Примена теорије група

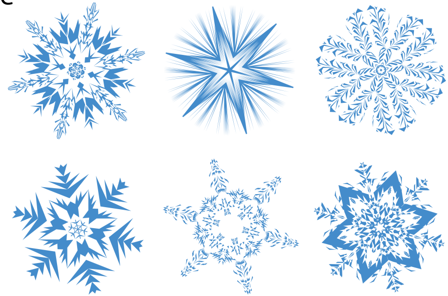
Данијел Силађи

Гимназија Јован Јовановић Zmaj

мај 2014.

Мотивација

- У свакодневном животу срећемо "симетричне" објекте
- Шта је заправо симетрија?
- Нешто "изгледа исто" кад га гледамо са различитих страна
- Формалније: симетрија неког објекта је нека трансформација у простору која пресликава тај објекат у самог себе

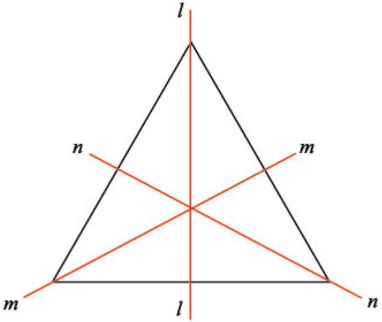


Мотивација 2

Људи су приметили да такве трансформације имају нека својства заједничка за све њих:

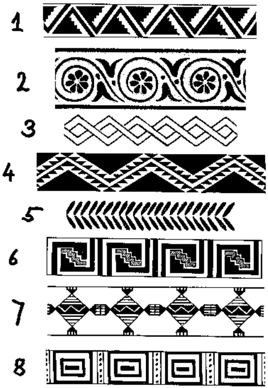
- Трансформације су бијективне, за сваку трансофмацију постоји њиј инверзна трансформација која "поништава" њен ефекат.
- Комбиновањем (композицијом) две трансформације добијамо опет трансформацију
- Сваки објекат има једну тривијалну симетрију, идентичко пресликавање - свака тачка се слика у саму себе

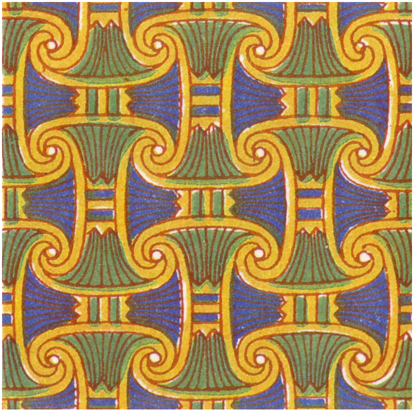
Пример - симетрије многоуглова



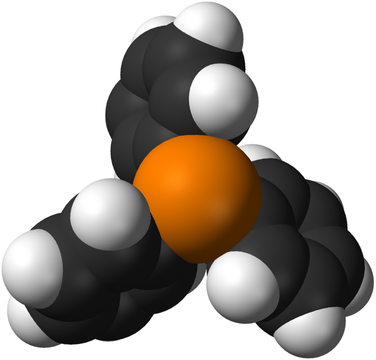
- Ротације око центра троугла: r (за $\pi/3$), $r \circ r = r^2$ (за $2\pi/3$) и $r \circ r \circ r = r^3 = e$ (за 2π, односно 0 радијана - идентичко пресликавање)
- Осне симетрије s_1, s_2 и s_3 у односу на праве l, m, n.
- Слично, важи $s_i \circ s_i = s_i^2 = e$, за $i \in \{1, 2, 3\}$, али и $s_1 s_2 = r^2$, ...

