Algebra

Grupe

A je neprazna množica. ***** je binarna operacija. $(A,*)$ je **algebrska struktura**.

1. $\forall a,b \in A \Rightarrow a*b \in A$ — **zaprtost** – notranjost
2. $\forall a,b,c \in A \Rightarrow (a*b)*c = a*(b*c)$ — **asociativnost**
3. $\exists e: \forall a \in A: \; a*e = e*a = a$ — **enota**
4. $\forall a \in A \; \exists a' \in A: \; a*a' = a'*a = e$ — **obstoj inverza**

Če velja (1), je struktura **grupoid**. Prvi dve lastnosti dasta **polgrupo**, prve tri **monoid**. Algebrsko strukturo, ki ima vse omenjene štiri lastnosti, imenujemo **grupa**.

Zgledi:

- $(\mathbb{N},\cdot)$. Ni grupa (inverza ni vedno v množici). Prve tri lastnosti veljajo, je **Abelov monoid** (Abelov zaradi komutativnosti).
- $(\mathbb{Z},\cdot)$ je **monoid**.
- $(\mathbb{Q},\cdot)$ je **monoid** (0 nima inverza!).
- $(\mathbb{Q}-0,\cdot)$ je **grupa**.
- $(\mathbb{N},+)$. Če ne vsebuje 0, je to **polgrupa**.
- $(\mathbb{Z},+)$ in $(\mathbb{Q},+)$ sta **grupi**.
- $(\mathbb{Z}_n,+_n)$ je **grupa**.
- $(\mathbb{Z}_n,\cdot_n)$ ***ni*** vedno grupa. Elementi, ki niso tuji modulu, nimajo inverza.
  - V $\mathbb{Z}_{12}$ imajo inverze le $\{1,5,7,11\}$.
    - Ali je $(\{1,5,7,11\},\cdot_{12})$ grupa?
      Napišemo Kellyjevo tabelo:

$\cdot_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Operacija je zaprta. Ostalo tudi velja. Je grupa.

Kdaj je $(\mathbb{Z}_n-0,\cdot_n)$ grupa? To **je grupa**, kadar **je *n* praštevilo**.

$\mathbb{Q}\sqrt{2}=\{a+b\sqrt{2}; a,b\in\mathbb{Q}\}$. Ali je $(\mathbb{Q}\sqrt{2},\cdot)$ grupa?

$a,b,x,y \in \mathbb{Q}$. $(a+b\sqrt{2})(x+y\sqrt{2})=ax+ay\sqrt{2}+bx\sqrt{2}+2by=ax+2by+\sqrt{2}(ay+bx)$. Zaprtost velja.

Operacija je navadno množenje, je asociativno.

$e=1=1+0\sqrt{2}$. Enota obstaja, je monoid.

Inverz: $\frac{1}{a+b\sqrt{2}}=\frac{a-n\sqrt{2}}{a^2-2b^2}=\frac{a}{a^2-2b^2}-\sqrt{2}\frac{b}{a^2-2b^2}$. Inverz je prave oblike. Imenovalec ne more biti 0, ker potem $\frac{a}{b}=\sqrt{2}$. To ni racionalno število. Vendar v primeru $a=b=0$ nimamo inverza. Struktura **ni grupa**, je le **monoid**.

Trditev: Če algebrska struktura premore enoto, je enota ena sama.

Dokaz: Recimo, da imamo dve enoti, e' in e'' . $e'*e''=?$. Če je prvo enota, dobimo drugo in obratno. Hkrati dobimo obe enoti. $e'=e''$. Enota je ena sama.

Trditev: Če *a* ima inverz, je inverz en sam.

Dokaz: Imamo inverza a' in a'' . $a\cdot a'=a'\cdot a=e,\ a\cdot a''=a''\cdot a=e$.
Velja $a'=a'\cdot e=a'\cdot(a\cdot a'')=(a\cdot a'')\cdot a'=(a'\cdot a)\cdot a''=e\cdot a''=a''$. V dokazu smo uporabili asociativnost!

Trditev: V **grupi** $(A,\cdot)$ velja pravilo krajšanja: $ax=bx \Rightarrow a=b$.

