Direktni produkt (notranji) $N_1 \ldots N_s \trianglelefteq G$

$$G = N_1 \cdot N_2 \cdot \ldots \cdot N_s \quad \wedge \quad N_i \cap N_{i+1} = \{1\} \text{ za } \forall i$$

- $\Leftrightarrow \forall g \in G.\ g = n_1 \cdot \ldots \cdot n_s \quad n_i \in N_i$ enoličen zapis

Komutator x in y je $[x,y] = xyx^{-1}y^{-1}$

- $M, N \trianglelefteq G,\ M \cap N = \{1\} \Rightarrow mn = nm \ \forall n \in N.\ \forall m \in M$

- $\underbrace{G = N_1 \cdot N_2 \cdot \ldots \cdot N_s}_{\text{notranji direktni produkt}} \Rightarrow G \cong \underbrace{N_1 \times N_2 \times \ldots \times N_s}_{\text{zunanji direktni produkt}}$

(Velja za končne grupe)

Abelove grupe

- $|G| = mn$; m, n tuji
  $H = \{x \in G;\ mx = 0\}$ $K = \{x \in G;\ nx = 0\}$
  Potem $G = H \oplus K$ in $|H| = m$;
- Posledica: $\forall$ končna abelova grupa je vsota p-grup
- p-grupa je ciklična $\Leftrightarrow$ vsebuje natanko 1 grupo moči p
- $\forall$ končna abelova abelova grupa je izomorfna direktni vsoti cikličnih p-grup

- končna abelova grupa G $|G| = p_1^{a_1} \cdot \ldots \cdot p_s^{a_s}$
  $H_i = \{x \in G;\ p_i^{a_i} x = 0\}$
  $\Rightarrow |H_i| = p_i^{a_i}$ $G = H_1 \oplus \ldots \oplus H_s$

- vsaka končno generirana abelova grupa je končna direktna vsota cikličnih grup

$$= \mathbb{Z}^m \oplus \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_n$$

KONČNE GRUPE

Delovanje $G \curvearrowright X$

1) $g\cdot(h\cdot x) = (gh)\cdot x$
2) $1\cdot x = x$

(levo delovanje)

Imamo delovanje $G \curvearrowright X$. Potem

$$\Phi : G \longrightarrow \mathrm{Sym}X$$
$$\Phi : g \longmapsto (x \longmapsto gx)$$

je homomorfizem

$\ker\Phi$ je **jedro delovanja**

Orbita $G\cdot x = \{g\cdot x \,;\, g \in G\}$

Stabilizator $G_x = \{g \in G \,;\, gx = x\}$

Fiksne točke g-ja $X^g = \{x \in X \,;\, gx = x\} = \mathrm{fix}(g)$

Fiksne točke (invariante)

$$X^G = \bigcap_{g\in G} X^g = \{x \in X \,;\, \forall g \in G \,.\, gx = x$$

- $G_x \leq G$
- $x \sim y \iff \exists g \in G \,.\, y = gx$. Ekvivalenčni razredi so obrbite $(G\cdot x)$

$$X/G = X/\sim \quad \text{prostor orbit}$$

- **Tranzitivno delovanje** delovanje z eno orbito

- $\forall x \in X \,.\, |G\cdot x| = [G : G_x]$

- G končna $\implies |G| = |G_x| \cdot |G x|$

- $\forall$ končno grupo G lahko vložimo v simetrično grupo S_n za nek $n \in \mathbb{N}$

Uporabne grupe ki niso izomorfne $\mathbb{Z}_n$

$4: \mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong \{id, (12), (34), (12)(34)\}$

$6: D_6 \cong S_3$

$8: \mathbb{Z}_4 \oplus \mathbb{Z}_2,\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2,\ D_8,\ Q$

$9: \mathbb{Z}_3 \oplus \mathbb{Z}_3$

$10: D_{10}$

$12: \mathbb{Z}_6 \oplus \mathbb{Z}_2, D_{12}, Dic_{12}, A_4 = \{ id,$

$\underbrace{(12)(34), (13)(24), (14)(23)}_{\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2}, (123), (132), (234),$

