PODGRUPA EDINKA IN KVOCIENTNA GRUPA

GRUPA EDINKA

Naj bo G grupa in $H \leq G$ podgrupa. Podgrupa H je edinka ($H \trianglelefteq G$), če za vsak $g \in G$ velja:

$$h \in H \Rightarrow ghg^{-1} \in H \quad \text{(oziroma } gHg^{-1} \subseteq H\text{)}$$

Primer: $\{e\}$ in G sta edinki v G

Primer: Če je G abelova grupa, je vsaka podgrupa edinka.

$$gHg^{-1} = H(gg^{-1}) = H$$

Primer: Če je $f: G \to K$ homomorfizem, je $\ker f = \{g \in G;\ f(g) = e_K\} \trianglelefteq G$.

$h \in \ker f$, $g \in G$

$ghg^{-1} \in \ker f$

$$f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = \quad (f(h) = e_K)$$
$$= f(g)f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_K$$

Primer: $G = S_3$, $H = \{id, (12)\}$ je podgrupa.

$g = (1\,3)$
$g^{-1} = (1\,3)$

$g h g^{-1} = (13)(12)(13) = (1)(23) = (23) \notin H$

Torej H ni edinka.

KVOCIENTNA GRUPA

Naj bo $H \triangleleft G$. Elementi kvocientne grupe G/H so levi odseki, torej $G/H = \{gH ; g \in G\}$.

Od prej vemo, da levi odseki tvorijo particijo G.

Kompozitum definiramo kot $(aH) * (bH) = (ab)H$.

Preverimo dobro definiranost:

$aH = a'H \quad ; \quad a, a' \in G$
$bH = b'H \quad ; \quad b, b' \in G$

$(ab)H = (a'b')H$

$aH = a'H \Rightarrow H = (a^{-1}a')H \Rightarrow e = (a^{-1}a')h$
$\Rightarrow h^{-1} = a^{-1}a' \in H$

Enako dobimo $b^{-1}b' \in H$.

$\Rightarrow a^{-1}a'\, \underbrace{b(\overbrace{b^{-1}b}^{H})b^{-1}}_{H,\ \text{ker je } H \text{ edinka}} \in H$

$\Rightarrow a^{-1}a'b'b^{-1} \in H \Rightarrow a'b' \in aHb \overset{H \text{ edinka}}{=} abHb^{-1}b$

$\Rightarrow a'b' \in (ab)H$ in $a'b' \in (a'b')H$

$\Rightarrow (ab)H \cap (a'b')H \neq \emptyset \Rightarrow (ab)H = (a'b')H$

Preverimo asociativnost:

$$((aH)*(bH))*(cH) = ((ab)H)*(cH) =$$
$$= ((ab)c)H = (a(bc))H = (aH)*((bH)*(cH))$$

Enota: $eH = H$
Inverz: $(aH)^{-1} = a^{-1}H$

Opomba: $\pi: G \to G/H$ je kvocientna projekcija, $\pi(g) = gH$, je homomorfizem:

$$\pi(ab) = (ab)H = (aH)(bH) = \pi(a)\,\pi(b)$$

Jedro $\ker \pi = H$:

$$\pi(g) = H \Leftrightarrow gH = H \Leftrightarrow g \in H$$

Izrek: Naj bo $f: G \to H$ homomorfizem grup. Potem velja $G/\ker f \cong \operatorname{im} f$.

Dokaz: $\ker f = \{g \in G;\ f(g) = e_H\}$
$\operatorname{im} f = \{f(g);\ g \in G\} \leq H$

Definirajmo $\Phi: G/\ker f \to \operatorname{im} f$ s predpisom $\Phi(g \ker f) := f(g)$.

Dobra definiranost Φ

$g \ker f \overset{(*)}{=} g' \ker f \Rightarrow f(g) = f(g')$

$g^{-1}/$

$(*) \Leftrightarrow \ker f = (g^{-1}g')\ker f \Leftrightarrow g^{-1}g' \in \ker f \Rightarrow$

$\Rightarrow f(g^{-1}g') = e_H \overset{f \text{ homo}}{\Rightarrow} f(g^{-1})f(g') = e_H \overset{f \text{ homo}}{\Rightarrow}$

$\Rightarrow (f(g))^{-1} f(g') = e_H \overset{f(g)/}{\Rightarrow} f(g') = f(g)$

Surjektivnost Φ

$\operatorname{im} f = \{ f(a) ; a \in G \}$

Φ je surjektivna, saj so v sliki Φ vsi ravno vsi $f(a)$.

