Алгебрични системи

Множества с набор от операции наричаме **алгебрични системи**.

Бинарна операция

Нека M е произволно множество.
Изображението $* : M \times M \to M$ наричаме **бинарна операция** (в множеството).

Ако $a, b \in M$, то $(a, b) \overset{*}{\to} a * b$ (**инфиксен запис**)

Най-простата алгебрична система е *групата* (с една бинарна операция).

Групи

Дефиниция

Нека G е непразно множество ($G \neq \emptyset$)
G наричаме **група** относно бинарната операция *, ако са изпълнени следните условия:

1.	$(a * b) * c = a * (b * c)$	**асоциативност на операцията**
2.	$\exists e: \quad a * e = e * a = a, \quad \forall a \in G$	**съществуване на неутрален елемент**
3.	$\forall a \in G, \quad \exists b_a \in G : a * b_a = b_a * a = e$	**противоположен елемент**

Записът $(G, *)$ означава, че G е група относно операцията $*$.

Ред на група

Ред на група наричаме броят на елементите в групата.

Отбелязва се с $|G|$.

Ако елементите на групата са краен брой, групата се нарича крайна ($|G| < \infty$)
Иначе - безкрайна ($|G| = \infty$)

Примери

Скрий

Пример 1
$(\mathbb{Z}, +)$ е група.
Непосредствено се проверява, че за $\forall\ a, b, c \in \mathbb{Z}$ са изпълнени и трите условия от дефиницията.
И все пак

1. $(a + b) + c = a + (b + c)$ за кои да е 3 цели числа.
2. Тук неутралният елемент е 0, защото знаем, че $a + 0 = 0 + a = a$ за всяко цяло a.
3. Освен това, за $\forall a \in \mathbb{Z}$, $\exists (-a) \in \mathbb{Z}$ и $a + (-a) = (-a) + a = 0$. $-a$ е противоположен на a.

И така, от дефиницията, се показва/доказва, че $(\mathbb{Z}, +)$ е група, при това безкрайна.

Пример 2
$(\mathbb{Q}, .)$ **не** е група. (. е операцията умножение)

На пръв поглед може да изглежда, че ситуацията е аналогична на тази от първия

пример, и $(\mathbb{Q}, .)$ е група, но все пак:

1. $(a.b).c = a.(b.c)$ за всеки три рационални числа.
2. Тук можем да наречем 1 неутрален елемент, тъй като $a.1 = 1.a = a$ за всяко $a \in Q$
3. Но нулата счупва дефиницията по третата точка, тъй като тя си няма обратен елемент.

И следователно $(\mathbb{Q}, .)$ **не е** група.
Възможно е да се дефинира мултипликативна група, ако специално се извади нулата от елементите на множеството.

Пример 3
Нека V е линейно пространство (vide Алгебра 1)
$\Longrightarrow \quad (V, +)$ е група.

> Ако знаеш какво е линейно пространство, ще ти се стори очевидно, а ако не знаеш - време е да научиш.

Пример 4

Нека $GL_n(F)$ е множеството от всички неособени квадратни матрици с елементи от полето F, т.е.

$$GL_n(F) = \{A \in M_{n,n} \mid detA \neq 0\}$$

> Напомням, че всички неособени квадратни матрици са обратими и детерминантата им е различна от нула. Друг е въпросът какво беше т'ва животно детерминанта и елементарният отговор: не можеш да разбереш Алгебра 2, ако все още не си разбрал Алгебра 1.
> (Конан Варварина, пред вестник Практична домакиня)

И тъй, ще покажем, че $GL_n(F)$ е група.

1. $(AB)C = A(BC)$ от свойствата на матриците.

2. $E \in GL_n(F)$ е единичната матрица (тази, която по диагонала си има единици, а всички други елементи са нули).
Набелязваме E за единичен елемент, тъй като знаем, че
$AE = EA = A$, $\forall A \in M_{n,n}$.

