Групи. Теорема на Кейли.

Нека $G(G \neq \varnothing)$ е множество с въведена бинарна операция $\cdot$, т.е. на всеки два елемента $a \in G$ и $b \in G$ е съпоставен елемент $a \cdot b \in G$[1]. Казваме, че G е *група*, ако са изпълнени следните три аксиоми:

1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ за всеки $a, b, c \in G$, т.е. въведената операция е *асоциативна*;

2. Съществува елемент $e \in G$, наречен *единичен елемент*, такъв че $a \cdot e = e \cdot a = a$ за произволен елемент $a \in G$;

3. За всеки елемент $a \in G$ съществува елемент $a^{-1} \in G$, наречен *обратен елемент*, такъв че $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Ако допълнително е изпълнено и

4. $a \cdot b = b \cdot a$ за $\forall a, b \in G$, т.е. ако въведената операция е *комутативна*, то групата G се нарича *абелева* или *комутативна*.

Броят на елементите в G бележим с $|G|$. Ако елементите на G са краен брой, то групата е *крайна*, а числото $|G|$ се нарича *ред на групата* G. В противен случай G е безкрайна група и $|G| = \infty$.

Примери за групи:

1. Числовите множества $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ са групи спрямо операцията събиране на числа, която ще запишем адитивно с $+$. Наистина,

1) Асоциативността $(a + b) + c = a + (b + c)$ е налице за всеки три числа.

2) Имаме, че $a + 0 = 0 + a = a$ за всяко число a, т.е. 0 играе ролята

[1]За удобство, на повечето места изпускаме знакът на операцията $\cdot$ и вместо $a \cdot b$ пишем просто ab. Този запис на операцията се нарича *мултипликативен*. Ако вместо това е въведена операция със знак $+$, то записът се нарича *адитивен*. Разликата в тези два записа е чисто нотационна и няма отношение към същността на предмета.

на неутрален елемент.

3) За всяко число a знаем, че е изпълнено $a + (-a) = -a + a = 0$, т.е. $-a$ е противоположният елемент на a.

Още повече имаме, че числовите множества образуват абелеви групи, защото е изпълнено и

4) $a + b = b + a$ за всеки две числа a и b.

По-общ пример е всяко числово поле F, $\mathbb{Z} \subseteq F \subseteq \mathbb{C}$ спрямо операцията събиране.

2. Нека F е числово поле и $F^* = F\backslash\{0\}$. Тогава F^* е абелева група относно умножението на числа $\cdot$ в F. Наистина

1) Асоциативността на умножението очевидно е изпълнена с $(ab)c = a(bc)$ за $\forall a, b, c \in F$, а оттам и за $\forall a, b, c \in F^*$.

2) Числото 1 играе ролята на единичен елемент.

3) За всяко число $a \in F*$ числото $\dfrac{1}{a} \in F*$ играе ролята на обратен елемент.

4) Знаем, че е налице комутативност на умножението в F, която се наследява и от F^*.

3. Нека $n \in \mathbb{N}$. Разглеждаме множеството

$$\mathbb{C}_n = \{z \in \mathbb{C} \mid z^n = 1\},$$

състоящо се от n-тите комплексни корени на единицата (уравнението $z^n = 1$ има точно n на брой различни комплексни корена). Тогава $\mathbb{C}_n$ е група относно операцията умножение $\cdot$ на комплексни числа. Наистина, ако $z_1, z_2 \in \mathbb{C}_n$, това означава, че $z_1^n = 1$ и $z_2^n = 1$. Тогава за тяхното произведение $z_1 z_2$ е в сила, че $(z_1 z_2)^n = z_1^n z_2^n = 1.1 = 1$, т.е. $z_1 z_2 \in \mathbb{C}_n$ и $\mathbb{C}_n$ е затворено относно операцията $\cdot$ в $\mathbb{C}$. Сега за трите аксиоми имаме

1) Асоциативността е наследена от асоциативността на $\cdot$ в $\mathbb{C}$.

2) Единичният елемент на групата е $1 \in \mathbb{C}$.