Injektivnost Φ

$\Phi(a \ker f) = \Phi(b \ker f) \Leftrightarrow f(a) = f(b)$
$\Leftrightarrow f(a)(f(b))^{-1} = e_H \overset{f \text{ homo}}{\Leftrightarrow} f(a) f(b^{-1}) = e_H$
$\Leftrightarrow f(ab^{-1}) = e_H \Leftrightarrow ab^{-1} \in \ker f$
$\Leftrightarrow a \in (\ker f) b \Leftrightarrow a = k \cdot b$
$\Leftrightarrow a = b b^{-1} k b \Leftrightarrow a \in b(\ker f)$
$\Rightarrow b \ker f b^{-1} \subseteq \ker f \Rightarrow a \ker f = b \ker f$
$\Rightarrow a = b$ □

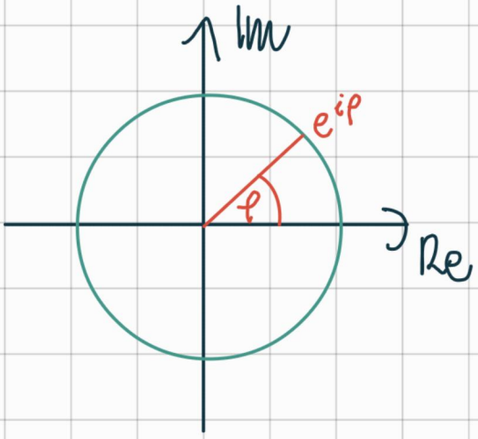
Če je G abelova, je vsaka njena podgrupa edinka.

Primer: $(\mathbb{Z}, +)$ podgrupa v $(\mathbb{R}, +)$ je edinka, ker je $(\mathbb{R}, +)$ abelova grupa.

Kaj je $\mathbb{R}/\mathbb{Z}$?

$f : (\mathbb{R}, +) \to (\mathbb{C} \setminus \{0\}, \cdot)$
$f(x) = e^{2\pi i x} = \cos(2\pi x) + i \sin(2\pi x)$

$f(x+y) = e^{2\pi i (x+y)} = e^{2\pi i x} \cdot e^{2\pi i y} = f(x) \cdot f(y)$
$\Rightarrow f$ je homomorfizem



$\ker f = \{x \in \mathbb{R};\ f(x) = 1\} = \{x;\ e^{2\pi i x} = 1\}$

$e^{2\pi i x} = 1 \iff 2\pi x = \varphi = 2k\pi,\ k \in \mathbb{Z}$
$\iff x = k,\ k \in \mathbb{Z}$

Torej: $\ker f = \mathbb{Z}$

Po izreku: $\mathbb{R}/\mathbb{Z} \cong \mathrm{im} f = S^1 = \{z \in \mathbb{C};\ |z| = 1\}$

$(S^1, \cdot)$ je grupa izomorfizma $\mathbb{R}/\mathbb{Z}$.

Primer: $(\mathbb{Z}, +)$ je grupa. Za $n \in \mathbb{N}$ je podgrupa $n\mathbb{Z} = \{nk;\ k \in \mathbb{Z}\}$. Ker je $\mathbb{Z}$ komutativna, je vsaka njena podgrupa edinka, torej je $n\mathbb{Z}$ edinka.

Naj bo $C_n = \{e, a, \ldots, a^{n-1}\}$ ciklična grupa z operatorjem a.

$\mathrm{red}(a) = n \quad (a^n = e,\ a^k \neq e \text{ za } k < n)$

$\mathbb{Z} \xrightarrow{f} C_n$
$k \longmapsto a^k$

$f(k) := a^k$
za $k = -n$: $a^k = (a^{-1})^n$
za $k = 0$: $a^0 = e$

$f(k+l) = a^{k+l} = a^k \cdot a^l = f(k) \cdot f(l)$
$\Rightarrow f$ je homomorfizem

Po izreku o izomorfizmu je $\mathbb{Z}/_{\ker f} \cong C_n$, saj je f očitno surjektivna.

