Групи-определение, примери, свойства

Сайт: learn.fmi.uni-sofia.bg
Курс: Алгебра 2, поток 1, летен семестър 2021/2022
Книга: Групи-определение, примери, свойства
Разпечатано от: Мартин Попов
Дата: Thursday, 24 March 2022, 21:26

Съдържание

1. Групи - определение и примери

Едно от основните понятия в съвременната алгебра е понятието за група.
Групата е алгебрична структура с една бинарна операция. Оказва се, че теорията на групите има множество приложения в различни клонове на науката - освен в другите области на математиката и информатиката, групите се използват във физиката , химията, биология и други. Първите резултати в тази област са от края на 18-ти век и началото на 19-ти век. Корените за разглежданията в теорията на групите са от една страна разглежданията на пермутационните групи, а от втора страна групите свързани с геометрията и освен това групите във връзка с теория на числата.

1.1. бинарна операция

Определение:
Нека M е непразно множество. Ще казваме, че в множеството M е зададена *бинарна операция*, когато на всяка наредена двойка елементи от множеството M е съпоставен елемент, който принадлежи на същото множество M

$$\begin{array}{rcl} \varphi : M \times M & \rightarrow & M \\ & \varphi & \\ a, b & \rightarrow & c \end{array}, \text{ където } a \in M,\ b \in M,\ c \in M$$

Примери:
Събирането $a + b$ и умножението $a.\,b$ на цели числа са примери на бинарни операции. Делението $a : b$ на цели числа *не е* бинарна операция, защото на нула не се дели (вторият аргумент не може да бъде 0), а освен това много често частното на две цели числа не е цяло число (например $5 : 3 \notin \mathbb{Z}$).

В алгебрата, обикновено не се използва функционалния запис на бинарната операция. Съгласно традицията, записването на бинарните операции се извършва като знакът съответстващ на бинарната операция се поставя между двата аргумента, например част от бинарните операции ще записваме по следните начини:
$a + b$, $a - b$, $a.\,b$, $a * b$, $a \circ b$, $a \oplus b$, $a \odot b$.

1.2. група - опр

При определянето на понятието група са използвани основните свойства на числата, известни ни от училище, които видяхме че се пренасят като основни свойства на събирането на $n-$мерни вектори и на събирането на матрици.

Отределение:
Нека G е непразно множество, в което има дефинирана бинарна операция - условно ще я записваме като $" * "$, т. е. определено е $a * b$ за произволни $a, b \in G$. Казваме, че G е група относно въведената операция, когато са изпълнени следните свойства (аксиоми):

- $(a * b) * c = a * (b * c),\ \forall a, b, c \in G$ - (*асоциативност*);
- съществува $e \in G$, за който $a * e = e * a = a,\ \forall a \in G$ (*неутрален елемент*);
- за всеки $a \in G$ съществува $b \in G$, за които $a * b = b * a = e$ (*симетричен елемент относно операцията*).

Когато искаме да уточним, че G е група относно операцията $" * "$, записваме по следния начин $(G, *)$.

Определение:
Ако в групата G е изпълнен комутативния закон $a * b = b * a,\ \forall a, b \in G$, тогава групата се нарича абелева или комутативна.

Комутативните групи се наричат абелеви в чест на норвежския математик от 19-ти век Нилс Абел.

1.3. примери - 1

Примери (числови адитивни групи):

Известните числови множества, които образуват абелеви групи относно събирането са: множеството на целите числа $(\mathbb{Z},+)$ множеството на рационалните числа $(\mathbb{Q},+)$, на реалните числа $(\mathbb{Z},+)$ и на комплексните числа $(\mathbb{C},+)$. За тези числови множества числото 0 е неутрален елемент относно събирането и за всяки число b съществува симетричен елемент относно събирането, което е точно противоположното $-b$ число и за тях е изпълнено $b+(-b)=0$. Всички тези групи са абелеви защото изпълняват комутативния закон.

Ясно е, че естествените числа $\mathbb{N}$ не образуват група относно събирането, защото неутралнията елемент 0 не принадлежи на $\mathbb{N}$, а също така противоположните числа на естествените числа не са естествени числа, т. е. в множеството на естествените числа няма симетрични относно събирането и не е изпълнена аксиома 3 на определението за група.

Пример (адитивна група):

Нека V е линейно пространство над поле F. Съгласно определението за линейно пространство събирането е бинарна операция във V, която е комутативна и асоциативна операция, съществува неутрален елемент (нулевия елемент от V) и за всеки елемент от V има противоположен елемент. Следователно множеството от всички вектори от линейно пространство V, образува абелева група относно събирането. По този начин получаваме в частност, че всички матрици от един тип образуват $M_{n\times k}(F)$ адитивна абелева група. По същия начин виждаме, че всички полиноми $\mathbb{R}[x]$ също образуват абелева група относно събирането.

Примери (числови мултипликативни групи):

Известно е, че на нула не се дели и ако искаме да разглеждаме групи с операцията умножение, които са съставени от числа, то нулата не трябва да принадлежи на разглежданото множество. Да разгледаме множеството от всички рационални числа без нулата $\mathbb{Q}^*=\mathbb{Q}\setminus\{0\}$, или от всички реални числа без нулата $\mathbb{R}^*=\mathbb{R}\setminus\{0\}$, или от всички комплексни числа без нулата $\mathbb{C}^*=\mathbb{C}\setminus\{0\}$. Произведението на две числа от някое от тези множества е число, което е елемент на същото множество, освен това за числото 1 е изпълнено $1.a=a$ и затова 1 е неутрален елемент относно умножението и принадлежи на всяко от изброените множества и обратният елемент a^{-1} за произволен елемент a от изброените множества също принадлежи на тях. По този начин установяваме, че $(\mathbb{Q}^*,.)$ $(\mathbb{R}^*,.)$ $(\mathbb{C},.)$ образуват абелеви мултипликативни групи.