3) За всеки елемент $z \in \mathbb{C}_n$ съществува съответен обратен елемент $\dfrac{1}{z} \in \mathbb{C}_n$, защото от $z^n = 1$ следва и че $\left(\dfrac{1}{z}\right)^n = \dfrac{1}{z^n} = \dfrac{1}{1} = 1$.

Освен това $\mathbb{C}_n$ е абелева, т.к. операцията $\cdot$ в $\mathbb{C}_n$ наследява комутативността на операцията $\cdot$ в $\mathbb{C}$. Ясно е също и че $|\mathbb{C}_n| = n$ е редът на $\mathbb{C}_n$ и следователно $\mathbb{C}_n$ е крайна група.

4. Нека F е произволно числово поле. Тогава множеството

$$GL_n(F) = \{A \in F_{n\times n} \mid \det A \neq 0\},$$

състоящо се от всички неособени квадратни матрици от ред n с елементи от F, е група относно операцията умножение на матрици, наречена *обща линейна група*[2]. Наистина, ясно е, че

1) $(AB)C = A(BC)$ за произволни матрици $A, B, C \in GL_n(F)$, т.к. това е в сила изобщо за проиволни матрици от $F_{n\times n}$.

2) Единичният елемент на групата е единичната матрица E.

3) За всяка матрица $A \in GL_n(F)$ съществува обратна матрица $A^{-1} \in GL_n(F)$ (защото $\det A \neq 0$) с $\det A^{-1} = \dfrac{1}{\det A} \neq 0$, която играе ролята на съответстващия ѝ обратен елемент.

Групата $GL_n(F)$ не е абелева, т.к. знаем, че в общия случай $AB \neq BA$ при $n > 1$.

Нека сега разгледаме множеството

$$SL_n(F) = \{A \in F_{n\times n} \mid \det A = 1\}.$$

То също е група относно умножението на матрици, наречена *специална линейна група*[3]. Наистина, $SL_n(F)$ е затворено относно посочената операция, т.к. за всеки две матрици $A, B \in SL_n(F)$ имаме, че $\det A = 1$ и $\det B = 1$, а оттам и за тяхното произведение AB следва, че $\det(AB) = \det A \det B = 1.1 = 1$ и следователно $AB \in SL_n(F)$. Свойствата от 1) до 3) се изпълняват по същия начин, както при $GL_n(F)$.

5. Нека Ω е някакво множество, а S_Ω е множеството на всички биекции на Ω върху себе си. За произволни биекции $f, g \in S_\Omega$ тяхното произведение $fg : \Omega \longrightarrow \Omega$, дефинирано чрез $(fg)(x) = f\,(g(x))$ за $\forall x \in \Omega$ също е биекция и следователно $fg \in S_\Omega$. Относно тази бинарна операция S_n е група, наречена *симетрична група на множеството* Ω, т.к. е изпълнено

1) $(fg)h = f(gh)$ за $\forall f, g, h \in S_\Omega$.

2) Единичен елемент на групата е идентитетът $\mathrm{id} : \Omega \longrightarrow \Omega$, за който е изпълнено $\mathrm{id}(x) = x$ за $\forall x \in \Omega$. Оттук е ясно, че $f.\mathrm{id} = \mathrm{id}.f = f$ за $\forall f \in S_\Omega$.

---

[2] General linear group

[3] Special linear group

3) За всяка биекция $f \in S_\Omega$ съществува обратно изображение f^{-1}, което също е биекция и следователно $f^{-1} \in S_\Omega$, така че е изпълнено $ff^{-1} = f^{-1}f = \mathrm{id}$.

Нека Ω е крайно множество с n елемента, т.е. мощността му е $|\Omega| = n$. Без ограничение може да считаме, че

$$\Omega = \{1, 2, \ldots, n\}.$$

В такъв случай, за по-голяма яснота и удобство пишем S_n вместо S_Ω и наричаме S_n *симетрична група от степен* n. Нека $f \in S_n$ е такава биекция, че $f(k) = i_k \in \Omega$ за всеки елемент $k \in \Omega$, $1 \leq k \leq n$. Тогава записваме

