Глава 2

Симетрична група и крайни матрични групи.

2.1 Симетрична група.

Симетричната група S_n дефинирахме в Глава 1 като групата от всички биекции на множеството $\{1, 2, \ldots, n\}$ в себе относно операцията композиция на изображения. В тази глава ще разгледаме подробно свойствата ѝ.

Дефиниция 2.1.1 ***Цикъл с дължина*** *k наричаме елемент π на S_n, за който съществуват k числа $i_1, i_2, \ldots, i_k$, такива че $\pi(i_\nu) = i_{\nu+1}$ за $\nu = 1, 2, \ldots, k-1$ и $\pi(i_k) = i_1$, а всички останали числа π оставя на място. Бележим за краткост $\pi = (i_1 i_2 \ldots i_k)$.*

Например, цикълът $\pi = (1\ 4\ 2) \in S_7$ в стандартен запис има вида

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 3 & 2 & 5 & 6 & 7 \end{pmatrix}.$$

Числата 3,5,6 и 7 остават неподвижни, а $1 \xrightarrow{\pi} 4 \xrightarrow{\pi} 2 \xrightarrow{\pi} 1$.
Очевидно всеки цикъл с дължина k има k различни на пръв поглед записа:

$$\pi = (i_1 i_2 \ldots i_k) = (i_2 \ldots i_k i_1) = (i_3 \ldots i_1 i_2) = \ldots = (i_k i_1 \ldots i_{k-2} i_{k-1}).$$

Дефиниция 2.1.2 *Два цикъла $\pi = (i_1 i_2 \ldots i_k)$ и $\tau = (j_1 j_2 \ldots j_l)$ наричаме* ***независими****, ако $\{i_1 i_2 \ldots i_k\} \cap \{j_1 j_2 \ldots j_l\} = \emptyset$.*

Например, независими са циклите $(1\ 4\ 2)$ и $(3\ 7)$, докато $(3\ 4\ 2)$ и $(3\ 7)$ не са такива. **Независимите цикли комутират помежду** си докато за два зависими цикли това не е вярно. Наистина $(1\ 4\ 2)(3\ 7) = (3\ 7)(1\ 4\ 2)$, докато

$$(3\ 4\ 2)(3\ 7) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 7 & 2 & 5 & 6 & 4 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 7 & 4 & 2 & 5 & 6 & 3 \end{pmatrix} = (3\ 7)(3\ 4\ 2).$$

Теорема 2.1.3 *Всяка пермутация на S_n се представя като (казва се също: разлага в) произведение на независими цикли. С точност до наредба на циклите това разлагане е единствено.*

Теорема 2.1.4 *Броят N на елементите на S_n, които се представят като произведение на a_1 цикли с дължина 1, a_2 цикли с дължина 2, и т.н. a_n цикли с дължина n, се дава с формулата*

$$N = \frac{n!}{1^{a_1}2^{a_2}\dots n^{a_n}a_1!a_2!\dots a_n!}.$$

Доказателство. Нека $\pi \in S_n$ е с исканата структура, т. е. с точност до наредба разлагането на π в произведение от независими цикли е следното:

$$\pi = \underbrace{(*)\dots(*)}_{a_1}\ \underbrace{(**)\dots(**)}_{a_2}\ \dots\ \underbrace{(*\dots*)\dots(*\dots*)}_{a_n}.$$

Общият брой на горните записи е $n!$ - толкова колкото са пермутациите на числата от 1 до n. Но всеки цикъл с дължина k има k различни записа (циклични премествания). Следователно за всеки цикъл (те са a_k на брой) с дължина k възможните записи за π се групират по k и всяка група представя една и съща субституция. Следователно $n!$ трябва да разделим на $1^{a_1}2^{a_2}\dots n^{a_n}$. Освен това, ако разместим два цикъла с дължина k субституцията π не се променя. Следователно за да получим различните π трябва да разделим $n!$ и на $a_1!a_2!\dots a_n!$.

Пример 2.1.1 Ще илюстрираме горната теорема с групата S_4. Цикловата йструктура е представена в Таблица 2.1. Оставяме на читателя да подреди елементите на S_4 съобразно разлагането им в произведение на независими цикли и да провери верността на числата дадени в таблицата.