Умножението е асоциативна операция в множеството на целите числа, $1\in\mathbb{Z}$, но единствените цели числа, на които обратните числа също са цели са $1,-1$. Умножението е бинарна операция за множеството $\mathbb{Z}^*=\{1,-1\}$ и получаваме, че $(\mathbb{Z}^*,.)$ е мултипликативна абелева група, която съдържа само два елемента.

Ако разгледаме множеството $E=\{1\}$ състоящо се само от числото 1, виждаме че се образува абелева група относно умножението и $(E,.)$ е група която съдържа възможно най-малко елементи - само един елемент.

1.4. пример - GL(n,F)

Нека да разгледаме множеството от всички квадратни матрици $M_{n\times n}(\mathbb{R})$. От курса по линейна алгебра, знаем че при умножението на квадратни матрици $n\times n$ се получава матрица от същия тип, т.е. умножението е бинарна операция за $M_{n\times n}(\mathbb{R})$. Доказали сме асоциативността на умножението, както и че за единичната матрица E е изпълнено $A.E=E.A=A$, където $A\in M_{n\times n}(\mathbb{R})$ е произволна матрица. Но множеството от всички квадратни матрици $M_{n\times n}(\mathbb{R})$ не е група относно умножението защото не всяка матрица е обратима.

Знаем, че една матрица A е обратима, когато има ненулева детерминанта $\det(A)\neq 0$ и освен това е изпълнено, че $\det(A.B)=\det(A).\det(B)$ и произведението на две обратими матрици също е обратима матрица. Ако F е произволно поле, разглеждаме множеството от всички обратими $n\times n$ матрици с елементи от F

$$GL_n(F)=GL(n,F)=\{A\in M_{n\times n}(F)\mid \det(A)\neq 0,\ \ \text{т.е. } A \text{ е обратима }\}.$$

Множеството $GL_n(F)$ е група относно умножението, защото в него умножението е бинарна операция, единичната матрица принадлежи на $GL_n(F)$ и обратната на всяка обратима матрица също е обратима. Известно ни е, че при $n\geq 2$ умножението на матрици е некомутативно и затова обратимите матрици формират некомутативна група с операцията умножение. Тази група се нарича пълна линейна група от степен n над полето F (general linear group).

1.5. пример - групата Z_n

Нека $n>1$ е естествено число. Ако $0 \leq k<n$ тогава k възможен остатък при делене на n и нека със $\bar{k}=\{k+ns \mid s \in \mathbb{Z}\}$ отбележим всички цели числа, които имат остатък k при разделяне на n, това множество често се нарича клас остатъци. Разглеждаме съвкупността от всички класове остатъци при делене на n:

$$\mathbb{Z}_n=\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$$

В множеството $\mathbb{Z}_n$, може да се дефинира събиране по следния начин .

$$\bar{a}+\bar{c}=\bar{r}, \quad \text{където } a+c=qn+r, \ \ 0 \leq r<n$$

Изпълнено е, че събирайки произволен елемент от класа $\bar{a}$ със произволен елемент от $\bar{c}$ винаги се получава елемент, който е от класа остатъци $\bar{a}+\bar{c}=\bar{r}$:

$$\left.\begin{array}{lll} a_1 \in \bar{a} & \Leftrightarrow & a_1=a+ns_1 \\ c_1 \in \bar{c} & \Leftrightarrow & a_2=a+ns_2 \end{array}\right\} \Longrightarrow a_1+c_1=a+c+n(s_1+s_2)=r+n(q+s_1+s_2) \in \bar{r}$$

Установяваме, че събирането е бинарна операция в множеството от класове остатъци по модул n. Освен това за събирането на цели числа са изпълнени комутативност и асоциативност, затова тези закони важат и за класовете остатъци по модул n

$$\left.\begin{array}{rcl} a+c=c+a & \Rightarrow & \bar{a}+\bar{c}=\bar{c}+\bar{a} \\ (a+c)+g=a+(c+g) & \Rightarrow & (\bar{a}+\bar{c})+\bar{g}=\bar{a}+(\bar{c}+\bar{g}) \end{array}\right. , \quad \forall\, \bar{a}, \bar{c}, \bar{g} \in \mathbb{Z}_n$$

Освен това е изпълнено, че $\bar{0}+\bar{a}=\bar{a}$ и по този начин се вижда, че множеството от класовете остатъци $\mathbb{Z}_n$ е група относно операцията събиране. Това е пример на крайна абелева група, която се нарича адитивната група от класовете остатъци по модул n.
Например, таблицата за събиране в групата $(\mathbb{Z}_7,+)$ е следната:

събиране в $\mathbb{Z}_7$:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

1.6. пример - S_n

Нека $M \neq \emptyset$ е непразно множество и със $S(M)$ да означим множеството от всички биективни изображения в множеството M.

$$S(M) = \{\varphi \mid \varphi : M \to M, \varphi - \text{биекция}\}$$

Множеството $S(M)$ от биекциите се разглежда с операцията композиция на изображения "$\circ$":

$$(\varphi \circ \psi)(x) = \varphi(\psi(x)) \ , \ \forall x \in M.$$

За композицията на изображения са в сила свойствата:

- Установява се, че $\varphi \circ \psi$ е *биекция* на множеството M и принадлежи на множеството $S(M)$, което означава че композицията е бинарна операция за множеството $S(M)$.
- Аасоциативността на композицията на изображения е в сила за произволни изображения $\varphi, \ \psi, \ \tau$ на множеството M, защото за произволен $x \in M$ е изпълнено

$$\begin{array}{l} (\varphi \circ \psi) \circ \tau(x) = \varphi \circ \psi(\tau(x)) = \varphi(\psi(\tau(x))) \\ \varphi \circ (\psi \circ \tau)(x) = \varphi(\psi \circ \tau)(x) = \varphi(\psi(\tau(x))) \end{array} \Rightarrow (\varphi \circ \psi) \circ \tau = \varphi \circ (\psi \circ \tau)$$

- Изображението идентитет $\mathtt{id} : M \to M$, за което е изпълнено $\mathtt{id}(x) = x, \forall x \in M$ е неутрален елемент, относно операцията композиция, защото $\varphi \circ \mathtt{id} = \varphi = \mathtt{id} \circ \varphi$.
- Ако изображението φ е биективно изображение, тогава е известно че съществува неговото обратно изображение φ^{-1} и е изпълнено $\varphi \circ \varphi^{-1} = \mathtt{id} = \varphi^{-1} \circ \varphi$.

Получихме, че множеството $S(M)$ от всички биекции на зададено множество M, разглеждано относно операцията композиция на изображения удовлетворява условията от определението за група $(S(M), \circ)$. Тази група се нарича **симетрична група за множеството** M, а в случая когато множеството M е крайно с n елемента групата се бележи S_n и се нарича симетрична група от степен n.

- В случая когато множеството има само един елемент $|M| = 1$, тогава за всяко биективно изображение $\varphi : M \to M$ е изпълнено $\varphi = \mathtt{id}$, и затова $|S_1| = 1$ и групата S_1 е Абелева.
- В случай когато $|M| = 2$, например $M = \{a, b\}$, да разгледаме биективно изображение $\varphi : M \to M$, което е различно от идентитета $\varphi \neq \mathtt{id}$. Единствената възможност е φ да действа по следния начин $\left| \begin{array}{l} \varphi(a) = b \\ \varphi(b) = a \end{array} \right.$ и всички елементи на групата са $\{\mathtt{id}, \varphi\} = S(M) = S_2$. Непосредствено проверяваме, че е изпълнено $\varphi^2 = \varphi \circ \varphi = \mathtt{id}$ и групата S_2 е Абелева.
- Ако $|M| > 2$, тогава групата $S(M)$ не е комутативна (не е Абелева). Нека $a, \ b, \ c$ са три различни елемента от множеството. Да разгледаме следните две изображения на M:

$$\left| \begin{array}{l} \varphi(a) = b \\ \varphi(b) = a \\ \varphi(x) = x, \ \forall x \neq a, x \neq b \end{array} \right. \qquad \left| \begin{array}{l} \psi(b) = c \\ \psi(c) = b \\ \psi(y) = y, \ \forall y \neq b, y \neq c \end{array} \right.$$

Пресмятаме по какъв начин действа $\varphi \circ \psi$:

$$\left| \begin{array}{l} \varphi \circ \psi(a) = \varphi(\psi(a)) = \varphi(a) = b, \\ \varphi \circ \psi(b) = \varphi(\psi(b)) = \varphi(c) = c, \\ \varphi \circ \psi(c) = \varphi(\psi(c)) = \varphi(b) = a, \\ \varphi \circ \psi(x) = \varphi(\psi(x)) = \varphi(x) = x, \ \forall x \ , \{x \neq a, x \neq b, x \neq c\} \end{array} \right.$$

Аналогичнор за $\psi \circ \varphi$ получаваме:

$$\left| \begin{array}{l} \psi \circ \varphi(a) = \psi(\varphi(a)) = \psi(b) = c, \\ \psi \circ \varphi(b) = \psi(\varphi(b)) = \psi(a) = a, \\ \psi \circ \varphi(c) = \psi(\varphi(c)) = \psi(c) = b, \\ \psi \circ \varphi(x) = \psi(\varphi(x)) = \psi(x) = x, \ \forall x \ , \{x \neq a, x \neq b, x \neq c\} \end{array} \right.$$

Получихме, че $\psi \circ \varphi \neq \varphi \circ \psi$, откъдето се установява, че групата $S(M)$ е некомутативна, когато $|M| > 2$, и в частност S_n не е Абелева за $n \geq 3$.

Нека множеството M е крайно и има n елемнта. Можем да номерираме тези числа и да считаме, че $M=\{1,2,\dots,n\}$ и ще изразяваме по какъв начин елементите на S_n действат върху номерата на елементите. По този начин всяка една биекция φ от симетричната група може да се напише еднозначно по следния начин:

$$\varphi=\begin{pmatrix}1 & 2 & \dots & n\\ i_1 & i_2 & \dots & i_n\end{pmatrix},\ \text{където } i_1=\varphi(1),\ i_2=\varphi(2),\dots,i_n=\varphi(n).$$

Елементът $\varphi=\begin{pmatrix}1 & 2 & \dots & n\\ i_1 & i_2 & \dots & i_n\end{pmatrix}$, изобразява по какъв начин действа биекцията φ върху $M=\{1,2,\dots,n\}$ и затова числата $i_1,i_2,\dots,i_n$ са различни помежду си и представляват пермутация на $1,2,\dots,n$. По този начин получаваме, че $|S_n|=n!$.

2. Групи - основни свойства

Използвайки единствено аксиомите от определението за групи се получават множество следствия, които повтарят добре известни свойства на действията с числа.