3. Нека $A \in GL_n(F)$.
За A знаем, че $\exists A^{-1}$, тъй като A е обратима, и освен това $detA^{-1} = \frac{1}{detA}$.
Но $detA \neq 0$, понеже A е неособена и, следователно, няма как $detA^{-1}$ да е нула.
Т.е. $A^{-1} \in GL_n(F)$.

От показаното дотук спокойно можем да твърдим, че $GL_n(F)$ е *група*, спрямо

операцията умножение на матрици.

Впрочем $GL_n(F)$ се нарича **пълна линейна група от степен n над полето F**

Терминология:

Операцията на дадена група може да бъде записана както *мултипликативно*, така и *адитивно*.
Според начина на записване се използват следните понятия:

Мултипликативен запис

- Операцията се нарича *умножение*. Използва се символът .
- $a.b$ наричаме *произведение* на a и b (често точката се пропуска $a.b = ab$)
- $e = 1$ наричаме *единичен* елемент
- a^{-1} наричаме *обратен* елемент на елемента a.

Адитивен запис

- Операцията се нарича *събиране*. Използва се символът $+$
- $a + b$ наричаме *сума* на a и b
- $e = 0$ наричаме *нулев* елемент
- $-a$ наричаме *противоположен* елемент на елемента a.

Идеята на двата записа е да се покаже, че все пак не е едно и също дали ще се събират или умножават два елемента на група.
Но, както ще се види по-късно, Алгебрата не прави разлика между двата записа стига поведението на елементите на групата и операцията в нея да е едно и също.

Основни свойства

Единичният (нулевият) елемент е единствен

Доказателство:
Допускаме, че $\exists\, e_1, e_2$, такива че
$e_1 a = a e_1 = a$ и $e_2 a = a e_2 = a$, $\forall a$.

Тогава:
$e_1 e_2 = e_1$, тъй като e_2 е единичен.
$e_1 e_2 = e_2$, тъй като e_1 е единичен.
От последните два реда, очевидно следва, че $e_1 = e_2$. $\square$

Обратният (противоположният) елемент е единствен

Доказателство:

Допускаме, че $\exists\, b_1, b_2$, такива че
$b_1 a = ab_1 = e$ и $b_2 a = ab_2 = e$.

$b_1 = b_1 e = b_1(ab_2) = (b_1 a)b_2 = eb_2 = b_2 \implies b_1 = b_2 . \square$

Тъй като доказахме, че обратният елемент е единствен, можем да го отбелязваме и по по-специален начин.
С a^{-1} отбелязваме обратния елемент на елемента a (при мултипликативен запис), а с $-a$ отбелязваме противоположния елемент на елемента a (при адитивен запис).

Обобщена асоциативност

$a_1 a_2, \ldots, a_k$
Идеята е, че при произволно разположение на скобите върху тези елементи се получава един и същи резултат.
Примерно
$a_1 a_2 a_3 a_4 = (a_1 a_2)(a_3 a_4) = (a_1 (a_2 a_3))a_4$ и т.н.

Така можема да дефинираме
$a^n = \underbrace{aa \ldots a}_{n}$
и да си изведем следните свойства:

при *мултипликативен* запис:
$a^k a^s = \underbrace{aa \ldots a}_{k} \underbrace{a \ldots a}_{s} = a^{k+s}$

и

$(a^k)^s = \underbrace{a^k a^k \ldots a^k}_{s} = a^{ks}$

NB:
$(ab)^n = \underbrace{(ab)(ab)\cdots(ab)}_{n}$
Не можем да твърдим, че $(ab)^n = a^n b^n$, тъй като никой не ни гарантира, че операцията в групата е комутативна.

при *адитивен* запис:
Дефинираме
$na = \underbrace{a + \cdots + a}_{n}$

> Тук na не е умножение, а обобщение на събирането"
> доц. Великова

Аналогично

$ka + sa = (k+s)a$ и $k(sa) = (ks)a$.