циклова структура	брой
$(*)(*)(*)(*)$	$\frac{4!}{1^4 4!} = 1$
$(*)(*)(**)$	$\frac{4!}{1^2 2^1 1! 2!} = 6$
$(**)(**)$	$\frac{4!}{2^2 2!} = 3$
$(*)(***)$	$\frac{4!}{1^1 3^1 1! 1!} = 8$
$(****)$	$\frac{4!}{4^1 1!} = 6$
общо	24

Таблица 2.1: Циклова структура на S_4.

Цикъл с дължина 2 се нарича ***транспозиция***. Всеки цикъл може да се представи като произведение на транспозиции, но това представяне не е еднозначно:

$$(i_1 i_2 \dots i_k) = (i_1 i_k)(i_1 i_{k-1})\cdots(i_1 i_{\nu+1})(i_1 i_\nu)\cdots(i_1 i_2) = (i_k i_{k-1})(i_k i_{k-2})\cdots(i_k i_1).$$

Наистина за дясната страна на първото равенство имаме

$$i_\nu \xrightarrow{(i_1 i_\nu)} i_1 \xrightarrow{(i_1 i_{\nu+1})} i_{\nu+1},\ \text{за } \nu = 2,3,\dots k-1, \qquad i_k \to i_1.$$

Ползвайки записа $(i_k i_1 i_2 \dots i_{k-1})$ получаваме и другото равенство.

Разлагането в произведение от транспозиции не е еднозначно, но както ще покажем по-долу четността на броя на множителите е инвариант.
Нека $f(x_1, x_2, \dots, x_n)$ е полином на променливите $x_1, x_2, \dots x_n$. Всяка пермутация $\sigma \in S_n$ дефинира изображение в пръстена от полиномите на n променливи по правилото

$$\sigma(f) \overset{\text{def}}{=} f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}).$$

В частност, лесно се вижда, че за полинома $\Delta = \prod_{1 \le i < j \le n}(x_i - x_j)$ е в сила $\sigma(\Delta) = \pm\Delta$ за всяка пермутация σ.

Дефиниция 2.1.5 *Нека $\sigma \in S_n$. Ако $\sigma(\Delta) = \Delta$ пермутацията наричаме **четна**. Ако $\sigma(\Delta) = -\Delta$, то σ се нарича **нечетна**.*

От дефиницията веднага следва, че **всяка транспозиция е нечетна пермутация**. Следователно в сила е

Твърдение 2.1.6 *Всяка пермутация $\sigma \in S_n$ може да се представи като произведение на транспозиции, като всяко такова представяне се състои от четен брой транспозиции, ако σ е четна пермутация и от нечетен брой, ако е нечетна пермутация. Броят на четните пермутации в S_n е равен на броя на нечетните пермутации.*

Пример 2.1.2 Следното равенство илюстрира нееднозначността на представянето като произведение от транспозиции: $(1\,2) = (1\,3)(2\,3)(1\,3)$.

Съвкупността от всички четни пермутации е подгрупа на S_n от ред $n!/2$ и се нарича ***алтернативна група***. Означава се с A_n.

Теорема 2.1.7 *Ако $\tau = (a_{11} \dots a_{1r})(a_{21} \dots a_{2s}) \dots (a_{m1} \dots a_{mt}) \in S_n$ и*

$$\sigma = \begin{pmatrix} a_{11} & \dots & a_{1r} & a_{21} & \dots & a_{2s} & \dots & a_{m1} & \dots & a_{mt} \\ b_{11} & \dots & b_{1r} & b_{21} & \dots & b_{2s} & \dots & b_{m1} & \dots & b_{mt} \end{pmatrix},$$

то

$$\sigma\tau\sigma^{-1} = (b_{11} \dots b_{1r})(b_{21} \dots b_{2s}) \dots (b_{m1} \dots b_{mt}).$$

Доказателство.

$$b_{jk} \xrightarrow{\sigma^{-1}} a_{jk} \xrightarrow{\tau} a_{j\,k+1} \xrightarrow{\sigma} b_{j\,k+1}$$

Следствие 2.1.8 *Две пермутации са спрегнати тогава и само тогава, когато имат една и съща циклова структура.*

Твърдение 2.1.9 *Алтернативната група A_n се поражда от тройните цикли и по-точно $A_n = <(1\,2\,3), (1\,2\,4), \dots, (1\,2\,n)>$.*