$f(k) = e \Leftrightarrow a^k = e \Leftrightarrow n$ deli $k \Leftrightarrow k \in n\mathbb{Z}$
$\Rightarrow \ker f = n\mathbb{Z}$
$\Rightarrow \mathbb{Z}/n\mathbb{Z} \cong C_n \cong \mathbb{Z}_n$

Primer: S_n ... grupa permutacij
S_n ni komutativna za $n \geq 3$

A_n ... množica sodih permutacij
A_n je alternirajoča podgrupa v S_n

i) id je soda
$\Rightarrow id \in A_n$

ii) $\pi_1, \pi_2 \in A_n$
$\Rightarrow \pi_1 \cdot \pi_2 \in A_n$ (tudi soda)

iii) $\pi \in A_n \Leftrightarrow \pi = \underbrace{(i_1, j_1) \cdots (i_{2m}, j_{2m})}_{\text{sodo transpozicij}}$

$(i,j)^{-1} = (i,j)$

$\Rightarrow \pi^{-1} = (i_{2m}, j_{2m}) \cdots (i_1, j_2) \in A_n$

$A_n \trianglelefteq S_n$

$\forall \tau \in S_n : \tau A_n \tau^{-1} \subseteq A_n$
$\Leftrightarrow \forall \tau \in S_n : \forall \pi \in A_n : \tau \pi \tau^{-1} \in A_n$

$\tau \pi \tau^{-1}$ ← m trans
← 2ℓ trans
← m trans

$\Rightarrow m + 2\ell + m = 2(m+\ell)$ transpozicij
$\Rightarrow \tau\pi\tau^{-1} \in A_n$
$\Rightarrow A_n$ je edinka

Kaj je S_n/A_n?

$C_2 = \{1, -1\}$ je grupa za množenje.

Iščemo epimorfizem $f: S_n \to C_2$ z jedrom A_n.

Definiramo $f(\pi) = s(\pi)$ znak permutacije.

Naloga: Preveri, da je f homomorfizem.

Očitno je $\pi \in \ker f \Leftrightarrow s(\pi) = 1 \Leftrightarrow \pi \in A_n$.

$\Rightarrow S_n/A_n \cong C_2 \cong \mathbb{Z}_2$

POLDIREKTNI PRODUKT GRUP

H, K grupi
$Aut(H) = \{f: H \to H;\ f$ izomorfizem$\}$ grupa avtomorfizmov
$\Phi: K \to Aut(H)$ homomorfizem

Množico $H \times K = \{(h,k);\ h \in H, k \in K\}$ opremimo z operacijo:

$(h_1, k_1)(h_2, k_2) = (h_1 \Phi(k_1)(h_2),\ k_1 k_2)$

Na ta način množica $H \times K$ postane grupa, ki jo imenujemo poldirektni produkt in označimo $H \times_\Phi K$.

Naloga: Dokaži, da res dobimo grupo.

Enota (e_H, e_K):

$(h,k)(e_H,e_K) = (h\phi(k)(e_H), ke_K) = (h\, e_H, k) = (h,k)$

$\phi(k)$ je homo $H \to H$, zato $\phi(k)(e_H) = e_H$.

Če za ϕ izberemo trivialni homomorfizem, torej $\phi(k) = id_H$ za vsak $k \in K$, dobimo:

$(h_1,k_1)(h_2,k_2) = (h_1\, id_H(h_2), k_1k_2) = (h_1h_2, k_1k_2)$

Če na $H \times K$ vzamemo kompozitum po komponentah, dobimo direktni produkt, ki ga ponavadi označimo $H \times K$.

Primer: $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6 \cong C_6 \cong \{e, a, a^2, \dots, a^5\}$

Iščemo $a \in \mathbb{Z}_2 \times \mathbb{Z}_3$ z redom 6:

$a = (1,1)$

za $k \in \mathbb{N}$:
$a^k = (k \pmod 2, k \pmod 3) = e = (0,0)$

$k \pmod 2 = 0$ in $k \pmod 3 = 0 \Leftrightarrow$ k deljiv z 2 in k deljiv s 3 $\overset{2,3 \text{ tuji}}{\Leftrightarrow}$ 6 deli k $\Rightarrow$ red$((1,1)) = 6$

Primer: $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$

Trditev: Naj bo G grupa, $H \trianglelefteq G$ podgrupa edinka in $K \leq G$ podgrupa. Če je $HK = G$ in $H \cap K = \{e\}$, potem $G \cong H \rtimes_\phi K$, kjer je $\phi(k)(h) = khk^{-1}$.

Dokaz: $HK = \{hk\,;\, h \in H, k \in K\}$

Ker je H edinka, za vsak $k \in K$ velja $kHk^{-1} \subseteq H$, torej za vsak $h \in H$ velja $khk^{-1} \in H$. Torej je $\phi(k): H \to H$ dobro definirana.

Zakaj je $\phi(k)$ homomorfizem? $\phi(k)(h_1 h_2) =$
$= k(h_1 h_2)k^{-1} = kh_1k^{-1}kh_2k^{-1} = \phi(k)(h_1)\,\phi(k)(h_2)$.

Iščemo izomorfizem $f: H \times_\phi K \to G$.

$f(h,k) = hk$

Surjektivnost:

Ker je $HK = G$, je f surjektivna.