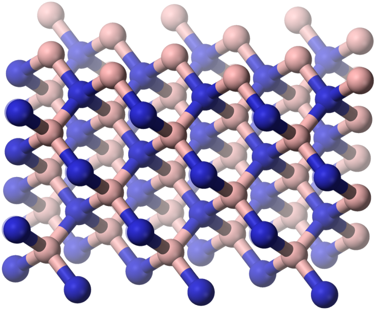
Пример - frieze и wallpaper цртежи





Пример - молекулске и кристалне симетрије





Основне дефиниције

Елементи неке групе не морају нужно да буду трансформације, већ елементи произвољног скупа G, за које смо дефинисали операцију "множења", са следећим особинама:

1. Ако a и b припадају G, онда и њихов производ, ab припада G
2. Операција множења је асоцијативна, односно важи $a(bc) = (ab)c$
3. G садржи *јединични елемент* e, за који важи $ae = ea = a$, за свако $a \in G$
4. За свако $a \in G$ постоји $b \in G$, за које важи $ab = ba = e$. Такав b се зове *инверзни елемент* за a, и обележава се са a^{-1}

Примери група

Иако операцију групе често називамо "множењем", она заправо и може а и не мора то да буде:

- Скуп рационалних (или реалних) бројева без 0 чини групу у односу на множење (у уобичајеном смислу)
- Скуп целих (али не и природних!) бројева чини групу у односу на сабирање
- Скуп свих инвертибилних (регуларних, њихова детерминанта је различита од 0) квадратних матрица, над пољем $\mathbb{R}$ или $\mathbb{C}$, димензија $n \times n$, чини групу, а операција групе је множење матрица.

Неке корисне ознаке и дефиниције

- Ако је операција групе комутативна, група је комутативна или *Абелова*
- $a^n \equiv \underbrace{aa\ldots a}_{n\text{ пута}}$, и $a^{-n} \equiv (a^{-1})^n = (a^n)^{-1}$
- Ако су сви степени a различити, група је *бесконачног реда*. Иначе, *ред елемента* је најмање $n \in \mathbb{N}$ за које важи $a^n = e$
- *Ред групе* је број елементата те групе
- Непразан подскуп H групе G је *подгрупа* групе G, ако је H група у односу на рестрикцију операције групе G на H
- $\langle A \rangle$ је *подгрупа генерисана скупом* A - најмања подгрупа G која садржи скуп A. Ако је $\langle A \rangle = G$, онда је A *генераторни скуп* групе G, а његови елементи - *генератори* групе G.

Пермутације

- *Пермутације* скупа $\{1, 2, \ldots, n\}$ су све функције π које бијективно пресликавају тај скуп у самог себе
- Записују се као

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix},$$

  где важи $\{a_1, a_2, \ldots, a_n\} = \{1, 2, \ldots, n\}$, и $\pi(i) = a_i$, за $1 \leq i \leq n$
- Пермутације n елемената чине групу S_n, *симетричну групу*
- Кејлијева (Cayley) теорема: Свака група G реда n је изоморфна са подгрупом симетричне групе S_n.

Лагранжова теорема

Теорема

Ако је G нека група реда n, и H њена подгрупа реда m, тада m дели n.

- У доказу, поделили смо групу G на k дисјунктних подскупова:

$$G = H \cup a_1 H \cup a_2 H \cup \ldots \cup a_{k-1} H$$

- Број k се зове *индекс* подгрупе H у групи G
- Скупови $a_i H$ се зову *леве класе* H у G
- Скуп свих левих класа неке подгрупе се обележава са G/H

Инваријантне подгрупе

- За елемент b групе G кажемо да је *конјугован* елементу a ако постоји $u \in G$ за који важи

$$uau^{-1} = b$$

- Релација конјугације је релација еквиваленције, разбија групу на класе конјугације
- Посматрајмо подгрупу H групе G. Тада се лако показује да је и aHa^{-1} (сви производи aha^{-1}, где $h \in H$) подгрупа од G, при чему је a произвољни елемент из G. Уколико за свако $a \in G$ важи

$$aHa^{-1} = H,$$

тада кажемо да је H *инваријантна* или *нормална подгрупа* групе G, и то обележавамо са $H \lhd G$.

