Naj bosta $H, K \lhd G$. G je notranji direktni produkt H in K, če je $H \cap K = \{1\}$ in $G = HK$.

Pokaži, da je D_{12} notranji direktni produkt grup $H = \langle r^2, z \rangle$ in $K = \langle r^3 \rangle$.

K je edinka, ker je $K \subseteq Z(D_{12})$.

$H \cap K = \{1\}$

Naj bo $g \in D_{12}$. Če je $g \in H$ ali $g \in K$, potem očitno $g = h \cdot k$ za neka $h \in H, k \in K$.

Sicer $g \notin H, g \notin K$.

$\Rightarrow g = r, r^5, zr, zr^3, zr^5$

Želimo $g = h \cdot r^3$ za $h \in H$. Pokažimo $gr^{-3} \in H$.

$g = z^i r^{2k+1}$

$\Rightarrow gr^{-3} = z^i r^{2k-2} \in H$

Naj bo G nekomutativna grupa in $|G| < 12$. Pokaži, da G ni notranji direktni produkt dveh svojih pravih edink.

Če je G direktni produkt H in K, je $|G| = |H| \cdot |K|$.

$\Rightarrow |H|, |K| \leq 5$

$\Rightarrow H, K$ Abelovi

$\Rightarrow H \times K$ Abelova

$G \cong H \times K$

$\Rightarrow G$ Abelova

Za katera naravna števila je grupa O_n notranji direktni produkt edink SO_n in $\{I, -I\}$?

$O \in O_n \Rightarrow O^T O = I$

Očitno $I \in SO_n$ in $-I \in SO_n$ za sode n.

$\Rightarrow$ Če je n sod, je $SO_n \cap \{I, -I\} \neq \{I\}$.

$\Rightarrow$ Za sode n ni direktni produkt.

Za lihe n je $SO_n \cap \{I, -I\} = \{I\}$.

Ker so O_n ortogonalne matrike, je $\det A = \pm 1$ za vse $A \in O_n$.

$\det A = 1: \quad A = A \cdot I$
$\det A = -1: \quad A = (-A) \cdot (-I)$

Naj bo $n \geq 5$. Pokaži, da ne obstaja taka edinka $N \triangleleft S_n$, da bi bila S_n notranji direktni produkt N in A_n.

$$S_n \cong A_n \times N \Rightarrow |N| = [S_n : A_n] = 2$$

$N = \{id, a\}$, red $a = 2$

$\Rightarrow$ a je produkt disjunktnih transpozicij (red elementa S_n je lcm dolžin disjunktnih ciklov).

$$bab^{-1} = a \quad \forall b \in S_n$$

$$\Rightarrow ba = ab$$

$$\Rightarrow a \in Z(S_n)$$

$$\Rightarrow a = id$$

$$\Rightarrow |N| = 1$$

Opomba: Če je $H \triangleleft G$, $K \leq G$, $H \cap K = \{1\}$ in $G = HK$, potem je G semidirektni produkt H in K:

$$G \cong H \rtimes K$$

S_n je semidirektni produkt A_n in $N := \{id, (1\ 2)\}$:

$g \in A_n: \quad g = g \cdot 1 \in A_n N$
$g \notin A_n: \quad g = (g(12))\,(12) \in A_n N$

KONČNE ABELOVE GRUPE

Ali je $\mathbb{Z}_{12} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_4$ in ali je $\mathbb{Z}_{12} \cong \mathbb{Z}_6 \oplus \mathbb{Z}_2$?

