Определение: Циклична група е група съставена от степените само на един елемент

$\langle g \rangle = \{ g^{\alpha} \mid \alpha \in \mathbb{Z} \}$

⑥ Нека $(G,\cdot)$ е група и $a,b \in G$. ДСД, че

А) ако $g \in G$, то $|a| = |g a g^{-1}|$ б) $|ab| = |ba|$

Д-во 1) сл. $|a| = n$ т.е. $a^n = e$ $g^{-1}agg^{-1}ag \dots g^{-1}ag = g^{-1}a^n g = g^{-1}eg = e \Rightarrow |g^{-1}ag| \leq n$

Доп., че $|g^{-1}ag| < n \Rightarrow \underbrace{g^{-1}ag\cancel{g}\cancel{g^{-1}}ag \dots g^{-1}ag}_{m<n} = e$ $g^{-1}a^m g = e \;|.g^{-1}$ $g^{-1}a^m = eg^{-1}$ $a^m = e$ ↯

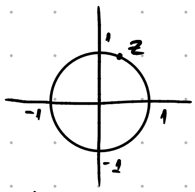
2сл. $|a| = \infty$ доп, че $|g^{-1}ag| = n < \infty$ $g^{-1}a^n g = e \Rightarrow g^{-1}a^n = g^{-1}$

$\underbrace{g^{-1}ag\cancel{g}\cancel{g^{-1}}ag \dots g^{-1}ag}_{n} = e$ $\Rightarrow a^n = e$ ↯ $\Rightarrow |g^{-1}ag| = \infty$

08.03.24

Зад1. ДСД, че групите $(\mathbb{U},\cdot)$ $\mathbb{U} = \{ z \in \mathbb{C} \mid |z| = 1 \}$ и $(SO_2(\mathbb{R}),\cdot)$ $SO_2(\mathbb{R}) = \{ A \in M_2(\mathbb{R}) \mid \det 1 \}$, A ортогонална $A^{-1} = A^T$

са изоморфни



$z = 1(\cos\varphi + i\sin\varphi)$

$|z| = z.\bar{z} = (\cos\varphi + \sin\varphi)(\cos\varphi - \sin\varphi)$

$= \cos^2\varphi - (-1)\sin^2\varphi = 1$

Д-во: $\varphi: SO_2(\mathbb{R}) \longrightarrow \mathbb{U}$

$A, B \in SO_2(\mathbb{R})$

Нека $A = \begin{pmatrix} \cos\varphi_A & -\sin\varphi_A \\ \sin\varphi_A & \cos\varphi_A \end{pmatrix}$ $B = \begin{pmatrix} \cos\varphi_B & -\sin\varphi_B \\ \sin\varphi_B & \cos\varphi_B \end{pmatrix}$

$\varphi(A.B) = \varphi(A).\varphi(B)$

$\varphi(AB) = \varphi\left(\begin{pmatrix} \overbrace{\cos\varphi_A\cos\varphi_B - \sin\varphi_A\sin\varphi_B}^{\sin(\varphi_A+\varphi_B)} & \overbrace{-\cos\varphi_A\sin\varphi_B + (-\sin\varphi_A)\cos\varphi_B}^{-\cos(\varphi_A+\varphi_B)} \\ \sin(\varphi_A+\varphi_B) & \cos(\varphi_A+\varphi_B) \end{pmatrix}\right) =$

$= \cos(\varphi_A+\varphi_B) + i\sin(\varphi_A+\varphi_B)$

$\varphi\left(\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}\right) = \cos\varphi + i\sin\varphi$

$\varphi(A).\varphi(B) = (\cos\varphi_A + i\sin\varphi_A)(\cos\varphi_B + i\sin\varphi_B) = \cos(\varphi_A+\varphi_B) + i\sin(\varphi_A+\varphi_B)$

$\Rightarrow \varphi(AB) = \varphi(A).\varphi(B) \Rightarrow \varphi$ е хомоморфизъм

Остава да докажем, че

φ е биекция:

Нека $A \neq B$, $\varphi(A) \overset{?}{=} \varphi(B)$

$\Rightarrow \varphi_A \neq \varphi_B \Rightarrow \cos\varphi_A + i\sin\varphi_A \neq \cos\varphi_B + i\sin\varphi_B \Rightarrow \varphi(A) \neq \varphi(B) \Rightarrow \varphi$ е инекция

Нека $z \in \mathbb{U} \Rightarrow z = \cos\varphi + i\sin\varphi$

$\Rightarrow \exists T: \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$, но $\det T = \cos^2\varphi + \sin^2\varphi = 1 \Rightarrow T \in SO_2(\mathbb{R}) \Rightarrow \varphi$ е сюрекция

$\Rightarrow \varphi$ е биекция, а оттам и изоморфизъм зад 2. $I=[0,1]$ $*: I\times I\to I$ $a,b\in I$ $a*b=\{a+b\}$ (пример: $\{0,5+0,7\}=\{0,2\}$) $[a+b]$ (пример: $[0,5+0,7]=[1]$)