Injektivnost:

$f(h_1,k_1) = f(h_2,k_2) \iff h_1k_1 = h_2k_2 \overset{h_2^{-1}/\dots/k_1^{-1}}{\iff}$
$\iff h_2^{-1}h_1 = k_2k_1^{-1}$
($h_2^{-1}h_1 \in H$, $k_2k_1^{-1} \in K$)

$H \cap K = \{e\} \Rightarrow h_2^{-1}h_1 = k_2k_1^{-1} = e$

$h_2 / h_2^{-1}h_1 = e \Rightarrow h_1 = h_2$
enako se $k_1 = k_2$

Torej $(h_1,k_1) = (h_2,k_2)$.

Homomorfizem:

$f((h_1k_1)(h_2k_2)) = f(h_1\underbrace{\phi(k_1)(h_2)}_{k_1h_2k_1^{-1}}, k_1k_2) =$

$= h_1(k_1h_2k_1^{-1})k_1k_2 = (h_1k_1)(h_2k_2) =$

$= f(h_1, k_1) f(h_2, k_2)$

Torej je f res izomorfizem.

Zadnja trditev ima tudi inačico za dijelotni produkt, kjer dodatno zahtevamo, da sta obe edinki.

Trditev: Naj bo G grupa, $H, K \triangleleft G$ edinki, $HK = G$ in $H \cap K = \{e\}$. Potem je $G \cong H \times K$.

Dokaz: Kot za poldirektni produkt definiramo izomorfizem $f(h,k) = hk$ na $H \times K$. Edino vprašanje je, ali je $\phi(k) = id_H$ za vsak $k \in K$.

$$\phi(k)(h) = khk^{-1} \overset{?}{=} h \iff kh = hk \iff$$

($H \triangleleft G$)

$$\underbrace{khk^{-1}h^{-1}}_{\in H} = e \quad \text{in} \quad \underbrace{k(hk^{-1}h^{-1})}_{\in K}$$

Sledi: $khk^{-1}h^{-1} \in H \cap K = \{e\}$

Opomba: Če je $\phi(k)(h) = khk^{-1}$, včasih pišemo le $H \times K$ namesto $H \times_\phi K$. Temu ϕ rečemo konjugacija.

STRUKTURA NEKATERIH ZNANIH GRUP

GRUPA PERMUTACIJ S_n

Podgrupa sodih permutacij A_n je edinka v S_n.

Pokažimo, da je $S_n \cong A_n \times \mathbb{Z}_2$.

V vlogi drugega faktorja vzemimo $K = \{id, (12)\} \cong \mathbb{Z}_2$.
$(12) = \tau$

Očitno je $A_n \cap K = \{id\}$.

$A_n K = S_n$

$\pi \in S_n$: $\pi = \sigma \cdot \omega$, $\sigma \in A_n$, $\omega \in K$

1) π soda: $\pi \in A_n$: $\pi = \underset{A_n}{\pi} \circ \underset{K}{id}$ ✓
2) π liha: $\underset{soda}{\pi\tau} \in A_n$: $\pi = \underset{A_n}{(\pi\tau)} \circ \underset{K}{\tau}$ ✓

Po trditvi je $S_n \rtimes \mathbb{Z}_2$.

Ali lahko tudi A_n razcepimo na neke faktorje?

$n = 2$: $A_n = \{id\}$

$n = 3$: $A_n = \{id, (123), (132)\} \cong \mathbb{Z}_3$

$n = 4$: $H = \{id, (12)(34), (13)(24), (14)(23)\}$ (red $= 2$, red $= 2$, red $= 4$)
$H \triangleleft A_4$ (celo $H \triangleleft S_4$)

$H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ (Kleinov četverček)

$\{id, (12)(34)\}, \{id, (13)(24)\} \triangleleft H$

Želimo $A_4 \cong H \rtimes K$.

$|A_4| = \frac{4!}{2} = 12$
$|H| = 4$

$\Rightarrow$ Moč drugega faktorja je $|K| = 3$.

$K = \{id, (123), (132)\}$

Vidimo $H \cap K = \{e\}$ in $HK = A_4$.

$\Rightarrow A_4 \cong (\mathbb{Z}_2 \times_H \mathbb{Z}_2) \rtimes_K \mathbb{Z}_3$

Za $n \geq 5$ je A_n enostavna grupa, kar pomeni, da nima netrivialnih ediink (dokaz pri Algebri 3).

Enostavnost za $n \geq 5$ se uporabi pri dokazu, da polinomske enačbe stopnje ≥ 5 ne moremo rešiti "s formulo".