$\gcd(n,m) = 1 \Leftrightarrow \mathbb{Z}_{nm} \cong \mathbb{Z}_n \oplus \mathbb{Z}_m$

$\mathbb{Z}_{12} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_4 \quad (\mathbb{Z}_3 \oplus \mathbb{Z}_4 = \langle (1,1) \rangle \cong \mathbb{Z}_{12})$

$\mathbb{Z}_{12} \not\cong \mathbb{Z}_6 \oplus \mathbb{Z}_2$

$\mathbb{Z}_{p^{k_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{k_n}} \cong \mathbb{Z}_{p^{l_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{l_m}}$
in $k_1 \geq \ldots \geq k_n$ in $l_1 \geq \ldots \geq l_m$

$\Rightarrow n = m$ in $k_i = l_i$

Pokaži naslednja izomorfizma.

a) $\mathbb{Z}_{36} \oplus \mathbb{Z}_{24} \cong \mathbb{Z}_{72} \oplus \mathbb{Z}_{12}$

$$\mathbb{Z}_{36} \oplus \mathbb{Z}_{24} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_8 \cong (\mathbb{Z}_9 \oplus \mathbb{Z}_3) \oplus (\mathbb{Z}_8 \oplus \mathbb{Z}_4)$$

$$\mathbb{Z}_{72} \oplus \mathbb{Z}_{12} \cong \mathbb{Z}_9 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong (\mathbb{Z}_9 \oplus \mathbb{Z}_3) \oplus (\mathbb{Z}_8 \oplus \mathbb{Z}_4)$$

b) $\mathbb{Z}_{78} \oplus \mathbb{Z}_{18} \cong \mathbb{Z}_{26} \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_6$

$$\mathbb{Z}_{78} \oplus \mathbb{Z}_{18} \cong \mathbb{Z}_{13} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_2 \cong$$
$$\cong \mathbb{Z}_{13} \oplus (\mathbb{Z}_9 \oplus \mathbb{Z}_3) \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_2)$$

$$\mathbb{Z}_{26} \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_6 \cong \mathbb{Z}_{13} \oplus (\mathbb{Z}_9 \oplus \mathbb{Z}_3) \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_2)$$

Do izomorfizma natančno natančno določi vse Abelove grupe reda 324.

$324 = 4 \cdot 81 = 2^2 \cdot 3^4$

Grupe reda 2^2:

$\mathbb{Z}_4, \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Grupe reda 3^4:

$\mathbb{Z}_{81}, \mathbb{Z}_{27} \oplus \mathbb{Z}_3, \mathbb{Z}_9 \oplus \mathbb{Z}_9, \mathbb{Z}_9 \oplus \mathbb{Z}_9, \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3,$
$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$

$G = H \oplus K$

$|H| = 2^2$
$|K| = 3^4$

$\Rightarrow 2 \cdot 5 = 10$ možnosti

Določi število neizomorfnih Abelovih grup reda $7^2 \cdot 3^2 \cdot 2^5$.

Grupe reda 7^2:

$7^2, 7 \cdot 7$

$\rightsquigarrow 2$

Grupe reda 3^2:

$3^2, 3 \cdot 3$

$\rightsquigarrow 2$

Grupe reda 2^5:

$2^5, 2^4 \cdot 2, 2^3 \cdot 2^2, 2^3 \cdot 2 \cdot 2, 2^2 \cdot 2^2 \cdot 1, 2^2 \cdot 2 \cdot 2 \cdot 2,$
$2 \cdot 2 \cdot 2 \cdot 2 \cdot 2$

$\rightsquigarrow 7$

$\Rightarrow \# = 2 \cdot 2 \cdot 7 = 28$

G p-grupa, H q-grupa, $p \neq q$ praštevili

Pokaži: G in H sta ciklični $\Leftrightarrow$ $G \oplus H$ je ciklična

$(\Rightarrow)$ $|G| = p^k$, $G \cong \mathbb{Z}_{p^k}$
$|H| = q^n$, $H \cong \mathbb{Z}_{q^n}$

p^k, q^n tuji

$\Rightarrow G \oplus H \cong \mathbb{Z}_{p^k q^n}$

$(\Leftarrow)$ $G \oplus H$ ciklična

$\Rightarrow G \oplus H$ Abelova

$\Rightarrow G, H$ Abelovi

$$|G \oplus H| = p^s q^t$$

$$G \oplus H \cong \underbrace{\overbrace{\mathbb{Z}_{p^{\alpha_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{\alpha_k}}}^{p^s}}_{G'} \oplus \underbrace{\overbrace{\mathbb{Z}_{q^{\beta_1}} \oplus \ldots \oplus \mathbb{Z}_{q^{\beta_l}}}^{q^t}}_{H'}$$