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix},$$

където поредицата от числа $i_1, i_2, \ldots, i_n$ представлява пермутация на числата $1, 2, \ldots, n$. Знаем, че борят на всички пермутации на числата от 1 до n е $n!$ и следователно S_n е крайна група от ред $|S_n| = n!$, чиито елементи също наричаме пермутации. При $n \geq 3$ S_n е неабелева. Наистина,

$$S_3 = \left\{ \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}}_{=\mathrm{id}}, \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}}_{=a}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}}_{=b} \right\}$$

и нека разгледаме произведенията ab и ba.

$$ab = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Това означава, че $b(1) = 2$ а след това $a(2) = 3$ и така $ab(1) = 3$; $b(2) = 3$, а след това $a(3) = 2$ и следователно $ab(2) = 2$; $b(3) = 1$, а след това $a(1) = 1$ и следователно $ab(1) = 1$. По този начин намерихме, че

$$ab = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

От друга страна

$$ba = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Това означава, че $a(1) = 1$, а след това $b(1) = 2$ и следователно $ba(1) = 2$; $a(2) = 3$, а след това $b(3) = 1$ и следователно $ba(2) = 1$; $a(3) = 2$, а след това $b(2) = 3$ и следователно $ba(3) = 3$. И така намерихме, че

$$ba = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Сега вече е ясно, че $ab \neq ba$ и няма как S_3 да е абелева.

Следствия от аксиомите:

а) Елементът e е единствен. Наистина, нека $e' \in G$ е такъв, че $ae' = e'a = a$ за $\forall a \in G$. Тогава при $a = e$ имаме $ee' = e'e = e$. Но e е единичен елемент и следователно $ee' = e'e = e$. Следователно $e = e'$.

б) За всеки елемент $a \in G$ елементът a^{-1} е единствен. Наистина, нека $a' \in G$ е такъв, че $aa' = a'a = e$. Тогава имаме, че $a' = ea' = (a^{-1}a)a' = a^{-1}(aa') = a^{-1}e = a^{-1}$.

в) Нека $a, b, c \in G$. От асоциативността на операцията (аксиома 1) имаме, че $(ab)c = a(bc)$ и следователно можем да запишем просто abc. По-общо, ако $a_1, a_2, \ldots, a_k \in G$, то елементът $a_1 a_2 \ldots a_k \in G$ е еднозначно определен.

г) За $a \in G$ и $k \in \mathbb{N}$ дефинираме $a^k = \underbrace{aa \ldots a}_{k \text{ пъти}}$. Лесно се вижда, че са в сила свойствата $a^k a^l = a^{k+l}$ и $(a^k)^l = a^{kl}$ за $\forall k, l \in \mathbb{N}$. Считаме, че $a^0 = e$ и дефинираме $a^{-k} = (a^{-1})^k = (a^k)^{-1}$ за произволно $k \in \mathbb{N}$. В такъв случай свойствата $a^k a^l = a^{k+l}$ и $(a^k)^l = a^{kl}$ се обобщават за произволни $k, l \in \mathbb{Z}$. Ако групата G е записана адитивно чрез операцията събиране $+$, то вместо a^k пишем $ka = \underbrace{a + a + \cdots + a}_{k \text{ пъти}}$ за $k \in \mathbb{N}$. По-общо, в сила са свойствата $ka + la = (k + l)a$ и $k(la) = (kl)a$ за $\forall k, l \in \mathbb{Z}$.

Нека множеството G е група относно операцията $\cdot$, а множеството G' е група относно операцията $*$ и $\varphi : G \longrightarrow G'$ е изображение (т.е. на всеки елемент $g \in G$ е съпоставен единствен елемент $\varphi(g) \in G'$. Изображението φ е *хомоморфизъм на групи*, ако

$$\varphi(a \cdot b) = \varphi(a) * \varphi(b) \quad \forall a, b \in G.$$

Свойства:

1. Ако e е единичният елемент на G, а e' е единичният елемент на G', то $\varphi(e) = e'$.

2. $\varphi(a^{-1}) = (\varphi(a))^{-1}$ за $\forall a \in G$.

Ако $\varphi : G \longrightarrow G'$ е хомоморфизъм на групи и освен това φ е биекция на G върху G', то казваме, че φ е *изоморфизъм на групи*. В такъв случай казваме, че групите G и G' са *изоморфни* и пишем $G \cong G'$. Това означава, че G и G' имат едни и същи свойства като групи и често биват отъждествявани.

