Групе

1. Полугрупа $(G, \cdot)$ је група ако у њој постоји леви неутрални елемент e и ако за сваки елемент $a \in G$, постоји $a' \in G$, такав да је $a'a = e$.

2. Показати од услова $a'a = e$ и асоцијативности добијамо

$(a')'$ $$a'(aa') = (a'a)a' = ea' = a'$$

$$(a')'\left(a'(aa')\right) = (a')'a' = e$$

$$\left((a')'a'\right)(aa') = e(aa') = e$$

$$aa' = e.$$

Сада, $ae = a(a'a) = (aa')a = ea = a.$

Аритметика групе

Нека је $(G, *, e)$ група. Тада је:

1) $(x^{-1})^{-1} = x$

$(x * y)^{-1} = y^{-1} * x^{-1}$

$(x^{n})^{-1} = (x^{-1})^{n}$

2) Сваки елемент групе је скратив

$(\forall x, y, z \in G)\ x * y = x * z \Longrightarrow y = z.$

3) $\forall a, b \in G$, јед. $a * x = b$, $y * a = b$ имају јединств. реш.

1) $x * x^{-1} = x^{-1} * x = e$ (x^{-1} је инвер. ел. за x)

$x^{-1} * x = x * x^{-1} = e$ (x је инверзни ел. за x^{-1})

тј. $(x^{-1})^{-1} = x$.

$x * y * (y^{-1} * x^{-1}) = x * (y * y^{-1}) * x^{-1} = x * e * x^{-1} =$
$= x * x^{-1} = e.$

тј. $(x * y)^{-1} = y^{-1} * x^{-1}$!

$(G, +)$:
$-(x+y) = -y - x$

$(x^n)^{-1} = (\underbrace{x * x * \dots * x}_{n})^{-1} = \underbrace{x^{-1} * x^{-1} * \dots * x^{-1}}_{n} = (x^{-1})^n$.

2) $x^{-1} \backslash\; x * y = x * z$

$x^{-1} * (x * y) = x^{-1} * (x * z)$

$(x^{-1} * x) * y = (x^{-1} * x) * z$

$e * y = e * z$

$y = z$

$(G, +, 0)$:
$\cancel{x} + y = \cancel{x} + z$
$y = z$

3) $a^{-1} \backslash\; a * x = b$, $y * a = b. / a^{-1}$

$a^{-1} * (a * x) = a^{-1} * b$

$(a^{-1} * a) * x = a^{-1} * b$

$\boxed{x = a^{-1} * b.}$

$(y * a) * a^{-1} = b * a^{-1}$

$y * (a * a^{-1}) = b * a^{-1}$

$y * e = b * a^{-1}$

$\boxed{y = b * a^{-1}}$

Претп. да постоји још једно решење јне $a * x = b$, на пр. x'!

Тада $\left.\begin{array}{l} a * x' = b \\ a * x = b \end{array}\right\} \Rightarrow a * x' = a * x$

$x' = x.$

$a + x = b$ $/ + (-a)$ с леве стр.

$(-a) + a + x = (-a) + b$

$0 + x = (-a) + b$ ~~$= -(-b) = -(-b+a) = b - a$~~

$\boxed{x = -a + b}$ $(-a) + b$

Лема:

Нека је $(G,*)$ полугрупа. Тада су еквивалент-
-ни следећи услови:

1) $(G,*)$ је група

2) Јне $a*x=b$ и $y*a=b$ имају решење за $\forall a,b\in G$.

Доказ:

1) $\Rightarrow$ 2) доказано.

2) $\Rightarrow$ 1) Јна $y*a=b$ има реш. $\forall a,b\in G$, па и за $b=a$, тј. јна $y*a=a$ има решење $y=e_a$, тј. $e_a*a=a$. Докажимо да је e_a леви јед. ел. у полугрупи $(G,*)$.

Заиста, $\forall b\in G$,

$$e_a*b=e_a*(a*x)=(e_a*a)*x=$$
$$=a*x=b.$$

Дакле e_a је леви јед. ел. Означ. са e.

Јна $y*a=b$ има реш. за $\forall b\in G$, па и за $b=e$, тј. ~~јна~~ $y*a=e$ има р. по y. Нека је то $y=a'$.

Дакле, $a'*a=e$. a' је леви инв. ел. за a. Како ово важи за $\forall a\in G$, па за $\forall$ ел. $a\in G$ постоји леви инверзни ел. у G.