Голяма част от използваните наименованя при групите са в пряка зависимост от символа за означаване на операцията в групата. Имената са съобразени с традиционно използваните в математиката знаци за събиране и умножение, а именно:

	адитивна група	**мултипликативна група**
знак	"$+$" или $\oplus$	"$.$" или $\odot$ (или $\circ$)
аргументи	събираеми	множители
резултат	сума	произведение, (композиция)
неутрален елемент	0 нула, нулев елемент	e; E; 1 (или id) единица (или идентитет)
симетричен елемент	$-a$ противоположен елемент	a^{-1} обратен елемент
кратност/ степен	$k(a) = \underbrace{a + \ldots + a}_{k}$ k кратно на a	$a^k = \underbrace{a.\ldots.a}_{k}$ $k-$та степен на a

2.1. свойства 1

Твърдение:
Ако $(G,*)$ е група, тогава са изпълнени следните основни свойства:

1. Неутралният елемент на групата е единствения, за който е изпълнено $a*e=e*a=a, \ \ \forall a\in G$.
2. За всеки елемент $a\in G$ има единствен елемент $b=b_a\in G$, който е симетричен относно операцията и за който е изпълнено $a*b_a=b_a*a=e$.
3. За произволни елементи $a,b\in G$, всяко едно от уравненията $a*x=b$ и $y*a=b$ има по единствено решение (*решенията на двете уравнения могат да бъдат различни*).

Доказателство:

1. Допускаме, че съществуват два неутрални елемента e_1 и e_2 и за всеки един от тях е изпълнено $a*e_i=e_i*a=a$, където $a\in G$ е произволен елемент. Тогава е изпълнено

$$e_1=e_1*e_2=e_2 \implies e_1=e_2.$$

   Получи се че в групата има единствен неутрален елемент. В случая когато групата е записана адитивно, неутралния елемент се нарича нула, а в случая на мултипликативен запис неутралния елемент се нарича единица (единичен елемент). При групи от изображения неутралния елемент се нарича идентитет.
2. Допускаме, че за елемент $a\in G$ съществуват два симетрични елемента относно операцията b_1 и b_2. Като се използва асоциативния закон се получава, че тези елементи съвпадат:

$$b_1=b_1*e=b_1(a*b_2)=(b_1*a)*b_2=e*b_2=b_2 \implies b_1=b_2$$

   Установихме, че за елемента $a\in G$ в групата има единствен симетричен елемент относно операцията. В случая когато групата е записана адитивно, симетричния елемент на a се нарича противоположен и се отбелязва като $-a$, а в случая на мултипликативен запис симетричния елемент се нарича обратен на елемента и се отбелязва с a^{-1}.

\item {Нека $a,c\in G$ са произволни елементи и с $a^{\triangledown}$ да бележим симетричния елемент на a спрямо операцията, за който $a*a^{\triangledown}=a^{\triangledown}*a=e$. Тогава, като умножим уравнението $a*x=b$ от лявата страна по $a^{\triangledown}$ получаваме, че ако това уравнение има решение, тогава то е равно на $a^{\triangledown}*b$, освен това с директно заместване на x със този елемент установяваме, че единственото решение на уравнението $a*x=b$ е равно на $x=a^{\triangledown}*b$.

$$\begin{aligned}&a*(a^{\triangledown}*b)=(a*a^{\triangledown})*b=e*b=b\Longrightarrow x=a^{\triangledown}*b \text{ е решение}\\&a*x=b\Rightarrow a^{\triangledown}*(a*x)=a^{\triangledown}*b\Rightarrow x=a^{\triangledown}*b\ \Rightarrow \text{ единствено решение}\end{aligned}$$

За да получим решение на $y*a=b$ трябва да умножим уравнението от дясната страна по $a^{\triangledown}$ - симетричния елемент на a, тогава се установява, че $y*a=b$ има единствено решение, равно на $y=b*a^{\triangledown}$.

$$\begin{aligned}&(b*a^{\triangledown})*a=b*(a^{\triangledown}*a)=b\Longrightarrow y=b*a^{\triangledown} \text{ е решение}\\&y*a=b\Rightarrow (y*a)*a^{\triangledown}=b*a^{\triangledown}\Rightarrow y=b*a^{\triangledown}\ \Rightarrow \text{ единствено решение}\end{aligned}$$

Да обърним внимание, че решенията на двете уравнения са записани различно и в общия случай при некомутативна група са различни. }
\end{enumerate}.
\end{proof}

2.2. свойства 2

Въпреки, че смисъла е един и същи, в зависимост от вида на групата - с адитивен или мултипликативен запис, изписването на свойствата от следващото твърдение изглежда по различен начин.

Твърдение:
Във всяка група са изпълнени следните основни свойства:

в случай на адитивна група $(L,+)$	**при мултипликативна група** $(G,.)$
1) $-(-a)=a;$	1) $(a^{-1})^{-1}=a;$
2) $-(a+b)=(-b)+(-a);$	2) $(a.b)^{-1}=b^{-1}.a^{-1};$
3) уравнението $a+x=b$ има единствено решение $x=(-a)+b$;	3) уравнението $a.x=b$ има единствено решение $x=a^{-1}.b$;
4) уравнението $y+a=b$ има единствено решение $y=b+(-a)$.	4) уравнението $y.a=b$ има единствено решение $y=b.a^{-1}$.