$G \oplus H$ ima element reda $p^s q^t$

$\Rightarrow G'$ ima element reda p^s
H' ima element reda q^t

$$\Rightarrow G' \cong \mathbb{Z}_{p^s}$$
$$H' \cong \mathbb{Z}_{q^t}$$

Zaradi enoličnosti zapisa velja:

$$G = G'$$
$$H = H'$$

Pokaži: Končna Abelova grupa je ciklična natanko tedaj, ko za vsako praštevilo p, kjer $p \mid |G|$, velja, da G vsebuje natanko $p-1$ elementov reda p.

$(\Rightarrow)$ G je ciklična

$$G \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \ldots \oplus \mathbb{Z}_{p_1^{\alpha_k}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{\beta_1}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{\beta_m}}$$

G je ciklična $\Longleftrightarrow k = 1, \ldots, m = 1$

$$G \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{\alpha_s}}$$

$|G| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$

BŠS: $p = p_1$

Pokažimo, da G ima natanko $p_1 - 1$ elementov reda p_1.

$(a_1, a_2, \dots, a_s)$ ima red $p_1 \Leftrightarrow (\overset{\text{red } p_1}{a_1}, 0, \dots, 0)$

Elementi reda p v $\mathbb{Z}_{p^\alpha}$:

$p^{\alpha-1}, 2 \cdot p^{\alpha-1}, \dots, (p-1) \cdot p^{\alpha-1}$

Torej imamo natanko $p-1$ elementov reda p.

$(\Leftarrow)$ $G \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \dots \oplus \mathbb{Z}_{p_1^{\alpha_k}} \oplus \dots \oplus \mathbb{Z}_{p_s^{\beta_1}} \oplus \dots \oplus \mathbb{Z}_{p_s^{\beta_m}}$

Za vsak p imamo natanko $p-1$ elementov reda p.

$\Rightarrow \mathbb{Z}_{p_1^{\alpha_1}} \oplus \dots \oplus \mathbb{Z}_{p_1^{\alpha_k}}$ ima natanko $p_1 - 1$ elementov reda p_1.

Pokažimo, da je $k = 1$.

Recimo, da je $k \geq 2$. Potem ima že $\mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}}$ vsaj $(p_1 - 1)^2 + \dots$ elementov reda p_1.

Če je $p_1 = 2$, dodatno imajo še (a,b), $(a,0)$, $(0,b)$ red 2. Sicer je že dk.

Torej je $k = 1$.

Naj bo G končna Abelova grupa in $|G| = n$. Pokaži, da za vsak delitelj m števila n, G ima podgrupo reda m.

Primer:

$|G| = 200$, G Abelova

Pokaži: G ima podgrupo reda 20

$200 = 2 \cdot 10^2 = 2^3 \cdot 5^2$

$G \cong G_1 \oplus G_2$
$|G_1| = 2^3 = 8$
$|G_2| = 5^2 = 25$

$20 = 2 \cdot 10 = 2^2 \cdot 5$

$H \cong H_1 \oplus H_2$
$|H_1| = 2^2 = 4$
$|H_2| = 5$

Dovolj je pokazati:

G_1 ima podgrupo H_1 reda 4
G_2 ima podgrupo H_2 reda 5

G_1: $\mathbb{Z}_8 \rightsquigarrow 2 \cdot \mathbb{Z}_8$
$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \rightsquigarrow 2\mathbb{Z}_4 \oplus \mathbb{Z}_2$
$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \rightsquigarrow \underbrace{2\mathbb{Z}_2}_{=\{0\}} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Imamo podgrupo reda 4.

Enako za G_2 ...

Splošno:

Dovolj je pokazati:

Vsaka podgrupa reda p^k ima podgrupo reda p^ℓ $(0 < \ell \leq k)$.

Naj bo $G = A_4$. Pokaži, da G nima podgrupe reda 6. Torej prejšnja trditev v splošnem ne velja.

$$A_4 = \{ \underset{8}{(i\,j\,k)},\ \underset{1}{1},\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3) \}$$

Predpostavimo, da obstaja podgrupa H reda 6.