GRUPA TRANSLACIJ $T(\mathbb{R}^n)$

$T(\mathbb{R}^n) := \{T_a(x) = x + a;\ a \in \mathbb{R}\} \cong (\mathbb{R}^n, +)$,
kjer $T_a \mapsto a$ določa izomorfizem $T(\mathbb{R}^n)$ in $(\mathbb{R}^n, +)$

AFINA GRUPA $Aff(\mathbb{R}^n)$

$A: \mathbb{R}^n \xrightarrow{lin} \mathbb{R}^n$, $\det A \neq 0$

$Aff(\mathbb{R}^n) = \{\rho_{b,a}: \mathbb{R}^n \to \mathbb{R}^n;\ b \in \mathbb{R}^n, A \in GL(\mathbb{R}^n)\}$

$\rho_{b,A}(x) = Ax + b$

$T(\mathbb{R}^n) \triangleleft Aff(\mathbb{R}^n)$

$(T_a = \rho_{a,id})$

Preverimo, da za $a, b \in \mathbb{R}^n$ in $A \in GL(\mathbb{R}^n)$ velja:
$\rho_{b,A} \circ T_a \circ \rho_{b,A}^{-1} \in T(\mathbb{R}^n)$

Opazimo zanimivo: $\rho_{b,A} = T_b \circ A$ *

$\Rightarrow T_b \circ A \circ T_A \circ A^{-1} \circ T_b^{-1}$

$(A \circ T_a \circ A^{-1})(x) = A(T_a(A^{-1}x)) = A(A^{-1}x + a) \overset{A \text{ lin}}{=}$
$= A(A^{-1}x) + Ax = x + Aa$

$\Rightarrow A T_a A^{-1} = T_{Aa} \in T(\mathbb{R}^n)$

$\Rightarrow T_b \underbrace{A T_a A^{-1}}_{T_{Aa}} T_b^{-1} \in T(\mathbb{R}^n)$ ✓

$* \Rightarrow Aff(\mathbb{R}^n) = T(\mathbb{R}^n) \cdot GL(\mathbb{R}^n)$

$T(\mathbb{R}^n) \cap GL(\mathbb{R}^n) = \{id\}$

$\Rightarrow Aff(\mathbb{R}^n) = \mathbb{R}^n \rtimes GL(\mathbb{R}^n)$

ORTOGONALNA GRUPA $O(n)$

$O(n) = \{f : \mathbb{R}^n \to \mathbb{R}^n ;\ f \text{ izometrija},\ f(0) = 0\}$
$SO(n) = \{f \in O(n) ;\ \det f = 1\}$

Spomnimo se: $f \in O(n) \Rightarrow \det f = \pm 1$

Definirajmo: $\tau(x_1, x_2, \dots, x_n) = (-x_1, x_2, \dots, x_n)$

Očitno je $\det \tau = -1$ in $\tau^2 = id$.
$\Rightarrow H = \{id, \tau\} \leq O(n)$ podgrupa

Dokažimo, da je: $O(n) \cong SO(n) \rtimes \mathbb{Z}_2$

1) $SO(n) H = O(n)$

i) $\rho \in O(n)$, $\det \rho = 1$
$\Rightarrow \rho \in SO(n)$
$\Rightarrow \rho \in \rho \circ id$ ✓
($\rho \in SO(n)$, $id \in H$)

ii) $\rho \in O(n)$, $\det \rho = -1$
$\Rightarrow \rho = (\rho\tau)\tau$ ✓
($\rho\tau \in SO(n)$, $\tau \in H$)

$$\det(\rho\tau) = \det\rho \cdot \det\tau = (-1)(-1) = 1$$

2) $SO(n) \cap H = \{id\}$
Očitno, ker $\tau \notin SO(n)$

3) $SO(n) \triangleleft O(n)$ edinka

Naj bo $\sigma \in SO(n)$, $\rho \in O(n)$.
Želimo $\rho\sigma\rho^{-1} \in SO(n)$.

$$\det(\rho\sigma\rho^{-1}) = \det\rho \cdot \det\sigma \cdot \det\rho^{-1} =$$
$$= \det\rho \cdot \det\rho^{-1} \cdot \det\sigma =$$
$$= \det(\rho \cdot \rho^{-1}) \cdot \det\sigma = 1 \cdot 1 = 1$$
($\rho \cdot \rho^{-1} = id$)

DIEDERSKA GRUPA D_{2n}

Naloga: Prepričaj se, da je diederska grupa D_{2n} izomorfna $\mathbb{Z}_n \rtimes \mathbb{Z}_2$.

$$D_{2n} \cong \mathbb{Z}_n \rtimes \mathbb{Z}_2$$