Нека например разгледаме множеството $\mathbb{R}^+$ на реалните положителни числа и множеството $\mathbb{R}$ на всички реални числа. $\mathbb{R}^+$ е група спрямо умножението на реални числа, а $\mathbb{R}$ е група спрямо събирането на реални числа. Търсим изображение

$$\varphi : \mathbb{R}^+ \longrightarrow \mathbb{R},$$

такова че $\varphi(ab) = \varphi(a) + \varphi(b)$ за $\forall a, b \in \mathbb{R}^+$ и φ да е биекция на $\mathbb{R}^+$ върху $\mathbb{R}$. Такова изображение е например функцията $\ln x$. Наистина, ако $\varphi = \ln$, то φ е биекция и освен това имаме, че $\varphi(ab) = \ln(ab) = \ln a + \ln b = \varphi(a) + \varphi(b)$. По този начин φ е изоморфизъм на групи и $\mathbb{R}^+ \cong \mathbb{R}$.

Нека G е група и $H \subseteq G$ $(H \neq \varnothing)$ е някакво непразно нейно подмножество. Казваме, че H е *подгрупа* на G, ако за $\forall a, b \in H \Rightarrow ab \in H$ и $\forall a \in H \Rightarrow a^{-1} \in H$. С други думи, H е такова подмножество на G, че е затворено спрямо груповата операция в G и освен това съдържа обратните на всички свои елементи. Означаваме $H \leq G$ или $H < G$, когато имаме строгото включване $H \subset G$. Нека $a \in H$. Тогава по дефиниция $a^{-1} \in H$ и $aa^{-1} = e \in H$. По този начин H е група спрямо същата бинарна операция в G.

Ще отбележим още, че сечението на подгрупи на G също е подгрупа на G.

Примери:

1. За всяка група G е очевидно, че $G \leq G$ и $\{e\} \leq G$ и това са тривиалните подгрупи на G.

2. $\mathbb{R}$ е подгрупа на $\mathbb{C}$ относно операцията събиране.

3. $SL_n(F) < GL_n(F)$.

4. В множеството на целите числа $\mathbb{Z}$, което е група относно операция-

та събиране, за произволно цяло число $m \in \mathbb{Z}$ разглеждаме множеството

$$m\mathbb{Z} = \{mz \mid z \in \mathbb{Z}\}.$$

При $m = 0$, имаме че $m\mathbb{Z} = \{0\}$, а при $m = \pm 1$ очевидно $m\mathbb{Z} = \mathbb{Z}$. За всички останали $m \in \mathbb{Z}\backslash\{0, \pm 1\}$ се получават нетривиални подгрупи на $\mathbb{Z}$. Например при $m = 2$ имаме, че $m\mathbb{Z} = \{$всички четни числа$\}$. И така, за провизолно $m \in \mathbb{Z}$ и произволно $mz \in m\mathbb{Z}$ имаме, че $-mz = m(\underbrace{-z}_{\in\mathbb{Z}}) \in m\mathbb{Z}$; за провизолни $mz_1, mz_2 \in m\mathbb{Z}$ имаме, че $mz_1 + mz_2 = m(\underbrace{z_1 + z_2}_{\in\mathbb{Z}}) \in m\mathbb{Z}$ и следователно $m\mathbb{Z} \leq \mathbb{Z}$.

5. Знаем че $\mathbb{C}_n = \{z \in \mathbb{C} \mid z^n = 1\}$ е абелева група от ред n спрямо умножението на комплексни числа. Нека $d \in \mathbb{N}$ и разгледаме множеството $\mathbb{C}_d = \{z \in \mathbb{C} \mid z^d = 1\}$. Ако $d \mid n$, то за произволен елемент $z \in \mathbb{C}_d$ имаме, че $z^d = 1$ и след повдигане на двете страни на степен $\frac{n}{d}$ получаваме, че $z^n = 1$, т.е. $z \in \mathbb{C}_n$. По този начин видяхме, че ако $d \mid n$, то $\mathbb{C}_d \subseteq \mathbb{C}_n$. Оттук директно се проверява и че $\mathbb{C}_d \leq \mathbb{C}_n$.