ДСД, че $(I,*)$ е група, изоморфна на $\mathbb{U}$

Д-во: 1) неутрален елемент: 0 $a*0=\{a+0\}=\{a\}=\{0+a\}=0*a$

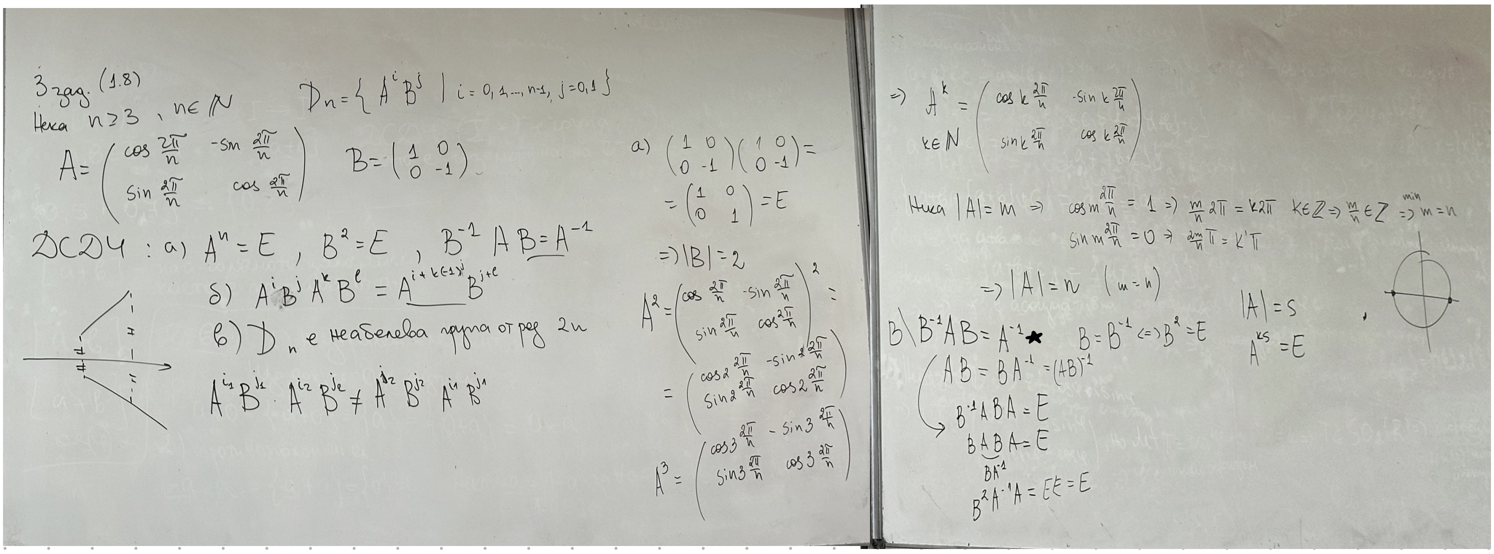
2) противоположен елемент: $\underline{-a}*a=\{\underline{-a}+a\}=0$ $(1-a)*a=\{1-a+a\}=\{1\}=0$

Нека $\underline{-a}=1-a$, $\forall a\in I$, $1-a\in I$ $a*(1-a)=\{a+1-a\}=\{1\}=0$

3) асоциативност $(a*b)*c\overset{?}{=}a*(b*c)$ $\forall x\in\mathbb{R}$ $x=[x]+\{x\}$ $\{x\}=x-[x]$

$(a*b)*c=\{a+b\}*c=\{\{a+b\}+c\}=\{a+b-[a+b]+c\}=a+b-[a+b]+c-[a+b-[a+b]+c]=$

$=a+b+c-\cancel{[a+b]}+\cancel{[a+b]}-[a+b+c]=\{a+b+c\}=\{a+\{b+c\}\}=a*\{b+c\}=a*(b*c)$



б) $A^iB^jA^kB^l\overset{?}{=}A^{i+k(-1)^j}B^{j+l}$

$B^jA^k=A^{k(-1)^j}B^j$

1) $j\equiv 0 \pmod 2$ $B^j\equiv E$

$A^k=A^k$ $\forall k\in\mathbb{Z}$

2) $j\equiv 1 \pmod 2$

$BA^k\overset{?}{=}A^{-k}B$ $/B^{-1}=B$ $(BAB)^k=\underbrace{BA\cancel{B}\cancel{B}A\cancel{B}\dots\cancel{B}AB}_{k}$

$BA^kB\overset{?}{=}A^{-k}$ $A^{-k}=BA^kB$

От ★ $\overset{B}{\overset{\parallel}{B^{-1}}}AB=A^{-1} \Leftrightarrow BAB=A^{-1}$ $\uparrow^k$