Доказателство. A_n се състои от пермутации, които са произведение на четен брой транспозиции. Следователно всяка четна пермутация може да разглеждаме като произведение от двойки транспоции. Но има само три възможности за тези двойки: да съвпадат, да имат един общ елемент и до са независими цикли.

$$\begin{array}{rcl}(a\,b)(a\,b) & = & \epsilon \\ (a\,b)(b\,c) & = & (a\,b\,c) \\ (a\,b)(c\,d) & = & (a\,b)(b\,c)(b\,c)(c\,d) = (a\,b\,c)(b\,c\,d)\end{array}$$

И в трите случая всяка двойка е произведение на тройни цикли. Следователно и всяка четна пермутация е произведение на тройни цикли.
Нека да вземем произволен троен цикъл $(x\,y\,z)$ и да разгледаме $\sigma = (1\,2\,x)(1\,2\,y)$. Тогава

$$\sigma(1\,2\,z)\sigma^{-1} = (1\,2\,x)[(1\,2\,y)(1\,2\,z)(1\,2\,y)^{-1}](1\,2\,x)^{-1} = (1\,2\,x)(1\,y\,z)(1\,2\,x)^{-1} = (x\,y\,z).$$

С това доказахме и втората част на твърдението.

Упражнение 2.1.1 *Покажете, че*

$$S_n =< (1\,2), (1\,3), \ldots, (1\,n) >=< (1\,2), (1\,2\,3\,\ldots\,n) >=< (1\,2), (2\,3\,\ldots\,n) > .$$

Пример 2.1.3 *Да определим колко пермутации на S_8 комутират с $\pi = (1\,3\,5)(2\,4)(6\,7)$.* Ако $\sigma \in S_8$ комутира с π, то $\sigma\pi = \pi\sigma$, т. е. $\sigma\pi\sigma^{-1} = \pi$. Но в такъв случай σ трябва да довежда наредената тройка $(1, 3, 5)$ в някоя от тройките $(1, 3, 5)$, $(3, 5, 1)$ или $(5, 1, 3)$, т.е. има три възможности за $(\sigma(1), \sigma(3), \sigma(5))$. Аналогично, σ трябва да довежда $(2, 4)$ в $(2, 4)$, $(4, 2)$, $(6, 7)$ или $(7, 6)$, което дава 4 въэможности за $(\sigma(2), \sigma(4))$. Тогава σ довежда $(6, 7)$ в $\{2, 4, 6, 7\} \setminus \{\sigma(2), \sigma(4)\}$, което дава 2 възможности за $(\sigma(6), \sigma(7))$. За $\sigma(8)$ има единствена възможност. Следователно могат да се конструират точно

$$3.4.2.1 = 24$$

пермутации $\sigma \in S_8$, които комутират с π.

Упражнение 2.1.2 *Да се намери броят на елементите на S_7, които комутират с $\pi = (1\,2\,3)(4\,5)$.*

Теорема 2.1.10 *Нека p е просто число и $G \subseteq S_p$. Ако G съдържа транспозиция и цикъл с дължина p, то $G = S_p$.*

Доказателство. Нека $\sigma \in G$ е с ред $o(\sigma) = p$ и $\tau \in G$ е транспозиция. Без ограничение на общност може да считаме, че $\sigma = (12\ldots p)$. Нека $\tau = (kl)$, $k < l$. Полагаме $d = l - k$. Тъй като $\sigma^\nu : \ x \to x + \nu$, то съгласно Теорема 2.1.7 $\sigma^\nu\tau\sigma^{-\nu} = (k + \nu,\ l + \nu)$.
Замествайки последователно $\nu = p-k+1, p-k+2, \ldots, p, 1, 2, \ldots, p-k$ получаваме, че следните транспозиции са в G:

$$(1,\ d+1),\ (2,\ d+2),\ \ldots,\ (i,\ i+d),\ \ldots,\ (p,\ d) \in G, \quad 1 \le i \le p.$$

Но тогава

$$\begin{aligned}(d+1,\ 2d+1)(1,\ d+1)(d+1,\ 2d+1) &= (1,\ 2d+1) \in G \\ (2d+1,\ 3d+1)(1,\ 2d+1)(2d+1,\ 3d+1) &= (1,\ 3d+1) \in G \\ \text{и т. н.} \quad & \dots\end{aligned}$$

Следователно всички

$$(1,\ d+1),\ (1,\ 2d+1),\ (1,\ 3d+1),\ \dots,\ (1,\ (p-1)d+1) \in G. \qquad (2.1.1)$$

Но $ad+1 \equiv bd+1 \pmod p \Leftrightarrow a \equiv b \pmod p$. Следователно горното множество от транспозиции съвпада с $\{(12),\ (13), \dots,\ (1p)\}$, откъдето

$$G \supseteq < (12),\ (13), \dots,\ (1p) >= S_p.$$

Следователно $G \equiv S_p$.