Свойство 4

Ако $a, b \in G \implies \exists!\, x \in G : ax = b$ и
$\exists! y \in G : ya = b$.

(или, иначе казано, дадените уравнения имат единствени решения)

Доказателство:
Съществуване ($\exists$)
$a(a^{-1}b) = (aa^{-1})b = eb = b \implies x = a^{-1}b$

Единственост (!)
Нека $ax_1 = b$.
Умножаваме двете страни на равенството с a^{-1} отляво и получаваме:

$$\begin{aligned} a^{-1}(ax_1) &= a^{-1}b \\ (a^{-1}a)x_1 &= a^{-1}b \\ ex_1 &= a^{-1}b \\ x_1 &= a^{-1}b \\ &\implies x_1 = x \end{aligned} \tag{1}$$

Следователно x е единствено.

Аналогично се получава, че $y = ba^{-1}$. $\square$

Абелева група

Групата $(G, *)$, за която е изпълнено, че $a * b = b * a \quad \forall a, b \in G$, наричаме **абелева (комутативна)**.

Примери

Скрий

Пример 1
Нека разгледаме групата $(\mathbb{Z}, +)$.
Знаем, че основно свойство на целите числа е това, че $a + b = b + a$, $\forall a, b \in \mathbb{Z}$.
От това, по дефиниция следва, че $(\mathbb{Z}, +)$ е безкрайна абелева група.

Пример 2
Разглеждаме множеството $\{1, -1\} \subset \mathbb{Z}$
Лесно се доказва, че $\{1, -1\}$ е група относно умножението.

Освен това тя е и абелева (лесно се забелязва, имайки предвид, че елементите са само два)

Като цяло $\{1, -1\}$ е крайна абелева група от втори ред.

Подгрупа

Подгрупа е непразно подмножество на дадена група, което също е група относно същата операция.

H - подгрупа на G отбелязваме по следния начин: $H \leq G$
Използва се и $H < G$ за случаите, когато е сигурно, че $H \neq G$

Примери

Скрий

Пример 1
Нека с $2\mathbb{Z}$ означим всички цели четни числа $(2\mathbb{Z} \subset \mathbb{Z})$
Лесно се вижда, че $(2\mathbb{Z}, +)$ е група, тъй като:

1. **(a + b) + c = a + (b + c)** за всички **a, b** и **c** четни.
2. Разгледаме нулата като неутрален елемент (**e = 0**) понеже знаем, че **a + 0 = 0 + a** за всяко цяло и четно **a**.
3. За всяко четно **a** съществува **-a**, такова, че **a + (-a) = e = 0**.

Освен това множеството от всички четни цели числа е подмножество на множеството на целите числа.
И така, по дефиниция, следва, че $(2\mathbb{Z}, +)$ е подгрупа на $(\mathbb{Z}, +)$.

Пример 2
Имайки предвид, че $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
и това, че всички тези множества са групи относно събирането, следва, че

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

Пример 3
Нека сега разгледаме подмножеството на множеството на целите числа $\{-1, 1\}$.
По-нагоре в темата доказахме, че и то е група.
Но $\{-1, 1\}$ е група относно операцията умножение, докато $\mathbb{Z}$ е група относно операцията събиране.

Т.е. $\{-1, 1\}$ **не** е подгрупа на $\mathbb{Z}$ относно събирането.

Пример 4
Нека
$\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$
$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$
$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$

$\mathbb{C}^* = \mathbb{C} \setminus \{0\}$

Всички те са групи относно операцията умножение и $\mathbb{Z}^* \subset \mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$.
От дефиницята можем да заключим, че:

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

Твърдение:

Нека **G** е група относно операцията **.**
и $H \subset G,\ H \neq \varnothing$

Тогава:

$$H < G \iff \begin{cases} ab \in H,\ \forall a, b \in H\ (1) \\ a^{-1} \in H,\ \forall a \in H\ (2) \end{cases} \iff ab^{-1} \in H,\ \forall a, b \in H\ (3) \tag{2}$$

Доказателство:
$|\Rightarrow|$

$H < G \Longrightarrow$
(1) е изпълнено, тъй като H е група спрямо тази операция.
(2) е изпълнено, поради *свойство 3* на дефиницията за група.

