Група $Q = \{1, -1, i, -i, j, -j, k, -k\}$

уз идентитете

$$(-1)^2 = 1, \quad i^2 = j^2 = k^2 = ijk = -1$$
$$ij = k, \quad ji = -k$$
$$jk = i, \quad kj = -i$$
$$ki = j, \quad ik = -j$$

Свака подгрупа групе Q је нормална.

Q припада класи Хамилтонових група, оних група код којих је свака подгрупа нормална.

<u>Лема</u> Алтернативна група A_4 је реда 12 и нема подгрупа реда 6.

<u>доказ</u>

$|A_n| = \frac{1}{2} n!$ за свако $n \in \mathbb{N}$, па је $|A_4| = 12$.

Ако A_4 садржи подгрупу H реда 6, онда $|G|H| = 2$.

На основу претходних лема следи да $\alpha^2 \in H$ за свако $\alpha \in A_4$.

Посматрамо циклусе дужине 3.

(...) Јасно је, сви циклуси дужине 3

припадају A_4

[illegible]

Нека је α један циклус дужине 3.

$\alpha^3 = \mathrm{Id} \Rightarrow \alpha^4 = \alpha.$

Дакле

$$(\alpha^2)^2 = \alpha$$

што значи $\alpha \in H$.

Међутим, 3-циклуса имамо 8, а $|H| = 6$. Контрадикција.

– Количничке групе

- теореме о изоморфизму (3)
- операције на косетима

Теорема о кореспонденцији

Нека је G група, а $H \trianglelefteq G$.

Посматрамо природни епиморфизам

$$\pi : G \to G/H$$

$$a \longrightarrow aH$$

Нека је $\mathrm{Sub}(G;H)$ скуп свих подгрупа групе G које садрже H, а $\mathrm{Sub}(G/H)$ скуп свих подгрупа групе G/H.

Нека је S подгрупа из $\mathrm{Sub}(G;H)$.

онда је $\{aH ; a \in S\}$
подгрупа у $Sub(G/H)$.
Тиме успостављамо кореспонденцију

$$S \to \varphi(S)$$

$S \in Sub(G;H)$, $\underbrace{\varphi(S) = \{aH | a \in S\}}_{S^*}$

$\in Sub(G/H)$.

$\varphi(S) = S^*$.

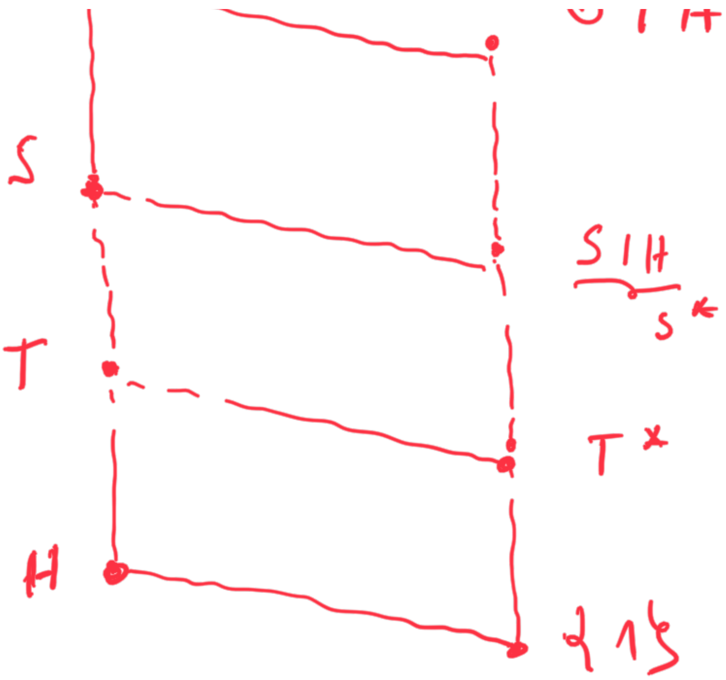
<u>Теорема</u>

Нека је G група, а $H \trianglelefteq G$. Посматрамо природни епиморфизам $\pi : G \to G/H$, успостављамо пресликавање φ између $Sub(G;H)$ и $Sub(G/H)$

$$\varphi : S \to S^*$$

$$S^* = \{aH | a \in S\}.$$

Онда је φ бијекција.