Инваријантне подгрупе - наставак

- За неку групу G и њену нормалну подгрупу H дефинишимо операцију $\cdot : G/H \to G/H$ као $aH \cdot bH := abH$
- Скуп свих левих класа G/H (у случају да је $H \lhd G$) група у односу на овако дефинисану операцију
- Јединични елемент је $eH = H$, а инверзни елемент за класу aH је $a^{-1}H$
- Овако добијена група се назива *фактор-група*, обележава се са G/H
- Њен ред индекс групе H у G
- Пример: $\mathbb{Z}/n\mathbb{Z}$, и сабирање

Векторски простори

Нека је $(V, +)$ комутативна група, а $(F, +, \cdot)$ поље. V је *векторски простор над пољем* F, ако је дефинисано пресликавање $F \times V \to V$, при чему слику пара (α, v) означавамо са αv, тако да за свако $\alpha, \beta \in F$, $u, v \in V$ важи:

1. $\alpha(u + v) = \alpha u + \alpha v$
2. $(\alpha + \beta)v = \alpha v + \beta v$
3. $(\alpha \cdot \beta)v = \alpha(\beta v)$
4. $1v = v$

где је са 1 означен неутрални елеменат за множење поља F. Елементи скупа F се називају *скалари*, а елементи скупа V - *вектори*. Ми ћемо у овом раду посматрати искључиво поља реалних и комплексних бројева.

База векторског простора

- *База* векторског простора је низ вектора који је линеарно независан и који генерише векторски простор.
- Још алтернативних дефиниција:
  - Низ вектора је база ако и само ако је тај скуп максималан линеарно независан скуп.
  - Низ вектора је база ако и само ако је тај скуп минималан скуп генератора
  - Низ вектора $v_1, \ldots, v_n$ је база ако и само ако се сваки вектор $x \in V$ може на јединствен начин написати у облику

$$x = \sum_{1}^{n} \alpha_i v_i, \quad \alpha_1, \ldots, \alpha_n \in F$$

- Све базе неког одређеног векторског простора V имају исти број елемената - *димензија векторског простора*, $\dim V$

Унитарни векторски простор

Нека је V векторски простор над пољем F (где је $F = \mathbb{R}$ или $F = \mathbb{C}$). *Унутрашњи (скаларни) производ* на V је свака функција $(,) : V \times V \to F$, при чему слику уређеног пара вектора $(x, y) \in V \times V$ означавамо са (x, y), за коју за свако $x, y, z \in V$ и свако $\alpha \in F$ важи

1. $(x, y) = \overline{(y, x)}$
2. $(x + y, z) = (x, z) + (y, z)$
3. $(\alpha x, y) = \alpha(x, y)$
4. $(x, x) \geq 0$
5. $(x, x) = 0 \Leftrightarrow x = 0$

- У унитарном векторском простору V функција $\| \ \| : V \to \mathbb{R}$, дефинисана са
$$\|x\| = \sqrt{(x, x)}$$
назива се *норма* на V
- Ненегативан реалан број $\|x\|$ назива се *норма вектора* x
- *Растојање* вектора x и y је дефинисано са
$$d(x, y) = \|x - y\|.$$
- У унитарном векторском простору V за свако $x, y \in V$ важи
$$|(x, y)| \leq \|x\|\|y\|,$$
при чему једнакост важи ако и само ако су вектори x и y линеарно зависни.

- У еуклидским векторским просторима можемо дефинисати угао између вектора $x \neq 0$ и $y \neq 0$, као реалан број $\alpha \in [0, \pi]$, такав да је

$$\cos\alpha = \frac{(x, y)}{\|x\| \|y\|}$$

- За два вектора x и y кажемо да су *ортогонални* ако је $(x, y) = 0$.
- За базу $B = \{b_1, \ldots, b_n\}$ неког унитарног векторског простора V кажемо да је *ортонормирана*, ако је

$$(b_i, b_j) = \begin{cases} 1 & \text{ако } i = j \\ 0 & \text{ако } i \neq j \end{cases}$$

- Сваки унитарни векторски простор поседује бар једну ортонормирану базу, и она се може добити из произвољне базе применом *Грам-Шмитовог поступка*

Линеарне трансформације

Дефиниција

Нека су V_1 и V_2 векторски простори над истим пољем F. Пресликавање $A : V_1 \to V_2$ такво да је

$$(\forall a, b \in V_1)(\forall \alpha, \beta \in F) A(\alpha a + \beta b) = \alpha A(a) + \beta A(b)$$

назива се *линеарна трансформација (линеарни оператор, хомоморфизам)* векторског простора V_1 у V_2. Уколико је $V_1 = V_2 = V$, тада је A просто линеарна трансформација векторског простора V.