Potem je H edinka.

$$|A_4/H| = 2$$

Kanonični epimorfizem:

$$\begin{aligned} \varphi : A_4 &\longrightarrow A_4/H \\ g &\longmapsto gH \end{aligned}$$

$g = (1\,2\,3)$

$\varphi(g)$ ima red $\underline{\underline{1}}$ ali 3

$\varphi(g) \in \mathbb{Z}_2$

$\Rightarrow \varphi(g) = 1 \quad \in \ker \varphi$

$\ker \varphi = H \Rightarrow |\ker \varphi| = 6$

$(i\ j\ k) \in \ker \varphi \Rightarrow |\ker \varphi| \geq 8$

Pokaži, da je podgrupa $B = \langle (1,1), (1,3) \rangle$ grupe $\mathbb{Z} \oplus \mathbb{Z}$ izomorfna grupi $\mathbb{Z} \oplus \mathbb{Z}$ in da je $(\mathbb{Z} \oplus \mathbb{Z})/B \cong \mathbb{Z}_2$.

$\mathbb{Z} \oplus \mathbb{Z}$ je generirana z $(1,0)$ in $(0,1)$.

$\varphi : \mathbb{Z} \oplus \mathbb{Z} \to B$

$\varphi(1,0) := (1,1)$
$\varphi(0,1) := (1,3)$

φ ohranja množenje generatorjev

$\Rightarrow \varphi$ se razširi do homomorfizma

$\varphi(\alpha, \beta) = \varphi(\alpha(1,0) + \beta(0,1)) =$

$= \alpha(1,0) + \beta(1,3) = (\alpha + \beta, \alpha + 3\beta)$

φ je injektiven

$\varphi(\alpha, \beta) = (0,0)$

$(\alpha + \beta, \alpha + 3\beta) = (0,0)$

$\alpha+\beta=0 \iff \alpha=-\beta$
$\alpha+3\beta=0 \iff 2\beta=0 \iff \beta=0=\alpha$

$\ker\varphi=\{(0,0)\}$

φ je surjektiven

$(1,1)\in \operatorname{im}\varphi$
$(1,3)\in \operatorname{im}\varphi$

$\Rightarrow \forall \alpha,\beta\in\mathbb{Z}: \ \alpha(1,1)+\beta(1,3)\in\operatorname{im}\varphi$

$\langle(1,1),(1,3)\rangle=\{\alpha(1,1)+\beta(1,3)\ ;\ \alpha,\beta\in\mathbb{Z}\}$

$\Rightarrow \varphi$ je izomorfizem

$(\mathbb{Z}\oplus\mathbb{Z})/B \cong \mathbb{Z}_2$

$\varphi:\mathbb{Z}\oplus\mathbb{Z}\to\mathbb{Z}_2$
$\ker\varphi=B$

$\varphi(\alpha,\beta):=(a+b) \bmod 2$

φ je homomorfizem

Očitno.

φ je surjektiven

$\varphi(1,1)=0$
$\varphi(1,0)=1$

$\ker\varphi=\{(\alpha,\beta)\ ;\ \alpha+\beta\equiv 0 \bmod 2\}=C$

$B \subseteq C$

$\alpha(1,1)+\beta(1,3) \in B \quad , \quad \alpha,\beta \in \mathbb{Z}$

$\alpha(1,1)+\beta(1,3) = (\alpha+\beta, \alpha+3\beta)$

$\alpha+\beta+\alpha+3\beta$ je sodo

$(\alpha+\beta, \alpha+3\beta) \in C$

$C \subseteq B$

$(a,b) \in C$

$a = \alpha+\beta$
$b = \alpha+3\beta$

$a-b = -2\beta$

$\beta = \frac{\overbrace{b-a}^{\text{sodo}}}{2} \in \mathbb{Z}$

$\alpha = a - \frac{b-a}{2} \in \mathbb{Z}$

$\Rightarrow \ker\varphi = C = B$