Доказателство:
1. Свойството следва от единствеността на обратния (или противоположен) елемент.
2. Следва със директна проверка. Например в адитивния случай имаме:

$$\text{при } (L,+):\ \begin{cases}(a+b)+(-b)+(-a)=a+(b+(-b))+(-a)=a+(-a)=0\\(-b)+(-a)+(a+b)=(-b)+(-a+a)+b=(-b)+b=0\end{cases}$$

Аналогична е провеката в мултипликативния случай

$$\text{при } (G,.):\ \begin{cases}(a.b).(b^{-1}.a^{-1})=a.(b.b^{-1}).a^{-1}=a.a^{-1}=e\\(b^{-1}.a^{-1}).(a.b)=b^{-1}.(a^{-1}.a).b=b^{-1}.b=e\end{cases}$$

3. Когато имаме адитивна група (L,+) и искаме да решим уравнението $a+x=b$, трябва да прибавим от двете страни на равенството противоположния елемент $-a$ и то трябва да го прибавим от лявата страна на равенството за да бъдат елементите a и $-a$ един до друг с цел да замести тяхната сума с 0. Получаваме, че ако това уравнение има решение, тогава то е равно на $(-a)+b$, освен това с директно заместване на x със този елемент установяваме, че единственото решение на уравнението $a+x=b$ е равно на $x=(-a)+b$.

$$a+(-a+b)=(a+(-a))+b=0+b=b \Longrightarrow x=-a+b \text{ е решение}$$
$$a+x=b\Rightarrow -a+(a+x)=-a+b\Rightarrow x=-a+b \ \Rightarrow \text{е единствено решение}$$

Аналогично се получава при мултипликативно записана група.

4. Когато имаме мултипликативна група (G,.), за да получим решение на $y.a=b$ трябва да умножим уравнението от дясната страна по a^{-1} - обратния елемент на a и тогава се установява, че $y.a=b$ има единствено решение, равно на $y=b.a^{-1}$.

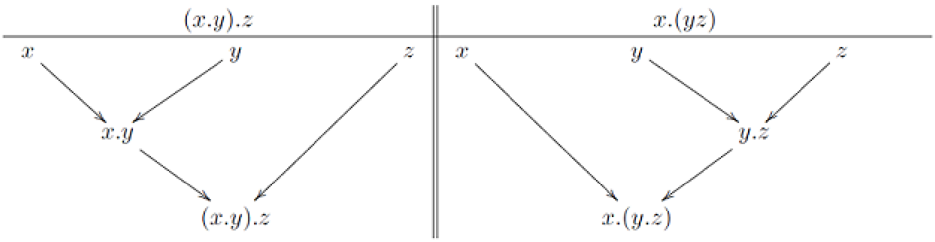
$$(b.a^{-1}).a=b.(a^{-1}.a)=b\Longrightarrow y=b.a^{-1} \text{ е решение}$$
$$y.a=b\Rightarrow (y.a)*a^{-1}=b.a^{-1}\Rightarrow y=b.a^{-1} \ \Rightarrow \text{ единствено решение}$$

Аналогично е и при адитивна група.

Да обърним внимание, че решенията на двете уравнения са записани различно и в общия случай при некомутативна група решенията на двете уравнения са различни.

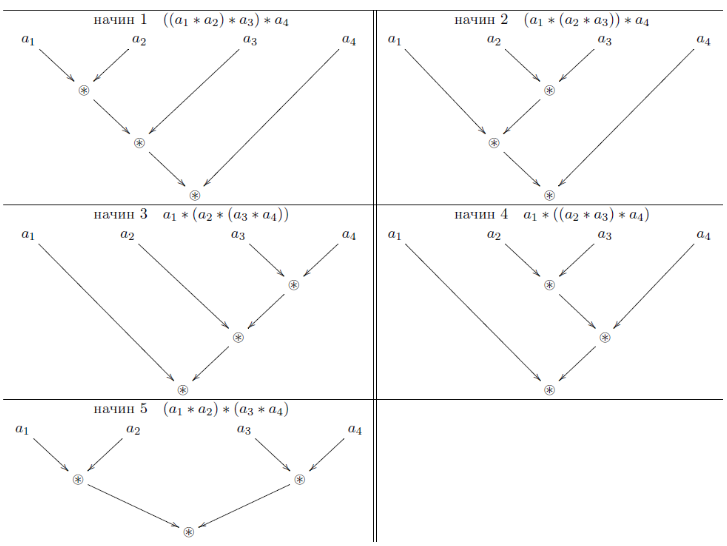
2.3. обобщена асоциативност

Бинарната операция в групата е операция на два аргумента. Когато искаме да приложим такава операция към повече аргументи ще трябва да се извършат няколко последователни действия, като последователността на извършване на тези и действия се задава от резположените скоби.
Например при три аргумента има два начина на разполагана на скобите е които съответстват на два пътя за извършване на действията, които схематично могат да се изразят по следния начин



Асоциативния закон ни постановява че по който и от двата начина да се извършат действията получения резултат е един и същи.

При нарастване броя на аргументите които искаме да бъдат използвани, нараства и броя възможни начини на ръзполагане на скобите и съответсващите им начини на извършване на действията. Например при четири аргумента имаме пет начина за разполагане на скобите, които съответстват на следните схеми



Твърдение (обобщена асоциативност):
Нека $a_1, a_2, \ldots, a_t$ са произволни елементи от група $(G, *)$. Ако без да се променя реда на множителите в израза $a_1 * a_2 * \ldots * a_t$ се разположат скобите по произволни начини, тогава винаги се получава еднакъв резултат.
Доказателство: При доказателството се изпълзва само асоциативността на операцията в групата.
Нека $a_1, a_2, \ldots, a_t \in G$ са произволни и да отбележим с $h(a_1, \ldots, a_n)$ резултатът, който се получава при разполагането на скобите, така че първо да се приложи операцията върху a_1 и a_2, после операцията се прилага врху получения резултат и следващия елемент a_3 и така нататък, като накрая се прилага действието върху резултата от предните елементи и a_t.