Матрица линеарне трансформације

- Претпоставимо да је $\{a_1, \dots a_n\}$ база векторског простора V. Тада, линеарну трансформацију A можемо задати са

$$A(a_1) = b_1, A(a_2) = b_2, \dots, A(a_n) = b_n$$

где су $b_1, \dots, b_n \in V$.

- Пошто је $\{a_1, \dots a_n\}$ база, сваки од вектора b_i може се на јединствен начин написати као линеарна комбинација вектора базе, па имамо:

$$A(a_1) = \alpha_{11} a_1 + \alpha_{21} a_2 + \dots + \alpha_{n1} a_n$$

$$A(a_2) = \alpha_{12} a_1 + \alpha_{22} a_2 + \dots + \alpha_{n2} a_n$$

$$\dots$$

$$A(a_n) = \alpha_{1n} a_1 + \alpha_{2n} a_2 + \dots + \alpha_{nn} a_n$$

- Ако напишемо коефицијенте α_{ij} као матрицу, вредност функције $A(x)$ (као линеарне трансформације произвољног вектора $x \in V$) можемо израчунати простим множењем матрица:

$$[A(x)] = [A][x] = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{bmatrix} \begin{bmatrix} \zeta_1 \\ \zeta_2 \\ \vdots \\ \zeta_n \end{bmatrix}$$

  при чему је $x = \zeta_1 a_1 + \zeta_2 a_2 + \dots \zeta_n a_n$.
- Матрични запис линеарне трансформације зависи од избора базе!

Групе матрица

- *Општа линеарна група*, $GL(n, \mathbb{C})$ скуп свих $n \times n$ регуларних (инвертибилних, детерминанта различита од 0) матрица над $\mathbb{C}$, у односу на множење матрица. Ове матрице одговарају свим инвертибилним линеарним трансформацијама простора $\mathbb{C}^n$. Њена подгрупа је $GL(n, \mathbb{R})$, скуп свих инвертибилних реалних матрица $n \times n$ у односу на множење.
- *Специјална линеарна група*,

$$SL(n, \mathbb{C}) = \{M \in GL(n, \mathbb{C}) | \det M = 1\}.$$

Слично,

$$SL(n, \mathbb{R}) = \{M \in GL(n, \mathbb{R}) | \det M = 1\}.$$

- *Унитарна група,* $U(n)$

  $$U(n) = \{M \in GL(n, \mathbb{C}) | MM^{\dagger} = I\}.$$

  Чува скаларни производ вектора $x = (x_1, ..., x_n)$, $y = (y_1, ... y_n)$: $(Mx, My) = (x, y) = \sum_{i=1}^{n} x_i \overline{y}_i$.
- *Специјална унитарна група*: $SU(n) = \{M \in U(n) | \det M = 1\}$.
- *Ортогонална група*: $O(n) = \{M \in GL(n, \mathbb{R}) | MM^T = 1\}$. Слично као унитарна група, чува стандардни скаларни производ $(Mx, My) = (x, y) = \sum_{i=1}^{n} x_i y_i$.
- *Специјална ортогонална* група, $SO(n) = \{M \in O(n) | \det M = 1\}$.