Dokaz:

$$ax=bx \quad /x^{-1}$$
$$axx^{-1}=bxx^{-1}$$
$$ae=be$$
$$a=b$$

(Opomba: uporabili smo nekoliko drugačno notacijo: $*=¿,\ 1\text{ je enota},\ a^{-1}\text{ je inverz}$. Obstaja še zapis $*=+,\ 0\text{ je enota},\ -a\text{ je inverz}$.)

Definiciji:

- Grupa $(G,\cdot)$ je **abelova** (oziroma **komutativna**) grupa, če $\forall a,b \in G: ab=ba$.
- Grupa $(G,\cdot)$ je **ciklična**, če obstaja **generator**, t.j. $\exists a$, tako da $G=\{e,a,a^{2,}\ldots,a^{r-1}\}$ in $a^r=e$.
  - ***Primer***: $(\mathbb{Z}_{12,}+_{12})$. Je abelova (ker je seštevanje komutativno). $1^2=1+1=2$ in tako dalje. Torej je ciklična grupa. 1 je generator. (Ker je operacija +, velja $a^n=na$.
  - Za $(\mathbb{Z}_n,+_n)$ velja enako.

Primer: Poišči vse generatorje v $(\mathbb{Z}_{12,}+_{12})$. **0 ni**. **1 je**. **2 ni**. Itd. **5 je** generator, ker je $5^5=5\cdot 5=1$ in za 1 vemo, da je generator. **7 in 11 sta** generatorja iz istega razloga.

Definicija: Naj bosta $(H, \cdot)$ in $(G, \cdot)$ grupi ter $H \subseteq G$, potem je H **podgrupa** G.

Primer: Poiščimo vse podgrupe v $(\mathbb{Z}_6, +_6)$. $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$.
Podgrupe: $(\{0\}, +_6)$, $(\mathbb{Z}_6, +_6)$ (ti dve vedno dobimo). Naprej lahko izbiramo: če je 1 v H, potem so tudi vse njene potence, to pa so vsi elementi; to podgrupo smo že zapisali. Sicer sklepamo podobno še za ostale elemente. Dobimo še $H = \{0, 2, 4\}$, $H = \{0, 3\}$.

Primer: Poiščimo podgrupe $(\mathbb{Z}_{12}, +_{12})$ z natanko 5 elementi. Ni jih.

Velja: H je podgrupa v G $\Rightarrow$ $|H| \mid |G|$ (moč *H*-ja deli moč *G*-ja).

Trditev: Če sta H_1 in H_2 podrupi v *G*, je $H_1 \cap H_2$ je podgrupa v *G*.

Dokaz: $H_1 \cap H_2 \neq \emptyset$; vsebuje vsaj enoto (torej ima enoto!). $x, y \in H_1 \cap H_2 \Rightarrow x \cdot y \in H_1 \cap H_2$ velja zato, ker je $x \cdot y \in H_1$ in $x \cdot y \in H_2$ (sicer H_1 in H_2 ne bi bili (pod)grupi). Asociativnost za operacijo že velja, ker velja v *G*. Imamo tudi inverz, saj $a \in H_1 \Rightarrow a^{-1} \in H_1$ in $a \in H_2 \Rightarrow a^{-1} \in H_2$.

Definicija: $(G, +)$, $(H, *)$ sta grupi. $f: G \rightarrow H$ je **homomorfizem**, če velja $\forall a, b \in G: f(a+b) = f(a) * f(b)$. **Bijektivni** homomorfizem je **izomorfizem**. Če pri tem velja *G* = *H*, je to **avtomorfizem**.

Kartezični produkt

$(G, *)$, $(H, \cdot)$ sta grupi.

$(G \times H, \square)$

Definicija *kvadratka*: $(g_1, h_1) \square (g_2, h_2) = (g_1 * g_2, h_1 \cdot h_2)$

Rezultat je grupa.

$$(g_1, h_1) \square [(g_2, h_2) \square (g_3, h_3)] = (g_1 * (g_2 * g_3), h_1 \cdot (h_2 \cdot h_3)) = ((g_1 * g_2) * g_3, (h_1 \cdot h_2) \cdot h_3) =$$
$$= (g_1 * g_2, h_1 \cdot h_2) \square (g_3, h_3) = [(g_1, h_1) \square (g_2, h_2)] \square (g_3, h_3).$$

Enota je (e_G, e_H). Inverz: $(g, h)^{-1} = (g^{-1}, h^{-1})$.