$(243), (341), (314), (412), (421)\}$

$14: D_{14}$

$$\mathbb{Z}_{12} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_3$$

- G p-grupa. $G \curvearrowright X \implies |X| \equiv |X^G| \mod p$
- Burnsidova lema $|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$
- $G \curvearrowright X$ netrivialno delovanje
  $\exists x_1 \dots x_r \in X - X^G \quad |X| = |X^G| + \sum_{i=0}^{r} |G : G_{x_i}|$
- Razredna formula
  $\exists x_1, \dots x_r \in X - Z(G).\ |G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(x_i)]$
- G p-grupa $\Rightarrow Z(G) \neq \{1\} \quad (p \mid |Z(G)|)$
- $|G| = p^2 \Rightarrow G$ je abelova
- Cauchyjev izrek $p \mid |G| \Rightarrow \exists a \in G.\ \mathrm{red}(a) = p$
- Lagraangev izrek $H \leq G \Rightarrow |H| \mid |G|$
- $H \leq G$ je p-podgrupa Sylowa če
  $|H| = p^\alpha; \quad p^\alpha \mid |G|; \quad p^{\alpha+1} \nmid |G|$
- Izrek Sylowa
  1) $p^\rho \mid |G| \Rightarrow \exists H \leq G.\ |H| = p^\rho$
  ($\exists$ p-podgrupa Sylowa)
  2) $\forall$ p-podgrupa G je vsebovana v p-podgrupi Sylowa
  3) Vse p-podgrupe Sylowa v G so konjugirane med sabo
  4) $n_p \dots$ št p-podgrup Sylowa
  $n_p \mid |G|; \quad n_p \equiv 1 \mod p$

$H \leq G$. $N(H) = \{a \in G ; aHa^{-1} = H\}$
je normalizator.

- velja: $N(H) \leq G$ $\quad H \triangleleft N(H)$
- $N(H) = G \Leftrightarrow H \triangleleft G$
- $n_p = 1 \Leftrightarrow S \triangleleft G$
- grupa je enostavna če sta $\{1\}$ in G edini edinki
- A_n je enostavna za $\forall n \in \mathbb{N} - \{4\}$
- grupa G je rešljiva, če $\exists$ končno zaporedje $\{1\} = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_k = G$
  $G_i \triangleleft G_{i+1}$; G_{i+1}/G_i abelove
- G rešljiva $\Longrightarrow$

  1) $H \leq G$ $\quad H$ rešljiva

  2) $N \triangleleft G \Rightarrow G/N$ rešljiva
- $N \triangleleft G$ rešljiva in G/N rešljiva $\Rightarrow G$ rešljiva

- konjugirana podgrupa aHa^{-1}
  za nek $a \in G$
- $H, K \leq G$ sta konjugirani če $aHa^{-1} = K$
- (levi) odsek $aH = \{ah ; h \in H\}$

  $$aH = bH \iff ab^{-1} \in H$$

- Fermatov mali izrek: $a^p \equiv a \mod p$
- $\varphi : G \longrightarrow G'$ homomorfizem
  - a) $H' \leq G' \Rightarrow \varphi^*(H') \leq G$
  - b) $N' \triangleleft G' \Rightarrow \varphi^*(N') \triangleleft G$
  - c) $H \leq G \Rightarrow \varphi_*(H) \leq G'$
  - d) $N \triangleleft G \wedge \varphi$ surj. $\Rightarrow \varphi(N) \triangleleft G'$
- korespondenčni izrek
  - a) $\forall$ podgrupa grupe H/N je oblike H/N
    kjer $H \leq G$ in $N \subseteq H$
  - b) $\forall$ edinka grupe G/N je oblike M/N
    kjer $M \triangleleft G$ in $N \subseteq M$
- K komutativen kolobar $M \triangleleft K$
  M maksimalen $\iff K/M$ je polje

Komutatorska podgrupa $[G,G] = G' = \{a^{-1}b^{-1}ab \,;\, a,b \in G\}$

- $H \triangleleft G \wedge G/H$ abelova $\Rightarrow [G,G] \subseteq H$
- $H < G$. $H \triangleleft G \Leftrightarrow [H,G] < H$
- $[G,G] \triangleleft G$
- $G/[G,G]$ je abelova

komutatorska vrsta $G \triangleright G' \triangleright G'' \triangleright \ldots$

- G je rešljiva $\Leftrightarrow$ komutatorska vrsta doseže $\{1\}$
- f epimorfizem $G \to H$. $f_*(G^{(k)}) = H^{(k)}$
- $H \triangleleft G \Rightarrow H' \triangleleft G$ $(H^{(k)} \triangleleft G$ za $\forall k)$
- A, B rešljivi. $\Rightarrow A \times B$ rešljiva
- $\forall$ končna p grupa je rešljiva
- $\forall$ grupa reda $p \cdot q$ $p \neq q$, $p, q \in \mathbb{P}$ je rešljiva
- grupa reda $8p$ je rešljiva