Свойство:

Нека G е група, $H \leq G$ и $a, b \in G$. Тогава, ако $ab \in H$ и $a \in H$, то $b \in H$. Наистина, щом $a \in H$, то тогава $a^{-1} \in H$. Оттук $a^{-1}(ab) \in H$ и $(a^{-1}a)b \in H$, което просто означава, че $eb = b \in H$. Аналогино се проверява и че, ако $ab \in H$ и $b \in H$, то $a \in H$.

Теорема на Кейли. *Всяка група от ред n е изоморфна на подгрупа на симетричната група S_n.*

Доказателство. Нека G е група от ред $|G| = n$. По-точно

$$G = \{g_1, g_2, \ldots, g_n\}.$$

Ще докажем, че G е подгрупа на S_G (симетричната група на множеството G) и от факта, че отъждествяваме S_G с S_n, теоремата ще бъде доказана. Нека $a \in G$ е произволен елмент. Разглеждаме изображението

$$L_a : G \longrightarrow G,$$

за което $L_a(x) = ax$ за $\forall x \in G$.

L_a е биекция на G върху G. Наистина, нека $y \in G$ е прозиволен елемент. Тогава $x = a^{-1}y \in G$ и имаме, че $L_a(x) = ax = a(a^{-1}y) = y$, т.е. всеки елемент $y \in G$ е образ на елемента $x \in G$ и по този начин L_a е сюрекция. Нека $x_1, x_2 \in G$ са такива, че $x_1 \neq x_2$. Ако допуснем, че $L_a(x_1) = L_a(x_2)$, то имаме че $ax_1 = ax_2$ и след ляво умножение с a^{-1} достигаме до противоречието, че $x_1 = x_2$. Следователно $L_a(x_1) \neq L_a(x_2)$ и L_a е инекция.

Сега ще докажем, че $G \leq S_G$. Ако $a, b \in G$, то имаме $(L_aL_b)(x) = L_a(L_b(x)) = L_a(bx) = a(bx) = (ab)x = L_{ab}(x)$. За $\forall a \in G$ е изпълнено, че $L_aL_{a^{-1}}(x) = L_{aa^{-1}}(x) = (aa^{-1})x = x$, т.е. $L_{aa^{-1}} = \mathrm{id}$ и $(L_a)^{-1} = L_{a^{-1}}$. Така $L_a \in S_G$ за $\forall a \in G$. Нека $G' = \{L_a \mid a \in G\}$. Тогава $G' \subseteq S_G$, $L_aL_b = L_{ab}$ (затвореност на G' относно композицията на изображения) и $(L_a)^{-1} = L_{a^{-1}} \in G'$ (затвореност относно обръщането на елементи) и следователно $G' \leq S_G$.

Нека разгледаме изображението

$$\varphi : G \longrightarrow G',$$

за което $\varphi(a) = L_a$. От това, което видяхме досега имаме, че $\varphi(ab) = L_{ab} = L_aL_b = \varphi(a)\varphi(b)$ за $\forall a, b \in G$. Това означава, че φ е хомоморфизъм на групи. Ще видим още, че φ е биекция. Наистина, всеки елемент $L_a \in G'$ е образ на елемента $a \in G$ под действието на φ и φ е сюрекция. Ако $a, b \in G$ са такива, че $a \neq b$, то допускането $\varphi(a) = \varphi(b)$ означава, че $L_a = L_b$ като изображения. Тогава $L_a(x) = L_b(x)$ за $\forall x \in G$ и в частност при $x = e$ имаме, че $L_a(e) = L_b(e)$, което води до противоречието $a = b$. Следователно $L_a \neq L_b$, а оттам и $\varphi(a) \neq \varphi(b)$ и φ е инекция. Дотук видяхме, че φ е хомоморфизъм на групи и φ е биекция, което означава, че φ е изоморфизъм на групи. Така $G \cong G'$, но $G' \leq S_G$. Така може да считаме, че $G \leq S_G$, а т.к. $S_G \cong S_n$ и че $G \leq S_n$. По този начин доказахме, че G е подгрупа на S_n. $\square$