$|\Leftarrow|$
От **(1)** следва, че операцията е бинарна за **H**.
(2) е еквивалентно на *свойство 3* на дефиницията за група.

$$H \neq \varnothing \Longrightarrow \exists a \in H \xrightarrow{(2)} \exists a^{-1} \in H \Longrightarrow aa^{-1} = e \in H \tag{3}$$

Следователно *свойство 2* на дефиницията за група е също изпълнено.

Асоциативността е в сила в **G** и, следователно, е в сила и в **H**.
Т.е. *свойство 1* е също изпълнено за **H**.

Така, по дефиниця, следва, че **H** е група.
И тъй като $H \subset G,\ H \neq \varnothing \Longrightarrow$ **H** е подгрупа на **G**.

Сега нека разгледаме (3)
Нека $b \in H$

$$\begin{aligned} &b \in H \Longrightarrow bb^{-1} = e \in H \Longrightarrow eb^{-1} = b^{-1} \in H \\ &a, b \in H \Longrightarrow b^{-1} \in H \Longrightarrow a(b^{-1})^{-1} \in H \Longrightarrow ab \in H \end{aligned} \tag{4}$$

И отново, щом асоциативността е изпълнена в **G**, то тя е в сила и в **H**

Т.е. отново получихме, че всички свойства от дефиницията са изпълнени и **H** е група.
И тък като **H** е подмножество на групата **G**, следва, че $H < G$. $\square$

Примери

Скрий

Пример 1

Нека разгледаме пълната линейна група от степен **n**.

$$GL_n(F) = \{A \in M_{n,n} \mid detA \neq 0\}$$

Сега нека разгледаме следното подмножество на тази група:

$$SL_n(F) = \{A \in M_{n,n} \mid detA = 1\}$$

Нека $A, B \in SL_n(F) \Longrightarrow detA = detB = 1.$

$$detAB = detAdetB = 1 \Longrightarrow AB \in SL_n(F)$$

$$detA = 1 \Rightarrow detA^{-1} = \frac{1}{detA} = 1 \Longrightarrow A^{-1} \in SL_n(F)$$

От доказаното по-нагоре твърдение $\Longrightarrow SL_n(F) < GL_n(F)$

За информация: $SL_n(F)$ се нарича **специална линейна група от степен n**.

Пример 2
Нека $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$

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

т.е. множеството C_n е съставено от n-тите корени на единицата.

Знаем, че уравнението $x^n = 1$ има **n** решения в множеството на комплексните числа, т.е. $C_n \subset \mathbb{C}^*$ [1]

Тези корени са от вида (**от формулите на Моавър**):

$$v_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} = \left(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\right)^k = {w_1}^k,\ k = 1, 2 \ldots, n-1 \tag{5}$$

Т.е.

$$C_n = \{1, w^1, w^2, \ldots, w^{n-1}\} \tag{6}$$

Сега нека $x_1, x_2 \in C_n$

$(x_1 x_2)^n = {x_1}^n . {x_2}^n = 1.1 = 1 \Longrightarrow x_1 x_2 \in C_n$ [2]

$\left(\frac{1}{x_1}\right)^n = \left(\frac{1}{{x_1}^n}\right) = 1 \Longrightarrow \frac{1}{x_1} \in C_n$ [3]

От [1], [2] и [3] можем да твърдим, че $C_n < \mathbb{C}^*$.

В следващите теми C_n се споменава доста често, така че ще е хубаво да се запомни още тук.
Впроем C_n се нарича **циклична група от ред n**. (тегаво, а? ;))

page revision: 16, last edited: 29 Jun 2009, 15:14 (1468 days ago)