Да се върнем към алтернативната група. Съгласно Твърдение 2.1.9

$$A_4 =< (\alpha = (123),\ \beta = (124) \mid \alpha^3 = \beta^3 = (\alpha\beta)^2 = \epsilon >,$$

но елементите ѝ не се изчерпват с произведенията $\alpha^k\beta^l$ понеже A_4 има 12, а не 9 елемента. Причината е, че подгрупата породена от троен цикъл не е нормална подгрупа. A_4 съдържа като нормална подгрупа само K_4 и

$$A_4 = K_4 \cup (123)K_4 \cup (132)K_4.$$

Но за алтернативните групи от по-висока размерност горното е невъзможно тъй като те нямат нормални подгрупи:

Теорема 2.1.11 *За всяко $n \geq 5$ алтернативната група A_n е проста група.*

Доказателство.

2.2 Крайни матрични групи.

2.2.1 Пермутационни матрици.

Дефиниция 2.2.1 *Една матрица се нарича **пермутационна**, ако елементите ѝса само нули и единици и ако във всеки ред и всеки стълб има само по една единица.*

Например следната матрица е пермутационна:

$$\mathbf{P}_1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad \det \mathbf{P}_1 = -1.$$

Името на дефинирания тип матрици произлиза от следния факт: Ако една матрица A се умножи отляво с пермутационна матрица резултатът е разместване на редовете на A. Умножението отдясно реализира същата пермутация, но върху стълбовете на A. Например, нека $\mathbf{A} = (a_{ij})$ е 3×3 матрица и

$$\mathbf{P}_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Тогава

$$\mathbf{P}_2\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{31} & a_{32} & a_{33} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}; \qquad \mathbf{A}\mathbf{P}_2 = \begin{pmatrix} a_{11} & a_{13} & a_{12} \\ a_{21} & a_{23} & a_{22} \\ a_{31} & a_{33} & a_{32} \end{pmatrix}.$$

В общия случай, ако номерираме редовете (съответно стълбовете) на матрицата $\mathbf{A}$ с числата от 1 до n, то пермутацията π върху редовете (съответно стълбовете), която $\mathbf{P} = (p_{ij})$ реализира се задава с правилото:

$$\pi(i) = j \Longleftrightarrow p_{ij} = 1.$$

В горните примери матрицата $\mathbf{P}_1$ реализира $\pi = (1432)$, а матрицата $\mathbf{P}_2$ реализира $\tau = (23)$.

Елементарните свойства на детерминантите ни дават, че детерминантата на една пермутационна матрица е ± 1. По точно, тя е 1, ако задава четна пермутация и -1, ако задава нечетна (Защо?!).

2.2.2 Група на кватернионите.

Да разгледаме следните 2×2 матрици над $\mathbb{C}$, т. е. от $GL(2, \mathbb{C})$:

$$\mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}; \qquad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}; \qquad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Непосредствено се проверяват равенствата:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{E} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$\mathbf{ij} = -\mathbf{ji} = \mathbf{k},\ \mathbf{jk} = -\mathbf{kj} = \mathbf{i},\ \mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

С тяхна помощ лесно се вижда, че

$$G = \{\pm\mathbf{E}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$$

е група от осем елемента относно стандартното умножение на матрици. Тя се нарича ***група на кватернионите*** и се означава обикновено с Q_8.

Да положим $a = \mathbf{i},\ b = \mathbf{j}$. В сила е $a^4 = \mathbf{E},\ a^2 = b^2$ и $bab^{-1} = a^{-1}$.

Твърдение 2.2.2 *Всяка абстрактна група G зададена в термините на образуващи и пораждащи съотношения с*

$$G = < a, b \mid a^4 = 1, a^2 = b^2, bab^{-1} = a^{-1} >$$

е изоморфна на Q_8.

