Циклична подгрупа (дефиниция)

Нека G е група и $a \in G$.
С $<a>$ ще бележим всички елементи от G, които са степени на a, т.е.

$$<a> \ = \{a^k \mid k \in \mathbb{Z}\}$$

$<a>$ наричаме **циклична подгрупа**, породена от елемента **a**.

За невярващите:

$$<a>= \{\ldots, a^{-2}, a^{-1}, a^0 = e, a^1, a^2, \ldots\}$$

$a^k a^s = a^{k+s} \in \ <a>, \ \forall k, s \in \mathbb{Z}$
$a^{-1} \in \ <a>$
$<a> \ \subset G$

Т.е. **<a>** наистина е подгрупа на **G**.

Циклична група (дефиниция)

Нека G е група.
Казваме, че G е **циклична**, ако $\exists a \in G$, такъв че $<a> \ = G$.

Ред на елемент (дефиниция)

Нека G е група и $a \in G$.
Казваме, че **редът на елемента** a е k, ако k е минималното естествено число, за което $a^k = e$.
Записваме $|a| = k$.

Ако такова число не съществува казваме, че редът е безкрайност. Записваме $|a| = \infty$

Твърдения

Твърдение 1

Нека $(G, .)$ е група и $a \in G,\ |a| = k$
Тогава:
1) $a^n = e \iff k|n$
2) $a^s = a^t \iff s \equiv t \pmod{k}$

Доказателство:

скрий

1)
$| \Rightarrow |$
От теоремата за деление с частно и остатък имаме, че:

$n = kq + r,\ 0 \leq r < |k|$

$e = a^n = a^{kq+r} = (\underbrace{a^k}_{e})^q a^r = a^r$

Т.е. получихме, $a^r = e,\ 0 \leq r < |k| = k, (k \in \mathbb{N})$.

$\Longrightarrow r = 0$, т.е. $k|n$.

$| \Leftarrow |$

$k|n \Longrightarrow n = kq$

Следователно $a^n = a^{kq} = e$.

2)

$a^s = a^t \iff a^{s-t} = e \iff k|(s-t) \iff s \equiv t \pmod{k}$. $\square$

Твърдение 2

Нека $(G, .)$ е група и $a \in G$

$|a| = k \iff |<a>| = k$

Доказателство:

скрий

$| \Rightarrow | \ |a| = k$

Нека $M = \{e, a, a^2, \ldots, a^{k-1}\}$

Нека $t \in \mathbb{Z}$
От теоремата за деление с частно и остатък, следва, че $t = kq + r,\ 0 \leq r < k$

Тогава $a^t = a^{kq+r} = (\underbrace{a^k}_{e})^q a^r = a^r \in M$

Т.е. за $\forall t \in \mathbb{Z} \Longrightarrow a^t \in M$ [1]

Ако допуснем, че $a^i = a^j \Longrightarrow i \equiv j \pmod{k}$ (от горното твърдение)
$\Longrightarrow a^i = a^j$ [2]

От [1] и [2] следва, че Misplaced & ?

$| \Leftarrow | \ |<a>| = k$

Това означава, че $|<a>|$ има k елемента
Тъй като $<a>$ е подгрупа $\Longrightarrow e \in <a>$.

Т.е. $<a>$ има следните елементи:

$<a> = \{e, a^1, a^2, \ldots, a^{k-1}\}$, където $a^j = a^i \iff j = i$

По дефиниция за всяко естествено $k \Rightarrow a^k \in <a>$, т.е.

$a^k \in \{e, a, a^2, \ldots, a^{k-1}\}$

Нека $a^k = a^s,\ s \in \{0, 1, \ldots, k-1\}$, освен това, нека редът на елемента a да е $r,\ r \in \mathbb{N}$

За r имаме, че: $a^r = e$ и $r > 0$, т.е. $r \geq k$
(Ако беше иначе, в $<a>$ щяхме да имаме повтарящи се еементи, което е просто недопустимо!)

Знаем, че $a^k = a^s \iff a^{k-s} = e \iff r|(k-s)$

Но $0 \leq s < k$, което означава. че $0 < k - s \leq k$

До тук имаме:
$0 < k - s \leq k \leq r$ и $r|k-s$

Единствената възмозност е $k - s = k = r$

Или, иначе казано, редът на a е k, $(|a| = k)$. $\square$

Групата Zn

Дефиниция

Нека $n \in \mathbb{N},\ n > 1$

Сега си дефинираме, следните множества:

$$\bar{0} = \{nk \mid k \in \mathbb{Z}\}$$

$$\bar{1} = \{1 + nk \mid k \in \mathbb{Z}\}$$

$$\vdots$$

$$\overline{n-1} = \{(n-1) + nk \mid k \in \mathbb{Z}\}$$

Очевидно това са *класовете на еквивалентност*, на които се разбива множеството $\mathbb{Z}$ от релацията *сравнимо по модул n*

Скрий

Всъщност, *сравнимо по модул n* е релация на еквивалентност, защото тя е:

1. рефлексивна $(a \equiv a \pmod{n},\ \forall a \in \mathbb{Z})$
2. симетрична $(a \equiv b \pmod{n} \Longrightarrow b \equiv a \pmod{n},\ \forall a, b \in \mathbb{Z})$
3. транзитивна $(a \equiv b \pmod{n},\ b \equiv c \pmod{n} \Longrightarrow a \equiv c \pmod{n})$

И както знаем, релацията на еквивалентност разбива дадено множество на *непресичащи се* класове на еквивалентност. (ала-бала-портокала)