Ако су T, S подгрупе групе G које садрже H

и $T \leq S$, онда $T^* \leq S^*$

и $[S:T] = [S^*:T^*]$ и

$T \trianglelefteq S$ ако и само ако $T^* \trianglelefteq S^*$, при

чему је $S/T \cong S^*/T^*$

<u>Пример</u>

Нека је $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

$|G| = 8$

$(G, +_2)$.

$$(i,j,k) + (i,j,k) = (0,0,0)$$

<u>Лема (Кошијева)</u>

Нека је G коначна Абелова група и p прост број такав да $p \mid |G|$.
Онда, G садржи елемент реда p.

<u>доказ</u>

Доказ вршимо индукцијом по $|G|$.

Ако је $n = 1 = |G|$, тврђење је тривијално јер не постоји прост број p, такав да $p \mid |G|$.

Ако је $n = |G| > 1$, онда претпоставимо да је $a \in G$ елемент такав да $\mathrm{ord}(a) = k > 1$.

1° Нека је $p \mid k$.
Онда је $a^{\frac{k}{p}}$ реда p.

2° Уколико $p \nmid k$, посматрајмо $H = \langle a \rangle$.
Пошто је G Абелова онда $H \trianglelefteq G$.
Посматрајмо G / H.
$|G/H| = \frac{n}{k}$
Пошто $p \nmid k$, онда $p \mid \frac{n}{k}$;

а како је $\frac{n}{k} < n$, онда по индуктивној претпоставци у G/H постоји елемент реда p.

Нека је то $bH \in G/H$, $b \in G$. Нека је $\mathrm{ord}(b) = m$.

$b^m = 1$.

$(bH)^m = H$

Међутим, ред bH је p.

Дакле $p \mid m$, што значи да $b^{\frac{m}{p}}$ има ред p.

<u>Лема</u> Нека је G коначна Абелова група и $d \mid |G|$. Онда G садржи подгрупу реда d.

<u>доказ</u>

Доказ изводимо индукцијом.
$|G| = 1$ је тривијално.
Нека је $d \mid |G|$, $d > 1$.
Онда постоји p, прост број, $p \mid d$.
По претходној леми знамо да постоји H,

По претходној леми, ...
подгрупа у G, тако да $|H| = p$.
Јасно, $H \trianglelefteq G$, па је група G/H реда $\frac{n}{p}$.
По индуктивној претпоставци, постоји подгрупа S^* у G/H реда $\frac{d}{p}$.

На основу теореме о кореспонденцији, постоји S, подгрупа у G, таква да

$$[G : S] = [G^* : S^*]$$

одакле је $|S| = d$.

<u>пример</u>

$\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ скуп свих остатака по модулу m.

$(\mathbb{Z}_m, +_m)$ је Абелова група

$\mathbb{I}_m = \{ a \in \mathbb{Z}_m \mid \text{НЗД}(a, m) = 1 \}$

$(\mathbb{I}_m, \cdot_m)$ је Абелова група

$|\mathbb{I}_m| = \varphi(m)$, φ - Ојлерова функција.

<u>φ је мултипликативна функција</u>

Ако су $k, \ell \in \mathbb{N}$ такви да $\text{НЗД}(k, \ell) = 1$
онда $\varphi(k\ell) = \varphi(k) \cdot \varphi(\ell)$.

p - прост број

$$\varphi(p) = p-1$$

$$\varphi(p^2) = ?$$

$$1, \dots, p, \dots, 2p, \dots, (p-1)p, \dots, p^2-1$$

$$\varphi(p^2) = p^2 - p = (p^2-1) - (p-1).$$

$$\vdots$$

$$\varphi(p^m) = p^m - p^{m-1}$$

$n = p_1^{s_1} \cdots p_k^{s_k}$ $\quad p_i$ - прости бројеви

$$\varphi(n) = \varphi\left(\prod_{i=1}^{k} p_i^{s_i}\right) = \prod_{i=1}^{k} \varphi(p_i^{s_i})$$

$$= \underline{\prod_{i=1}^{k} \left(p_i^{s_i} - p_i^{s_i-1}\right)} = \prod_{i=1}^{k} p_i^{s_i}\left(1 - \frac{1}{p_i}\right)$$

$$= n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

(p - прост број)

<u>Зад</u> Нека је $n \in \mathbb{N}$.