$$\begin{array}{rcl} h(a_1, a_2, \ldots, a_{t-1}, a_t) & = & (\ldots((a_1 * a_2) * a_3) * \ldots a_{t-1}) * a_t \\ h(a_1, a_2, \ldots, a_{t-1}, a_t) & = & h(a_1, a_2, \ldots, a_{t-1}) * a_t \end{array}.$$

Да обърнем внимание, че от последното равенство функцията h на n аргумента може да се изрази рекурсивно чрез стойността на h на $n-1$ аргумента. Ще докажем, следното твърдение:

При $t \geq 2$ и при произволно разполагане на скоби в израза $a_1 * \ldots * a_t$, резултата винаги е равен на $h(a_1, \ldots, a_n) = (\ldots((a_1 * a_2) * a_3) * \ldots a_{t-1}) * a_t$.

Доказателството се извършва с индукция по $t \geq 3$.

- В случая $t = 2$ няма какво да се доказва, а в случая $t = 3$ твърдението следва от асоциативния закон $a_1 * (a_2 * a_3) = (a_1 * a_2) * a_3 = h(a_1, a_2, a_3)$.
- Нека $t \geq 3$ и да предположим, че твърдението е изпълнено за всички естествени числа k, за които $3 \leq k \leq t$.
- Разглеждаме произведение $f(a_1, \ldots, a_{t+1})$, в което скобите са разположени по произволен начин. Нека скобите, съответстващи на последното произведение, което трябва да бъде извършено да се намират между a_s и a_{s+1}, това означава, че f може да се представи като произведение на две функции - първата зависеща от аргументите $a_1, \ldots, a_s$, а втората функция е функция на следващите останали аргументи.

$$f(a_1, \ldots, a_{t+1}) = l(a_1, \ldots, a_s).\, r(a_{s+1}, \ldots, a_{t+1})$$

  - Когато $s < t$, прилагаме двукратно индукционното предположение и прилагаме рекуренсивното свойството на функцията h, както и асоциативния закон получаваме

$$\begin{aligned} f(a_1, \ldots, a_{t+1}) &= l(a_1, \ldots, a_s) * r(a_{s+1}, \ldots, a_{t+1}) = \\ &= l(a_1, \ldots, a_s) * h(a_{s+1}, \ldots, a_{t+1}) = \\ &= l(a_1, \ldots, a_s) * (h(a_{s+1}, \ldots, a_t) * a_{t+1}) = \\ &= (l(a_1, \ldots, a_s) * h(a_{s+1}, \ldots, a_t)) * a_{n+1} = \\ &= h(a_1, \ldots, a_t) * a_{t+1} = \\ &= h(a_1, \ldots, a_t, a_{t+1}) \end{aligned}$$

  - В случая, когато $s = t$, директно прилагаме индукционното предположение за $l(a_1, \ldots, a_t)$ и получаваме търсеното равенство

$$\begin{aligned} f(a_1, \ldots, a_{t+1}) &= l(a_1, \ldots, a_t) * a_{t+1} = \\ &= h(a_1, \ldots, a_t) * a_{t+1} = h(a_1, \ldots, a_{t+1}) \end{aligned}$$

2.4. степен/ кратно

Твърдение (степен (кратно) на елемент от група):
Нека $n > 2$ е естествено число, тогава:

- Ако $(G, .)$ е мултипликативна група и $a \in G$, тогава елемента $a^n = \underbrace{a. \ldots . a}_{n}$ се нарича $n-$ та степен на $a \in G$ и за степените на елементите вгрупата са изпълнени свойствата:

$$\begin{array}{l} a^{n+k} = a^n . a^k \\ (a^n)^k = a^{nk} \end{array}, \quad n, k \in \mathbb{N}$$

- Ако $(L+)$ е адитивна група и $x \in L$, тогава елемента $n(x) = \underbrace{x + \ldots + x}_{n}$ се нарича $n-$ кратно на $x \in L$ и за кратните са изпълнени:

$$\begin{array}{l} (n+k)(x) = n(x) + k(x) \\ k(n(x)) = (kn)(x) \end{array} \quad n, k \in \mathbb{N}$$

Доказателство:
В случая на мултипликативна група $(G, .)$, като резултат от обобщената асоциативност получаваме, че в произведението $a^n = \underbrace{a. \ldots . a}_{n}$ няма нужда от поставяне на скоби, защото винаги се получават еднакви стойности. Тогава

$$a^n . a^k = \underbrace{a. \ldots . a}_{n} . \underbrace{a. \ldots . a}_{k} = \underbrace{a. \ldots . a}_{n+k} = a^{n+k}$$

$$(a^n)^k = \underbrace{(\underbrace{a. \ldots . a}_{n}) . \ldots . (\underbrace{a. \ldots . a}_{n})}_{k} = \underbrace{a. \ldots . a}_{k.n} = a^{n.k}$$

Аналогични е доказателството, когато групата е записана адитивно.

Това са добре познатите ни от училище свойства на степенуването. Да обърнем внимание, че в общия случай, при некомутативна група единственото нещо, което можем да напишем за степента $(a * b)^k$ е следното:

$$(a * b)^k = \underbrace{(a * b) * \ldots * (a * b)}_{k} \neq a^k * b^k$$

3. подгрупа

Определение:
Нека $(G, *)$ е група. Подмножеството $K \subset G$ се нарича подгрупа на групата G, ако K е група относно операцията "$*$", която получава ("наследява") от групата G. Ако K е подгрупа на G, тогава записваме $K < G$.