Ali je grupa $(\mathbb{Z}_2, +_2) \times (\mathbb{Z}_4, +_4)$ izomorfna grupi $(\mathbb{Z}_8, +_8)$? (Odgovor je ne.) Iščemo lastnosti, ki so različne, recimo komutativnost (je/ni abelova), cikličnost, ... Druga grupa je ciklična.

Podobno $\mathbb{Z}_2 \times \mathbb{Z}_2$ ni izomorfno $\mathbb{Z}_4$, je pa $\mathbb{Z}_2 \times \mathbb{Z}_3$ izomorfno $\mathbb{Z}_6$.

Ko iščemo homomorfno preslikavo, enoto preslikamo v enoto in generator v generator. Tako pri slednjem primeru velja $f(1) = (1, 1)$, $f(2) = (0, 2)$, $f(3) = f(1+2) = (1, 0)$, ... (Ciklični grupi istega reda sta vedno izomorfni.)

Trditev (kriterij za podgrupe): H je podgrupa ntk. $\forall a,b\in H: \ a^{-1}b\in H \ \wedge \ H\neq\emptyset$.

Dokaz:

- $(\Rightarrow)$ $a,b\in H \ \Rightarrow \ a^{-1}\in H \ \Rightarrow \ a^{-1}b\in H$
  $e\in H \ \Rightarrow \ H\neq 0$
- $(\Leftarrow)$
  Vzamemo $b\rightarrow a$ $(b:=a)$. Dobimo $a^{-1}\cdot a=e\in H$. Vzamemo $b\rightarrow e$ $(b:=e)$. Dobimo $a^{-1}\in H$. Vzamemo $a:=a^{-1}$. Dobimo $(a^{-1})^{-1}b=ab\in H$.

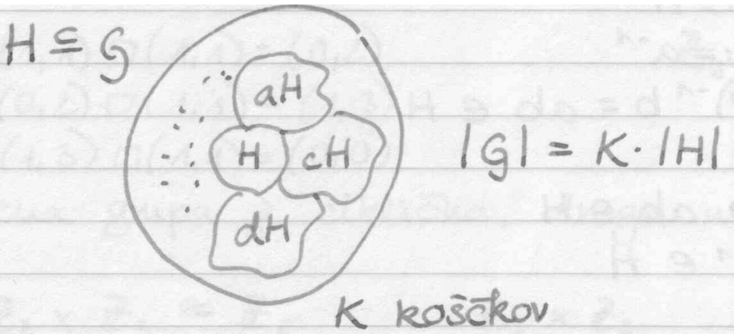
Uporabljena dejstva: $a,b\in H \ \Rightarrow \ ab\in H; \ a\in H \ \Rightarrow \ a^{-1}\in H; \ e\in H$.

Trditev (poenostavitev kriterija za končne grupe): G je končna grupa:
$H\subseteq G \Leftrightarrow H$ trdna podmnožica* .

Dokaz: $a\in H. \exists h,d: \ a^h=a^{h+d}$ zaradi končnosti (h,d najmanjša taka) .
$a^h=a^{h+d} \quad / a^{-h} \quad (a^{-h}=(a^{-1})^h)$
$e=a^d \ \Rightarrow \ e\in H \quad d=\mathrm{red}(a)$
$a^n\cdot a^{d-n}=e$
$a\cdot a^{d-1}=e \quad (a^{d-1}=a^{-1}$ - inverz)

Velja: $f:G\rightarrow G, \ a\in G$
$x\rightarrow ax$ $(f(x)=ax)$ je bijekcija (inj.: $f(x)=f(y)$ ... $ax=ay$ ... $x=y$, surj.: $ax=y$ ... $x=a^{-1}y$). Zato $\forall a\in G, \forall H\subseteq G: \ |H|=|aH|=|Ha|$. aH je **desni odsek** in Ha je **levi odsek** (**za podgrupo**): $aH=\{ah:h\in H\}, \ Ha=\{ha:h\in H\}$.