Онда је $\boxed{n = \sum_{d \mid n} \varphi(d)}$

<u>Упутство:</u>

Ако је G кон. циклична група реда n, онда за свако d, $d \mid n$, постоји јединствена циклична група реда d, $|H| = d$, $H \leq G$.
Број елемената реда d у H је $\varphi(d)$.

Примјер

$n = 12$, $d \in \{1, 2, 3, 4, 6, 12\}$

$$\left.\begin{aligned} \varphi(1) &= 1, \\ \varphi(2) &= 1, \\ \varphi(3) &= 2, \\ \varphi(4) &= 2, \\ \varphi(6) &= 2, \\ \varphi(12) &= 4. \end{aligned}\right\} + \quad = 12.$$

Теорема Група G реда n је циклична ако и само ако за сваки дјелитељ d од n постоји највише једна подгрупа реда d.

Дејства групе на скуп (group actions)

Теорема (Кејли)

Свака група G је изоморфна подгрупи симе-

симетричне групе S_G (група свих бијекција на скупу G),

Специјално, ако је $|G| = n$, онда је G изоморфна подгрупи S_n.

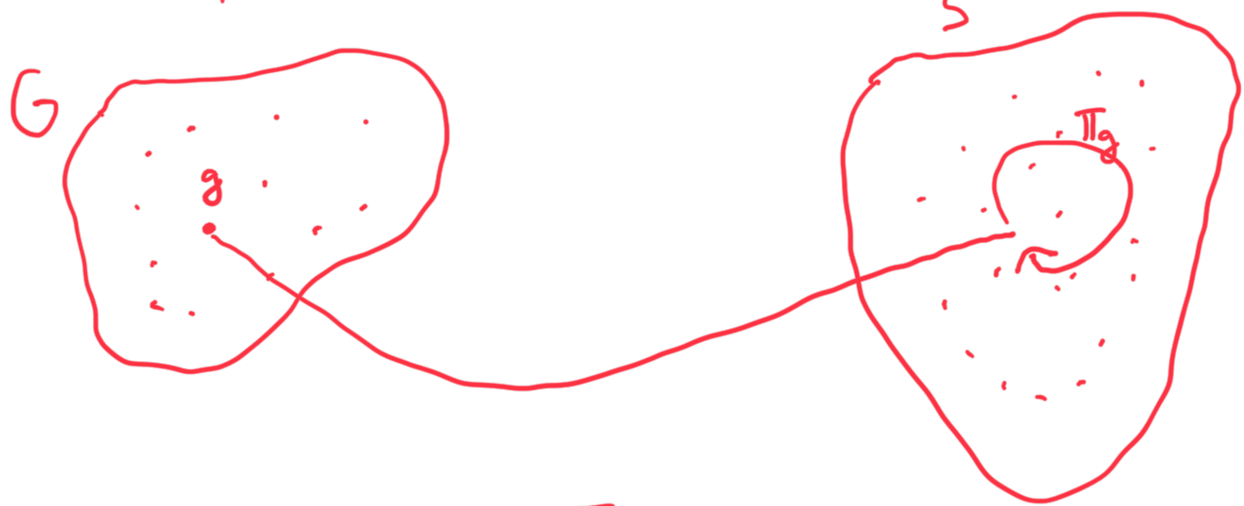
<u>доказ</u>:

$$a \in G \longrightarrow \tau_a \in S_G$$

$$\tau_a(x) = ax, \quad x \in G.$$

Ова кореспонденција је мономорфизам.

Дакле, $G \cong \mathrm{Im}(G) \le S_G$.



$$g \longrightarrow \Pi_g$$

Π_g је пермутација скупа S

$$\phi : G \to \underbrace{\mathrm{Sym}(S)}_{\text{скуп свих бијекција скупа } S}$$