Доказателство. Доказателството оставяме на читателя.

Твърдение 2.2.3 *Групата на кватернионите Q_8 не е изоморфна на диедралната група с осем елемента D_4.*

Доказателство. Доказателството оставяме на читателя.

2.2.3 Групата от матрици на Pauli.

Дефиниция 2.2.4 ***Група от матрици на Pauli*** *се нарича групата Pl породена от матриците*

$$\sigma_{\mathbf{x}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \qquad \sigma_{\mathbf{y}} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \qquad \sigma_{\mathbf{z}} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Тази група е популярна и се използва в квантовата физика.

Ползвайки означенията от предния параграф веднага можем да напишем

$$\sigma_{\mathbf{x}} = -i\mathbf{k}, \qquad \sigma_{\mathbf{y}} = -i\mathbf{j}, \qquad \sigma_{\mathbf{z}} = -i\mathbf{i}.$$

В сила са и следните равенства

$$\sigma_{\mathbf{x}}{}^2 = \sigma_{\mathbf{y}}{}^2 = \sigma_{\mathbf{z}}{}^2 = \mathbf{E},$$

$$\sigma_{\mathbf{x}}\sigma_{\mathbf{y}} = -\sigma_{\mathbf{y}}\sigma_{\mathbf{x}} = \mathbf{i} = i\sigma_{\mathbf{z}}$$

$$\sigma_{\mathbf{y}}\sigma_{\mathbf{z}} = -\sigma_{\mathbf{z}}\sigma_{\mathbf{y}} = \mathbf{k} = i\sigma_{\mathbf{x}}$$

$$\sigma_{\mathbf{z}}\sigma_{\mathbf{x}} = -\sigma_{\mathbf{x}}\sigma_{\mathbf{z}} = \mathbf{j} = i\sigma_{\mathbf{y}}$$

С тяхна помощ читателят лесно може да провери, че са в сила следните твърдения:

Твърдение 2.2.5 *Групата на Pauli се състои от 16 елемента, а именно:*

$$Pl = \{\pm\boldsymbol{E}, \pm\sigma_{\mathbf{x}}, \pm\sigma_{\mathbf{y}}, \pm\sigma_{\mathbf{z}}, \pm i\boldsymbol{E}, \pm i\sigma_{\mathbf{x}}, \pm i\sigma_{\mathbf{y}}, \pm i\sigma_{\mathbf{z}}\} = \{\pm\boldsymbol{E}, \pm\sigma_{\mathbf{x}}, \pm\sigma_{\mathbf{y}}, \pm\sigma_{\mathbf{z}}, \pm i\boldsymbol{E}, \pm\boldsymbol{k}, \pm\boldsymbol{j}, \pm\boldsymbol{i}\}$$

Твърдение 2.2.6 *Групата на Pauli съдържа Q_8 като нормална подгрупа с индекс 2 и*

$$Pl = Q_8 \cup i\boldsymbol{E}Q_8 = <\sigma_{\mathbf{x}}> \times_s Q_8,$$

т. е. тя е полудиректно произведение на Q_8 и $<\sigma_{\mathbf{z}}>$.

Доказателство. Q_8 е подгрупа с индекс 2, следователно тя е нормална подгрупа: $Q_8 \lhd Pl$. По точно

$$\sigma_{\mathbf{z}}\,\mathbf{i}\,\sigma_{\mathbf{z}} = \mathbf{i}, \quad \sigma_{\mathbf{z}}\,\mathbf{j}\,\sigma_{\mathbf{z}} = -\mathbf{j}, \quad \sigma_{\mathbf{z}}\,\mathbf{k}\,\sigma_{\mathbf{z}} = -\mathbf{k}.$$

2.2.4 $GL(n,\mathbb{F})$ и $SL(n,\mathbb{F})$ над крайно поле $\mathbb{F}$.

Теорема 2.2.7 *Нека $\mathbb{F} = GF(q)$ е крайно поле с q елемента. Тогава*

$$\begin{aligned}|GL(n,\mathbb{F})| &= (q^n-1)(q^n-q)(q^n-q^2)\dots(q^n-q^{n-1}) = q^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}(q^i-1),\\ |SJ(n,\mathbb{F})| &= \frac{1}{q-1}\mid GL(n,\mathbb{F})\mid.\end{aligned}$$

Доказателство. Редовете на всяка матрица от $GL(n,\mathbb{F})$ трябва да са линейно независими. Затова за първия ред имаме q^n-1 възможности, втория ред можем вече да изберем по q^n-q начина (махнали сме всички пропорционални на парвия ред, третия ред - по q^n-q^2 начина (не участват всички линейни комбинации на първите редове) и т. н., за последния ред имаме q^n-q^{n-1} възможности.