Trditev: $aH\cap bH\neq\emptyset \ \Rightarrow \ aH=bH$



$a,b: \ aH=bH$ ali $aH\cap bH=\emptyset$

Dokaz: Naj bo $c\in aH\cap bH$. $c=a\cdot h_1, \ h_1\in H; \ c=b\cdot h_2, \ h_2\in H$. $ah_1=bh_2; \ a=bh_2h_1^{-1}$ (kjer $h_2h_1^{-1}\in H$). $a=b\cdot h_3$. $aH=b\cdot h_3\cdot H$, $(h_3\cdot H=H; \ h\in H: hH=H)$. $aH=bH$.

Definicija: Naj bo $H\leq G$. Če je število levih odsekov po podgrupi H končno, ga imenujemo

indeks podgrupe H v grupi G in označimo $[G:H]$.

Lagrangeov izrek: Naj bo G končna grupa in $H \leq G$. Potem je moč grupe G deljiva z močjo podgrupe H in velja formula: $|G|=[G:H]\cdot|H|$.

Naj bo a element končne grupe G. $\{\ldots, a^{-2}, a^{-1}, e=a^0, a^1, a^2, \ldots\}=H=\{e, a, a^2, \ldots, a^{k-1}\}$. H je podgrupa, torej $|H| \| |G|$. $a\hat{\imath} \cdot a^{-j}=a^{i-j} \in H$.

Trditev: Naj bo G končna grupa in $a \in G$. Potem $\mathrm{r}(a) \| |G|$.

Trditev: Če je moč grupe praštevilo, potem je grupa ciklična.

Dokaz:
Naj bo $a \in G$ in naj bo $\mathrm{r}(a)=11$. $\{e, a, a^2, \ldots, a^9, a^{10}\}=G$.
Naj bo $a \in G$ in naj bo $\mathrm{r}(a)=p$. $\{e, a, a^2, \ldots, a^{p-2}, a^{p-1}\}=G$.
Red enote je 1. Red vseh ostalih je p.

Trditev: G_1, G_2 ciklični grupi. $|G_1|=|G_2| \Rightarrow G_1 \cong G_2$.

Dokaz: Naj bo $|G_1|=|G_2|=n$. $G_1=<a>,\ G_2=<b>$.
Potem: $G_1=\{e_1, a, a^2, \ldots, a^{n-1}\}$ $a *_1 a=a^2$, $G_2=\{e_2, b, b^2, \ldots, b^{n-1}\}$ $b *_2 a=b^2$.
Definirajmo: $g: G_1 \rightarrow G_2:\ f(a^k)=b^k$. Imamo bijekcijo. Homomorfizem:
$f(a^k *_1 a^m)=f(a^k) *_2 f(a^m)=b^{k+m},\quad f(a^k *_1 a^m)=f(a^{k+m})=b^{k+m}$.

Če izberemo katerokoli grupo moči n, ki je ciklična, je enaka grupi $(\mathbb{Z}_n, +_n)$.

Izrek (opis končnih Abelovih grup): Naj bo G končna Abelova grupa, $n=|G|$. Potem obstaja tak zapis števila n v obliki $n=p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, kjer so p praštevila in $p_1 \leq p_2 \leq \ldots \leq p_k$, $\alpha_i > 0$. Tako je $G \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \ldots \times \mathbb{Z}_{p_k^{\alpha_k}}$.

Primer: $n=70=2 \cdot 5 \cdot 7:\ \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7$.

Pomni: $\mathbb{Z}_2 \times \mathbb{Z}_2=\mathbb{Z}_2^2 \neq \mathbb{Z}_4$!

Trditev: $\mathbb{Z}_m \times \mathbb{Z}_n \cong Z_{mn} \Leftrightarrow \gcd(m, n)=1$

Dokaz: $(\Rightarrow)$ Recimo, da je $\gcd(m, n)=d$. $e=\mathrm{lcd}(m, n)=d m_1 n_1$. $m=m_1 d, n=n_1 d$. $m_1 \perp n_1$.

(Zapiske pošlje profesor.)