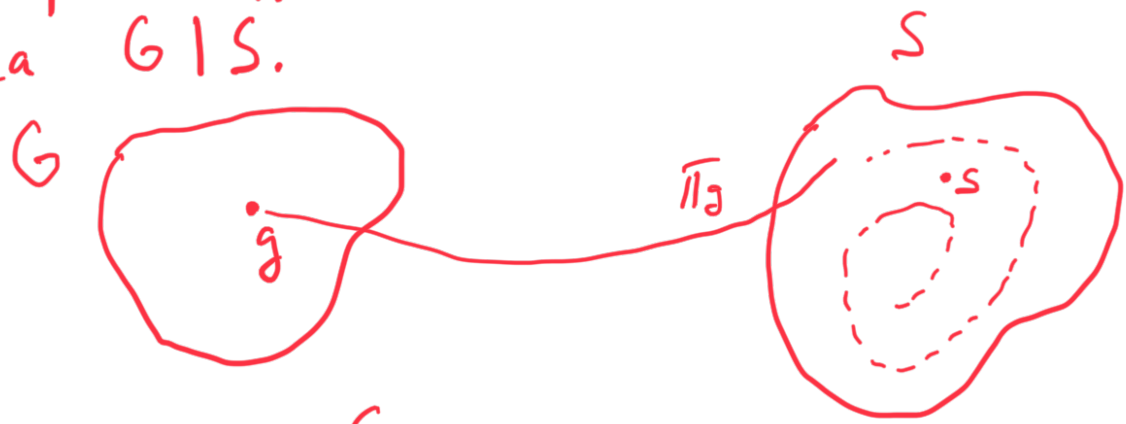
$$\phi(g) = \Pi_g$$

$\varphi(g) \quad g.$

Уколико је φ хомоморфизам, онда за φ кажемо да је то <u>дејство групе G на скуп S</u>.

$$\varphi(g_1 \cdot g_2) = \pi_{g_1} \circ \pi_{g_2}.$$

Дејство групе G на скуп S означавамо са $G | S$.



$$\pi_g(s) \in S$$

Често се означава

$$\pi_g(s) := s^g$$

<u>Теорема</u> Нека је G група, а $H \leq G$ коначног индекса n. Онда постоји хомоморфизам $f : G \to S_n$, тако да $\operatorname{Ker} f \leq H$.

<u>скица доказа</u>

$$G | H = \{ aH \mid a \in G \}$$

$$|G | H| = n$$

$$\underbrace{G \ni a \longrightarrow \tau_a : G/H \to G/H}_{f}$$

$f(a) = \tau_a$

$\tau_a(bH) = (a \cdot b)H$

- f је хомоморфизам
- τ_a је бијекција на G/H
- $\operatorname{Ker} f \leq H$

$$\underbrace{H, a_1H, \dots, a_{n-1}H}_{\in G/H}$$

$$\tau_g : \begin{pmatrix} H & a_1H & \dots & a_{n-1}H \\ gH & ga_1H & \dots & ga_{n-1}H \end{pmatrix}$$

Ако је $\tau_g \equiv Id_{G/H}$

онда $gH = H \Rightarrow g \in H$.

<u>Лема</u> Нека је G група реда 6.

Онда је $G \cong \mathbb{Z}_6$ или $G \cong S_3$.

<u>доказ:</u>

Могући редови елемената у G су:

2, 3, 6.

Ако G има елемент реда 6 $\Rightarrow$ $G \cong \mathbb{Z}_6$. √

Ако G не посједује елемент реда 6, показујемо да G мора у сваком случају да има елемент реда 2.

Наиме, G је група парног реда.

У групи парног реда имамо непаран број елемената реда 2.

<u>G је Абелова</u>

$a \in G$ је реда 2.

По Кошијевој теореми, постоји $t \in G$ реда 3.

$at \in G$

Ред at мора бити 6.

Дакле $G \cong \mathbb{Z}_6$.

<u>G није Абелова</u>

Ако G нема елемената реда 3, онда за свако $x \in G$, $x^2 = 1$.

У том случају, G би била Абелова.

Дакле, G мора садржати $s \in G$ реда 3.

Онда $K = \langle s \rangle$ је индекса 2 у G, што

та је $K \trianglelefteq G$.

Нека је a елемент реда 2 у G.

$a = a^{-1}$.

$$asa^{-1} = asa \in K$$

$\Rightarrow asa = s^i \quad i = 0, 1, 2.$

Елиминацијом $i = 0, 1$, закључујемо

$asa = s^2 = s^{-1}$

Нека је $H = \langle a \rangle$. $|H| = 2$.

$$f : G \longrightarrow Sym(G|H)$$

$$g \longrightarrow \tau_g$$

$$G|H = \{H, sH, s^2H\}$$

$\operatorname{Ker} f \leq H$ (претходна лема)

Ако претпоставимо да је $a \in \operatorname{Ker} f$

то значи да је

$\begin{pmatrix} H & sH & s^2H \\ aH & asH & as^2H \end{pmatrix}$ идентитет

(покажите сами)

f је инјекција

$G \cong Im(f) = \underbrace{Sym(G|H)}$

S_3