Упражнение 2.2.1 *Покажете, че подмножествата на $SL(2,\mathbb{Z}_p)$*

$$P_1 = \left\{\begin{pmatrix}1 & \alpha\\ 0 & 1\end{pmatrix} \mid \alpha\in\mathbb{Z}_p\right\} = \left\langle\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right\rangle \quad и \quad P_2 = \left\{\begin{pmatrix}1 & 0\\ \beta & 1\end{pmatrix} \mid \beta\in\mathbb{Z}_p\right\} = \left\langle\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\right\rangle$$

са циклични подгрупи от ред p на $SL(2,\mathbb{Z}_p)$.

2.2.5 Проективните групи $PGL(n,\mathbb{F})$ и $PSL(n,\mathbb{F})$.

Нека $\mathbb{F}$ е произволно поле. Скаларните матрици $\mathcal{D} = \{d\mathbf{E} \mid d\in\mathbb{F}^*\}$ комутират с всички матрици и следователно образуват нормална подгрупа на $GL(n,\mathbb{F})$. Съответно $\mathcal{D}\cap SL(n,\mathbb{F}) \lhd SL(n,\mathbb{F})$. ***Проективните линейна и специална групи*** дефинираме с

$$\begin{aligned}PGL(n,\mathbb{F}) &= GL(n,\mathbb{F})/\mathcal{D}\\ PSL(n,\mathbb{F}) &= SL(n,\mathbb{F})/(\mathcal{D}\cap SL(n,\mathbb{F}))\end{aligned}$$

Упражнение 2.2.2 *Докажете, че $PSL(n,\mathbb{Z}_3)\cong A_4$. Изпишете елементите ѝ. (Вижте задачи 2.6 и 2.7.)*

За $p>3$ групите $PSL(n,\mathbb{Z}_p)$ са прости и наред с A_n това са едни от най-ранните примери на прости групи. $PSL(n,\mathbb{Z}_p)$ е групата от преобразования на проективната права, $P(1,\mathbb{Z}_p) = \{0,1,2,\dots,p-1\}\cup\{\infty\}$.

2.2.6 Афинните групи $AGL(n,\mathbb{F})$.

Нека $\mathbb{F}$ е произволно поле. Да разгледаме съвкупността от изображения

$$T_{\mathbf{A},\mathbf{b}} : \left|\begin{array}{ccc}\mathbb{F}^n & \to & \mathbb{F}^n\\ \mathbf{x} & \to & \mathbf{A}\mathbf{x}+\mathbf{b}\end{array}\right. ,$$

където $\mathbf{A} \in GL(n, \mathbb{F})$ и $\mathbf{b} \in \mathbb{F}^n$. ($\mathbb{F}^n$ го разглеждаме като пространство от вектор-стълбове за да запазим означенията, които ползваме при работа с матрици на линейни оператори.) Лесно се вижда, че всяко изображение се определя еднозначно от $\mathbf{A}$ и $\mathbf{b}$, биекция е и всички такива изображения образуват група относно композицията. Нарича се ***афинна линейна група***. Бележим $AGL(n, \mathbb{F})$.

Упражнение 2.2.3 *Докажете свойствата:*

$$T_{\mathbf{C},\mathbf{d}} T_{\mathbf{A},\mathbf{b}} = T_{\mathbf{CA},\mathbf{Cb}+\mathbf{d}}, \qquad T^{-1}_{\mathbf{A},\mathbf{b}} = T_{\mathbf{A}^{-1},-\mathbf{A}^{-1}\mathbf{b}}$$

Множеството

$$T(\mathbb{F}^n) = \{T_{\mathbf{E},\mathbf{b}} \mid \mathbf{b} \in \mathbb{F}^n\}$$

от всички транслации е нормална подгрупа на $AGL(n, \mathbb{F})$, тъй като тя е ядрото на хомоморфизма $AGL(n, \mathbb{F}) \to GL(n, \mathbb{F})$, зададен с $T_{\mathbf{A},\mathbf{b}} \to \mathbf{A}$. Следователно от теоремата за хомоморфизмите получаваме

$$AGL(n, \mathbb{F})/T(\mathbb{F}^n) \cong Gl(n, \mathbb{F}).$$

2.2.7 Групите $O(n)$ и $SO(n)$.