Псеудоортогонална група

- Нека је g дијагонална матрица $g = \mathrm{diag}(\underbrace{1, .., 1}_{p}, \underbrace{-1, ..., -1}_{q})$.
- Псеудоортогонална група $O(p, q)$ се дефинише као

$$O(p, q) = \{M \in GL(n, \mathbb{R}) | M^T gM = g\}.$$

- То управо матрице које чувају квадратну форму

$$\sum_{i=1}^{p} x_i y_i - \sum_{i=1}^{q} x_{p+i} y_{p+i}.$$

- Најпознатија група ове врсте је Лоренцова група $O(1, 3)$, са којом ћемо се позабавити на крају овог рада.

Симетрије унитарних векторских простора

Дефиниција

Нека је дат еуклидски векторски простор V коначне димензије.

Изометријске трансформације су трансформације (пресликавања) $M : V \to V$, које чувају растојање, тј. за свако $u, v \in V$ важи

$$\|u - v\| = \|M(u) - M(v)\|$$

Ортогоналне трансформације су трансформације $M : V \to V$ које чувају скаларни производ, тј. за све $u, v, \in V$

$$(u, v) = (M(u), M(v))$$

Две теореме

Теорема

Нека је $M : V \to V$ ортогонално пресликавање еуклидског векторског простора. Тада је M изометријска трансформација која чува 0, тј. $M(0) = 0$.

Теорема

Нека је M изометрија неког еуклидског векторског простора и нека је $M(0) = 0$. Тада је M ортогонална трансформација

...и трећа теорема

Теорема

Ако је M ортогонална трансформација коначнодимензионалног еуклидског простора, тада важи

1. M *је линеарна трансформација*
2. *Ако је* $[M]$ *матрица трансформације* M *у односу на неку ортонормирану базу, тада важи* $[M]^T[M] = I$
3. M *је инвертибилна и* M^{-1} *је такође изометрија*
4. $\det[M] = \pm 1$ *(у било којој бази)*

Лоренцове трансформације и метрика Минковског

- У специјалној теорији релативности, једина инваријантна метрика у простор-времену је *метрика Минковског*:

$$\Delta s^2 = c^2\Delta t^2 - \Delta x^2 - \Delta y^2 - \Delta z^2$$

- Лоренцове трансформације можемо посматрати као "ротације" простор-времена, аналогно ротацијама тродимензионалног еуклидског простора (које чувају метрику $s^2 = x^2 + y^2 + z^2$)
- Такође, $s^2 = X \cdot X = X^T \eta X$, при чему је матрица η (понекад и њу називамо метриком Минковског) дата са

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

Лоренцова група

- Тражимо решења матричне једначине $\Lambda^T \eta \Lambda = \eta$
- Очекујемо и добијамо 6 независних решења, подељених у 2 класе: просторне ротације и *Лоренцови потисци*

$$\Lambda = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & & & \\ 0 & & R & \\ 0 & & & \end{bmatrix} \text{ или } \Lambda = \begin{bmatrix} \gamma & -\gamma v/c & 0 & 0 \\ -\gamma v/c & \gamma & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

- R је матрица ротације у 3 димензије, а $\gamma = \frac{1}{\sqrt{1-\frac{v^2}{c^2}}}$.
- Ове матрице чине групу, $O(1,3)$ ($\det \Lambda = \pm 1$). Подгрупе: $SO(1,3)$ ($\det \Lambda = 1$) и њена подгрупа $SO^+(1,3)$ ($\Lambda_{11} > 0$)

Лоренцова група и $SL(2, \mathbb{C})$

- Представимо вектор $X = (ct, x, y, z)$ као (Хермитску) матрицу
$$\hat{X} = \begin{bmatrix} ct + z & x - iy \\ x + iy & ct - z \end{bmatrix}$$
- Све 2×2 Хермитске матрице се могу записати у овом облику
- Згодно својство $X \cdot X = \det \hat{X} = c^2 t^2 - x^2 - y^2 - z^2$
- Испоставља се да је $SO(1,3)^+ \cong SL(2, \mathbb{C})/\mathbb{Z}_2$, односно да се све Лоренцове трансформације могу представити матрицама из $SL(2, \mathbb{C})$, и обрнуто
- Свели смо један потпуно "физички" проблем на чисту математику!

Хвала на пажњи!