 = 7.$$

  Како постоји 14 подгрупа и како се у једној класи конјугације налази 7 погрупа реда двадесет четири, то постоје две класе конјугације.

Пошто се у центру групе G налази само елемент E, лако се уочава да је:

$$GL(3, \mathbb{Z}_2) = SL(3, \mathbb{Z}_2) = PGL(3, \mathbb{Z}_2) = PSL(3, \mathbb{Z}_2).$$

По Теореми 7. група $PSL(3, 2)$ је проста, одакле следи да је и група $GL(3, 2)$ проста.
Може се показати следећа:

Теорема 12. *Свака проста група реда 168 је изоморфна групи* $GL(3, \mathbb{Z}_2)$.

Као директна последица претходне теореме се наводи следећа релација:

$$GL(3, \mathbb{Z}_2) \cong PSL(2, \mathbb{Z}_7).$$

Подгр.	Ред п.	Тип	Бр. кл. конј.	Норм.	Ред н.
$\langle E\rangle$	1	циклична	1	G	168
$\langle F\rangle$	2	циклична	21	$\langle N, L\rangle$	8
$\langle D\rangle$	3	циклична	28	$\langle D, F\rangle$	6
$\langle A\rangle$	4	циклична	21	$\langle A, F\rangle$	8
$\langle F_1', F_2'\rangle$	4	$\mathbf{V}_4$	7	$\langle D, F_1', F_2', F\rangle$	24
$\langle F_1'', F_2''\rangle$	4	$\mathbf{V}_4$	7	$\langle D, F_1'', F_2'', F\rangle$	24
$\langle D, F\rangle$	6	$\mathbf{S}_3$	28	$\langle D, F\rangle$	6
$\langle B\rangle$	7	циклична	8	$\langle B, D\rangle$	21
$\langle A, F\rangle$	8	$\mathbf{D}_4$	21	$\langle A, F\rangle$	8
$\langle F_1', F_2', D\rangle$	12	$\mathbf{A}_4$	7	$\langle D, F_1', F_2', F\rangle$	24
$\langle F_1'', F_2'', D\rangle$	12	$\mathbf{A}_4$	7	$\langle D, F_1'', F_2'', F\rangle$	24
$\langle B, D\rangle$	21	$\langle a, b : ab = ba^4\rangle$	8	$\langle B, D\rangle$	21
$\langle D, F_1', F_2', F\rangle$	24	$\mathbf{S}_4$	7	$\langle D, F_1', F_2', F\rangle$	24
$\langle D, F_1'', F_2'', F\rangle$	24	$\mathbf{S}_4$	7	$\langle D, F_1'', F_2'', F\rangle$	24
G	168	$GL(3, \mathbb{Z}_2)$	1	G	168
			Укупно: 179		

Библиографија

[1] GABE CUNNINGHAM, *The General Linear Group*

[2] EYAL Z. GOREN, *Group Theory*, MCGILL University, 2003.

[3] JEAN DIEUDONNÉ, *La Géometrié Des Groupes Classiques*, Springer – VerlacE, Berlin, 1955.

[4] GOJKO KALAJDŽIĆ, *Algebra*, Zavod za udžbenike, Beograd, 2011.

[5] PASCAL ORTIZ, *Exercices D′Algèbre*, Ellipses, Paris

[6] DANIEL PERRIN, *Cours D′Algèbre*, Ellipses, Paris, 1996.

[7] P. PUUSEMP, *Group of Order* 24 *and Their Endomorphism Semigroups*, Journal of Mathematical Sciences, Vol. 144, No.2, 2007.

[8] P. PUUSEMP, *Group of Order Less Than* 32 *and Their Endomorphism Semigroups*, Journal of Nonlinear Mathematical Physics, Vol. 13, 2006.

[9] JOSEPH J. ROTMAN, *An Introduction to the Theory of Groups*, Springer – Verlag, New York, 1995.

[10] $http://groupprops.subwiki.org/wiki/GL(2,3)$

[11] $http://en.wikipedia.org/wiki/List_of_small_groups$

[12] $http://math.ucdenver.edu/\ tvis/Coursework/Fano.pdf$

[13] $http://planetmath.org/exampleofgroupsoforderpq$

[14] $http://www.math.kent.edu/\ soprunova/61051f13/solutions5.pdf$

[15] $http://www.math.niu.edu/\ beachy/aaol/grouptables2.html$

[16] $http://www.math.umn.edu/\ garrett/m/algebra/exercises/s06.pdf$