В Глава 1 дефинирахме ортогонолната група $O(n)$ като групата от всички ортогонални $n \times n$ матрици над $\mathbb{R}$, а $SO(n)$ като подгрупата ѝ от матриците с детерминанта равна на 1. Ортогоналните матрици представят изометриите (еднаквостите) в $\mathbb{R}^n$, а $SO(n)$ е подгрупата от движенията (еднаквостите на твърдото тяло), т. е. тези еднаквости, които не променят ориентацията. От линейната алгебра знаем следните резултати:

Теорема 2.2.8 *Групата $O(2)$ се поражда от матриците*

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}, \quad \alpha \in (0, 2\pi).$$

Следствие 2.2.9 *Еднаквостите запазващи началото в $\mathbb{R}^2(O)$ се изчерпват с ротациите около O на ъгъл $\alpha \in [0, 2\pi)$, осевите симетрии относно прави през O и произведенията им.*

Забележка 2.1 *Транслацията от гледна точка на линейната алгебра е изоморфизъм на линейните пространства $\mathbb{R}^2(O)$ и $\mathbb{R}^2(O')$. Напомняме, че произведението на две осеви симетрии е ротация.*

Упражнение 2.2.4 *Докажете горната теорема.*

Упражнение 2.2.5 *Докажете, че ако $\mathbb{F}$ е крайно поле, то*

$$O(2, \mathbb{F}) = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{F},\ a^2 + b^2 = 1 \right\rangle$$

$$SO(2, \mathbb{F}) = \left\langle \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{F},\ a^2 + b^2 = 1 \right\rangle$$

Теорема 2.2.10 (Ойлер) *Движенията в пространството $\mathbb{R}^3(O)$ се изчерпват с въртенията около ос през точката O.*

Горната теорема показва, че за всяко движение в $\mathbb{R}^3(O)$ има 2 точки върху единичната сфера, наричани ***полюси***, които остават неподвижни.

2.3 Допълнителни задачи към Глава 2.

Задача 2.1 *Покажете, че в* S_n *за* $x \neq y$ *е в сила*

$$(x\ z)(y\ z) = (x\ y)(x\ z), \qquad (x\ z)(y\ z) = (y\ z)(x\ y).$$

Задача 2.2 *Докажете, че*

$$G_1 =< (12),\ (1234) >, \quad G_2 =< (12),\ (1234) >, \quad G_3 =< (12),\ (1234) >,$$

изчерпват подгрупите от ред 8 на S_4 *и всяка от тях е изоморфна на диедралната група* D_4*. Разпишете всичките им елементи. Намерете сечението им.*

Задача 2.3 *Постройте графа от всички погрупи на* S_4*. (Върховете са подгрупите, като два върха са свързани точно когато едната подгрупа съдържа другата. На върха да е* S_4*, а на дъното* $\{\epsilon\}$*.)*

Задача 2.4 *Докажете, че една пермутация* $\sigma \in S_n$ *е четна тогава и само тогава, когато в* $(\sigma(1), \sigma(2), \dots, \sigma(n))$ *има четен брой инверсии.*

Задача 2.5 *Ползвайки системата GAP намерете структурите от подгрупи на* S_5, S_6, S_7 *и* S_8*. Опишете, кои от включванията са като нормални подгрупи.*

Задача 2.6 *Да се провери, че множеството от матрици над* $\mathbb{Z}_3$*:*

$$\pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \pm\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}, \quad \pm\begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}, \quad \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

образуват нормална подгрупа на $SL(2, \mathbb{Z}_3)$*, която е изоморфна на* Q_8*.*

Задача 2.7 *Да се покаже, че групите* S_4 *и* $SL(2, \mathbb{Z}_3)$ *не са изоморфни.*

Задача 2.8 *Докажете, че* $SO(2, \mathbb{Z}_7)$ *е циклична група от ред 8 и намерете образуващата ѝ. Определете* $O(2, \mathbb{Z}_7)$*.*