Дефинираме: $Z_n = \bar{0} \cup \bar{1} \cup \cdots \cup \overline{n-1}$

Сега си дефинираме и операцията *събиране на класове* по следния начин:
$\overline{a+b} = \bar{a} + \bar{b} = \bar{z}$, където $z \equiv (a+b) \pmod{n},\ z \in \{0, 1, \ldots, n-1\}$

Очевидно $\bar{z} \in Z_n$, т.е. операцията е бинарна и добре дефинирана, демек:

$$+ : Z_n \times Z_n \to Z_n$$

Сега ще покажем, че Z_n е група относно събирането (на класове):

1. Асоциативността е ясна (дано!): $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c}),\ \forall \bar{a}, \bar{b}, \bar{c} \in Z_n$
2. За неутрален елемент си избираме $\bar{0}$, защото $a \equiv (a+0) \pmod{n}$, т.е. $\bar{a} + \bar{0} = \bar{a}$
3. Противоположен на елемента $\bar{k} \in Zn$ се явява елемента $\overline{n-k} = -\bar{k}, \quad (\bar{k} + n - k = \bar{0})$

Следователно, Z_n е **група** относно бинарната операция **събиране на класове**.

Изоморфизъм на групи (дефиниция)

Нека $(G_1, *)$ и $(G_2, .)$ са групи.

Казваме, че изображението $\varphi : G_1 \to G_2$ е **изоморфизъм**, ако:

1. φ е биекция.
2. $\varphi(a * b) = \varphi(a).\varphi(b)$ (хомоморфизъм - операциите са съгласувани)

Когато две групи са изоморфни, записваме $G_1 \cong G_2$.

Теорема (класификация на цикличните групи)

Нека G е циклична група.

- Ако G е крайна, т.е. $|G| = k < \infty \Longrightarrow G \cong Z_k (\cong C_k)$
- Ако G е безкрайна, т.е. $|G| = \infty \Longrightarrow G \cong \mathbb{Z}$

Доказателство:

Първа част

Първо, нека G е крайна и $|G| = k$

G е циклична $\Longrightarrow \exists a \in G : \ G = <a>$

Тогава следва, че $G = \{e, a, a^2, a^3, \ldots, a^{k-1}\}$

Имайки предвид, че $Z_k = \{\bar{0}, \bar{1}, \ldots, \overline{k-1}\}$,
можем да си дефинираме изображението:

$\varphi : G \to Z_k$, като
$\varphi(a^i) = \bar{i}$

1. **Биекция**: Сега ще докажем, че φ е биекция. Както знаете *биекция = инекция + сюрекция*:
1.1. **инекция**: Следните равенства са равносилни (но ако погледнете отгоре надолу подред даже може да разберете защо):

$$\begin{aligned} \varphi(a^p) &= \varphi(a^q) \\ \bar{p} &= \bar{q} \\ p &\equiv q \pmod{k} \\ a^p &= a^q \end{aligned} \tag{1}$$

1.2. **сюрекция**: Очевидно за всяко $\bar{x} \in Z_k$ съществува $a^x \in G$ такова, че $\varphi(a^x) = \bar{x}$.
С което биективността на φ е доказана!
Забележка: До скоро тук пишеше, че биекция има, защото множествата имат равен брой елементи и са крайни … е да ама ние искаме да докажем че **точно** тази функция която сме написали е биекция, а не да си опъваме мустаците и да говорим

теоретично, че **съществува** някаква биекция, защото просто произволна биекция не би била хомоморфизъм, right[1]?

2. **Хомоморфизъм**:
Нека a^s и a^t са два произволни елемента от G.

$\varphi(a^s a^t) = \varphi(a^{s+t}) = \varphi(a^r) = \bar{r}$ [1], където $s + t = qk + r,\ 0 \leq r < k$

А иначе:
$\varphi(a^s) + \varphi(a^t) = \bar{s} + \bar{t} = \bar{r}$ (по дефиниция) [2]

От [1] и [2] следва, че $\varphi(a^s a^t) = \varphi(a^s) + \varphi(a^t)$, т.е. φ е хомоморфизъм [2].

Доказахме, че φ е хомоморфизъм и биекция, т.е. φ е изоморфизъм, от където следва, че $G \cong Z_k$.

Втора част:

Сега нека G безкрайна и циклична

Т.е. $\exists a \in G :\ G = <a>,\ |a| = \infty$

Демек $G = \{a^k \mid k \in \mathbb{Z}\}$

Сега си дефинираме изображението:

$\psi : G \to \mathbb{Z}$
$\psi(a^k) = k$

1. **Биекция**
1.1 **Инекция**: Следните 3 равенства са равносилни. В правата посока е очевидно, наобратно използваме, че $a^k = a^s \iff a^{k-s} = e \iff k - s = 0$ (от реда на групата):

$$\begin{aligned} \psi(a^k) &= \psi(a^s) \\ k &= s \\ a^k &= a^s \end{aligned} \tag{2}$$

1.2 **Сюрекция**: За всяко $z \in \mathbb{Z}$, съществува $a^z \in G$, такова че $\psi(a^z) = z$.

2. **Хомоморфизъм**: Сега нека забележим, че
$\psi(a^k a^s) = \psi(a^{k+s}) = k + s = \psi(a^k) + \psi(a^s)$
Следователно ψ е хомоморфизъм, и, както вече знаем:

ψ = *хомоморфизъм* + *биекция* = *изоморфизъм*

Т.е., иначе казано, G и $\mathbb{Z}$ са изоморфни ($G \cong \mathbb{Z}$). $\square$

Footnotes

1. Впрочем, знаете ли каква е разликата между жените във ФМИ и крокодилите ;)

page revision: 16, last edited: 22 Jun 2011, 00:43 (746 days ago)