Лема: Нека је $(G,*)$ групоид. Тада су еквивалентни следећи услови

1° $(G,*)$ је група

2° Јед. $a*x=b$ и $y*a=b$ имају решење за $\forall a,b\in G$.

Примери:

1) $(Z,+)$ група целих бројева (бесконачна)

2) $(Z_m,+)$ група целих бр. по модулу m (коначна)

$Z_6=\{0,1,2,3,4,5\}$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

3) $(GL(n,R),\cdot)$ група регуларних квадратних матрица

поље реал. бр. <u>општа</u> <u>линеарна група</u>

4) Ако је $X=\{1,2,3,\dots,n\}$ коначан скуп, онда скуп свих бијективних пресликавања скупа X, обележава се са S_n, а $(S_n,\cdot)$ је <u>група пермутација</u>

5) Група аутоморфизама неке алгебре

6) Адитивна група вектора

- Подгрупе -

Деф: Подскуп H ~~групе~~ G је подгрупа групе $(G, \cdot)$ ако је он сам за себе група. То значи:

1° $\forall h_1, h_2 \in H \Rightarrow h_1 h_2 \in H$.

2° $e \in H$

3° $(\forall h \in H)\ h^{-1} \in H$.

Пишемо, $H \leq G$. Тривијалне подгрупе су $\{e\}$ и G.

Ако је $H \leq G$, при чему $H \neq \{e\}$, $H \neq G$
H се назива правом подгрупом групе G.

Лема: $H \leq G \iff (\forall h_1, h_2 \in H)\ h_1 h_2^{-1} \in H$ (само)

Лема: Ако су $A, B \leq G$, тада је $A \cap B \leq G$.
Слично, ако су $A_i \leq G$, $i \in I$, тада је $\bigcap_{i \in I} A_i \leq G$.

Деф: Нека је $(G, \cdot)$ група и $A \subseteq G$ (подскуп).
Са $\langle A \rangle$ обележимо пресек $\langle A \rangle = \bigcap_{i \in I} H_i$, $A \subseteq H_i$,
што је подгрупа групе G која је генерисана подскупом A. Специјално,
$G = \langle A \rangle$. $G = \langle \{a\} \rangle$ циклична група
↓ група G је генерисана подскупом A.

— $\langle A \cup B \rangle$ подгр. гр. G ген. унијом две подгрупе
$[A] = \{a_1^{k_1} \dots a_n^{k_n} \mid a_i \in A,\ k_i = \pm 1\}$ [унија две подгр. $A \cup B$ није подгр. гр. G уоп. сл.]
*) $[A] \leq G$, при чему је $[A] = \langle A \rangle$.
— Ако је $H \leq G$, тада деф. релацију на следећи начин
$x \sim y \iff x \cdot y^{-1} \in H$ Ово је рел. екв.
— $x \equiv y \pmod{H}$
$(G, +)$ $x - y \in H$ $n\mathbb{Z} \leq \mathbb{Z}$ | Све подгрупе дате групе у односу на опер. $A \cap B$, $\langle A \cup B \rangle$ чине мрежу.]

<u>Деф:</u> Нека је $(G, \cdot, e)$ група. Најмањи позит. цео број k, за који је $x^k = e$, назива се <u>ред елемента</u> $x \in G$.

$[(G,+,0)$: $kx = 0 \Rightarrow \underbrace{x+x+\cdots+x}_{k} = 0\,]$

<u>Деф:</u> Група, у којој сваки елемент има коначан ред, зове се <u>периодична</u> (<u>торзиона</u>) група.

Ако је једини елемент коначног реда јединични елемент, онда је реч о <u>групи без торзије</u>.

<u>Деф:</u> Група G, у којој је сваки елемент $(\neq e)$ коначног реда облика степена простог броја p, назива се <u>p-групом</u> (<u>примарном</u>).

*) $[A] \leq G$, јасно!

По деф. $[A]$ види се да је $A \subseteq [A]$.

$\Rightarrow \langle A \rangle \leq [A]$

$\downarrow$ најмања подгр. која садржи A, а $[A]$ је једна таква

$\Leftarrow$ Како је $\langle A \rangle$ затворен у односу на производ (множење) и инверзне елементе, то је $[A] \subset \langle A \rangle$, тј. $[A] \leq \langle A \rangle$.