Пример:
Ако $(G, *)$ е група, и $e \in G$ е единичния елемент, тогава едноелементното подмножество $E = \{e\} \subset G$ е подгрупа, която е "тривиална" подгрупа. Групата G може да се разглежда и като подподгрупа на G, което е и другата "тривиална" подгрупа.

Пример:
При числата имаме, че стойността на сумата на две цели числа не зависи от това дали ги разглеждаме като цели, или като рационални, или като реални или като комплексни числа. Чрез такива разсъждения можем да се убедим, че е налице следната редица от подгрупи

$$(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +).$$

Аналогично е и при мултипликативните групи на основните числови множества:

$$(\mathbb{Z}^*, .\,) < (\mathbb{Q}^*, .\,) < (\mathbb{R}^*, .\,) < (\mathbb{C}^*, .\,).$$

3.1. твърдение

Твърдение:
Нека G е група и $\emptyset \neq K \subset G.$ Тогава е изпълнено:

$$K \text{ е подгрупа на } G \ \Leftrightarrow \ \left\{ \begin{array}{ll} ab \in K, & \forall a, b \in K \\ a^{-1} \in K, & \forall a \in K \end{array} \right\} \Leftrightarrow ab^{-1} \in K, \ \forall a, b \in K.$$

Доказателство:
$\boxed{\Rightarrow}$ Нека K е подгрупа на G. Следователно K е група и операцията "$*$" (получена от G), е бинарна операция в K и затова $a * b \in K, \ \forall a, b \in K$. В K има единичен елемент и нека това да бъде $\tilde{e} \in K$, за който е изпълнено $\tilde{e} * a = a, \ \forall a \in K.$ Установяваме, че $\tilde{e}$ не е нещо ново, а е точно равно на единичния елемент на цялата група $e \in G$:

$$\begin{array}{rcll} \tilde{e} * a & = & a, & \forall a \in K, \ (\text{равенство в подгрупата } K \subset G) \\ & \Downarrow & & \exists \ (a^{-1}) \in G \\ \tilde{e} * a * (a^{-1}) & = & a * (a^{-1}) & (\text{равенство в групата } G) \\ & \Downarrow & & \\ \tilde{e} & = & e \ \in K & (e \text{ е единичен елемент в } K < G) \end{array}$$

Аналогично, за всеки елемент $b \in K \subset G$ съществува обратен елемент в подгрупата K и нека да го означим със $\widetilde{b^{-1}} \in K$, този елемент си има обратен елемент и в цялата група G, който означаваме с b^{-1}, тогава лесно установяваме че тези елементи съвпадат:

$$\widetilde{b^{-1}} = \widetilde{b^{-1}} * e = \widetilde{b^{-1}} * (b * b^{-1}) = e * b^{-1} = b^{-1}$$

$\boxed{\Leftarrow}$ Ако за $K \subset G$ са изпълнени двете условия, тогава от $a * b \in K, \ \forall a, b \in K$ следва, че операцията "$*$" е бинарна операция за $K.$ Асоциативния закон важи за всички елементи от множеството G, следователно и за елементите на подмножеството K. Ако $a \in K \Rightarrow a^{-1} \in K$ и получаваме, че $e = a * a^{-1} \in K$ единичния елемент на G принадлежи на K. Следователно получихме, че са изпълнени всички условия от определението за група и затова $(K, *)$ е подгрупа на $(G, *)$.

3.2. примери

Пример:

Да разгледаме подмножеството от комплексни числа,за които $x^n = 1$ (n-ти корени на единицата)

$$C_n = \{x \in \mathbb{C} \mid x^n = 1\} \subset \mathbb{C}^*$$

Тези числа образват група, относно операцията умножение, и тази група е подгрупа на мултипликативната група $(\mathbb{C}^*, .)$. Проверяваме

$$z_1, z_2 \in C_n \Longrightarrow \begin{cases} (z_1 . z_2)^n = z_1^n . z_2^n = 1.1 = 1 \Rightarrow z_1 . z_2 \in C_n \\ (z_1^{-1})^n = (z_1^n)^{-1} = 1^{-1} = 1 \Rightarrow z_1^{-1} \in C_n \end{cases} .$$

Получихме, че C_n е подгрупа на мултипликативната група на комплексните числа$(\mathbb{C}^*, .)$. Знаем че елементите на тази група, записани в тригонометричен вид са следните $C_n = \{\omega_k \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \mid k = 0, 1, \ldots, n-1\}$.

От формулите на Моавър е изпълнено $\omega_k = \omega_1^k$. Следователно елементите на групата могат да се опишат по следния начин $C_n = \{1, \omega_1, \omega_1^2, \ldots, \omega_1^{n-1}\}$ И е изпълнено $\omega^n = 1$ = Поради тази причина тази група се нарича циклична група от ред n.

Пример:

Прилагаме твърдението към множеството $4\mathbb{Z} = \{4a | a \in \mathbb{Z}\} \subset \mathbb{Z}$, и проверяваме $4a + 4b = 4(a+b) \in 4\mathbb{Z}$ и $-4a = 4(-a) \in 4\mathbb{Z}$. Получаваме, че множеството $4\mathbb{Z}$ е подгрупа на адитивната група $(\mathbb{Z}, +)$.

Да обърнем внимание, че елементите на групата $\mathbb{Z}_4$, които са класове остатъци по модул 4 представляват подмножества от цели числа и затова групата $(\mathbb{Z}_4, +)$ не е подгрупа на адитивната група на целите числа $(\mathbb{Z}, +)$.

