Direktni produkt (notranji) $N_1 \dots N_s \triangleleft G$

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

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

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

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

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

(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

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 $(G\cdot x)$

  $X/G = X/\sim$ prostor orbit

- Tranzitivno delovanje delovanje z eno orbito

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

- G končna $\Longrightarrow |G| = |Gx|\cdot|G_x|$

- G p-grupa. $G \curvearrowright X \Rightarrow |X| \equiv |X^G| \bmod p$
- Burnsidova lema $|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$
- 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 $p \mid |G| \Rightarrow \exists a \in G.\ red(a) = p$
- 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) $p^\ell \mid |G| \Rightarrow \exists H \leq G.\ |H| = p^\ell$
     ($\exists$ 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
     $n_p \mid |G|\quad ;\quad n_p \equiv 1 \bmod p$

S p-podgrupa Sylowa; normalizator S v G je $N_G(S) = \{g \in G;\ gSg^{-1} = S\}$

- $n_p = 1 \Leftrightarrow S \triangleleft G$
- 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 abelova

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

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

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

$6: D_6 \cong S_3$

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

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

$10: D_{10}$

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

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

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

$14: D_{14}$

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

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

- Fermatov mali izrek: $a^p \equiv a \mod p$
- $\varphi : G \longrightarrow G'$ homomorfizem
  a) $H' \leq G' \Rightarrow \varphi^*(H') \leq G$
  b) $N' \lhd G' \Rightarrow \varphi^*(N') \lhd G$
  c) $H \leq G \Rightarrow \varphi_*(H) \leq G'$
  d) $N \lhd G \wedge \varphi$ surj. $\Rightarrow \varphi(N) \lhd G'$

- 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 $M \lhd G$ in $N \subseteq M$

- K komutativen kolobar $M \lhd K$
  M maksimalen $\Leftrightarrow K/M$ je polje

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

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