$\underbrace{BA\cancel{B}\cancel{B}A\cancel{B}\dots\cancel{B}AB}_{k}=A^{-k}$

$BA^kB=A^{-k}$

в) $A^{i_1}B^{j_1}A^{i_2}B^{j_2}\neq A^{i_2}B^{j_2}A^{i_1}B^{j_1}$

4 зад. Нека G е група и $a\in G$, $|a|=r$. ДСД, че
а) $a^n=1 \Leftrightarrow r/n$
б) $a^m=a^n \Leftrightarrow m\equiv n \pmod r$
в) a^k $(k\in\mathbb{Z})$ има ред $\frac{r}{GCD(k,r)}$ в частност $|a^k|=|a|$, ако $GCD(k,r)=1$ (взаимно прости)

Д-во: а) $n=q.r+t$, $0\le t<r$

$a^n=a^{qr+t}=(a^r)^q.a^t=e^q.a^t=a^t$ Но $|a|=r \Rightarrow$ ако $t\neq 0$ $\exists t<n$ $a^t=e$ ↯ $\Rightarrow t=0 \Rightarrow r/n$

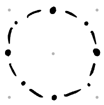
б) $a^{-n} \mid a^m = a^n \iff a^m \cdot a^{-n} = e \iff a^{m-n} = e \iff r / m-n, \quad m \equiv n \pmod r$

в) Нека $GCD(k,r) = d \Rightarrow k = k_1 d$ Нека $|a^k| = s$. Ако $s = \frac{r}{d}$ $a^{k\frac{r}{d}} = a^{\frac{k_1 d r_1 \cancel{d}}{\cancel{d}}} = a^{r.k_1}$ и $r / k_1 r \Rightarrow a^{rk_1} = e \Rightarrow$
$r = r_1 . d$

$\Rightarrow |a^k| \le \frac{r}{d}$. Допускаме, че $s < \frac{r}{d} = r_1 \Rightarrow a^{ks} = e \Rightarrow r / ks$
$r_1 d / k_1 d s \iff r_1 / k_1 s$, но $GCD(r_1, k_1) = 1 \Rightarrow r_1 / s$ ↯

$\Rightarrow |a^k| = \frac{r}{d}$

3ти час



$g \in G$ $|G| = n$ $G_0 = \{e, g^1, g^2, \dots, g^{n-1}\}$ Ако $G_0 \equiv G$, то g е пораждащ на G

зад 5 Нека G е крайна група от четен ред. DCD, че в G има елем. от ред 2

Д-во: Единствената възм. за $a \in G \setminus \{e\}$ $a = a^{-1}$ е когато $|a| = 2$, защото $a = a^{-1} \iff a^2 = e$

Допускаме противното $\Rightarrow \forall a \in G \setminus \{e\}$ $a \ne a^{-1}$. Тогава $G = \{e, a, a^{-1}, b, b^{-1}, \dots, d, d^{-1}, \dots\}$ и

$|G| = 1 + 2m$, $m \in \mathbb{N}$, т.е. 2 не дели $|G|$ ↯ $\Rightarrow \exists a \in G : |a| = 2$

зад 6 Нека G е група, която има единствен елемент от ред 2. DCD, че той комутира с всички елементи от G

I начин

Д-во: Нека $b \in G$ и $|b| \ne 2$. Допускаме, че $ab \ne ba$ $| . b^{-1}$ $e = a^2 \ne (bab^{-1})^2 = ba\cancel{b^{-1}}\cancel{b}ab^{-1} = ba^2b^{-1} = e$

$a \ne b.ab^{-1}$ $\uparrow^2$ $e \ne e$ ↯

II начин $|a| = |g^{-1}ag| = 2$ $\forall g \in G$ $\iff g . |g^{-1}ag = a \iff ag = ga$ $\forall g \in G$

Свойство ——— $|a| = n$

$g^{-1}a\cancel{g}\cancel{g^{-1}}a\cancel{g} \dots \cancel{g^{-1}}ag = g^{-1}a^n g = e \Rightarrow |g^{-1}ag| \le n$

Доп. че $|g^{-1}ag| = s < n$, $g . |g^{-1}a^s g = e$

$\iff a^s g = g \iff a^s = e$, но $|a| = n > s$ ↯

Циклична група G – група. $g \in G$

1) относно умножението $G_0 = \{\dots g^{-2}, g^{-1}, e, g^1, g^2, \dots\}$ – подгрупа на G

2) относно събирането $G_0 = \{\dots, -2g, -g, 0, g, 2g, \dots\}$ – подгрупа на G

Ако $G_0 \equiv G$, казваме че G е породена от g и пишем $G = \langle g \rangle$

- $(\mathbb{Z}, +)$ – хомоморфна* на всички безкрайни циклични групи
- $(C_n, \cdot)$ – хомоморфна на всички крайни циклични групи

$\varphi : (G_1, +_1) \longrightarrow (G_2, +_2)$
φ е хомоморфна ако $\forall a, b \in G_1$
$\varphi(a +_1 b) = \varphi(a) +_2 \varphi(b)$