Пример:

Нека да разгледаме подмножеството от матриците с детерминанта равна на 1.

$$SL_n(\mathbb{R}) = \{A \in M_{n\times n}(\mathbb{R}) \mid \det(A) = 1\} \subset GL_n(\mathbb{R}).$$

Ясно е, че е изпълнено

$$\text{ако} A, B \in SL_n(\mathbb{R}) \Longrightarrow \begin{cases} \det(A.B) = \det(A).\det(B) = 1 & \Longrightarrow A.B \in SL_n(\mathbb{R}) \\ \det(A^{-1}) = (\det(A))^{-1} = 1 & \Longrightarrow A^{-1} \in SL_n(\mathbb{R}) \end{cases}$$

откъдето получаваме, че множеството $SL_n(\mathbb{R})$ е група, която е подгрупа на пълната линейна група $GL_n(\mathbb{R})$. Подгрупата $SL_n(\mathbb{R})$ се нарича специална линейна група от степен n.

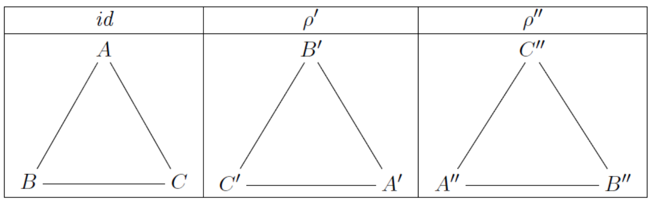
3.3. пример

Пример:

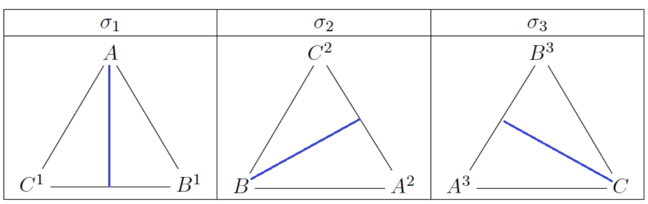
Нека в равнината е зададен равностранен триъгълник $\triangle ABC$ и да разгледаме подмножеството от еднаквости в равнината при които образът на дадения равностранен триъгълник е същия триъгълник. Еднаквостите в равнината (отбелязваме я с $\mathbb{R}^2$) представляват биективни изображения на равнината в себе си, и подмножеството от всички еднаквости, запазващи $\triangle ABC$ е подмножество на симетричната група на точките в равнината $S(\mathbb{R}^2)$. Композицията на две такива еднаквости е еднаквост, която запазва същия триъгълник, и обратното изображение на еднаквост от това множество е еднаквост, запазваща $\triangle ABC$. По този начин получаваме групата от еднаквостите на равностранния триъгълник D_3 която се нарича диедрална група от степен 3.

За да опишем елементите на D_3, съобразяваме, че при прилагане на тези еднаквости образите на всеки от върховете на триъгълника $\triangle ABC$ също е връх на триъгълника. По този начин можем да лесно да съобразим вида на еднаквостите от групата D_3.

Освен идентитета, в групата имаме две ротации ρ', ρ'' - около центъра на триъгълника на ъгъл $\pm 120^\circ$. На схемите образът на всеки връх на триъгълника е отбелязан със същата буква но с горен индекс, показваш за коя еднаквост става дума:



Освен това имаме и три осеви симетрии $\sigma_1, \sigma_2, \sigma_3$, които са с оси по всяка една от височините на триъгълника.

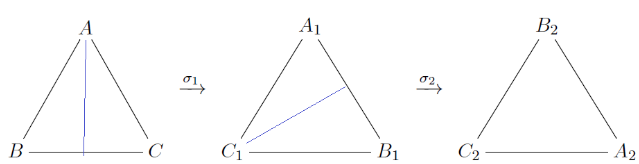


Не е трудно да се съобрази, че всички елементи на диедралната група D_3 са шест на брой и това са $D_3 = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3, \rho', \rho''\}$.

Понякога операцията на елементите на крайна група може да се зададе с таблица на операцията и такава таблица се нарича таблица на Кейли. В таблицата редовете и стълбовете са индексирани от елементите на групата и от доказаното свойство за единствеността решението на уравненията от вида $a * x = b$ или $y * a = b$ следва, че във всеки ред на таблицанта всеки елемент от групата участва точно на едно място, освен това произволен стъблб също съдържа всички елементи от групата. Когато таблицата е симетрична това означава че групата е абелева, както напремер таблицанта на Кейли на групата от класовете остатъзи по модул 7. Когато не е симетрична групата не е абелева.

Такава е например групата S_n $n > 3$ В случая на диедралната група от степен 3, съдържаща еднаквостите на равностранен триъгълник таблицата на Кейли изглежда по следния начин:

Например, да определим $\sigma_{2\circ}\sigma_1$ като не забравяме,че първо действа последно записаната еднаквост σ_1. Получаваме



Получихме че композицията $\sigma_{2\circ}\sigma_1$ действа върху върховете на триъгълника по същия начин както ротацията ρ' По този начин се попълва цялата таблица и се получава:

$D_3 = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3, \rho', \rho''\}:$

$\circ$	id	σ_1	σ_2	σ_3	ρ'	ρ''
id	id	σ_1	σ_2	σ_3	ρ'	ρ''
σ_1	σ_1	id	ρ''	ρ'	σ_3	σ_2
σ_2	σ_2	ρ'	id	ρ''	σ_1	σ_3
σ_3	σ_3	ρ''	ρ'	id	σ_2	σ_1
ρ'	ρ'	σ_2	σ_3	σ_1	ρ''	id
ρ''	ρ''	σ_3	σ_1	σ_2	id	ρ'