Type af en permutation. Cykel-index. p-grupper.

En permutation $\sigma \in S_n$ kan skrives som produkt af disjunkte cykler (cykler af længde 1 medtages):

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_r$$

hvor σ_ℓ er en cykel af længde i_ℓ. Da disjunkte cykler kommuterer kan vi antage at $i_1 \leq i_2 \leq \ldots \leq i_r$.

Vi siger da at σ har type $i_1 \leq i_2 \leq \ldots \leq i_r$.

Desuden defineres cykel-indexet af σ som

$$\zeta_\sigma(x_1, x_2, \ldots, x_n) = x_{i_1} x_{i_2} \cdots x_{i_r}.$$

For en undergruppe G af S_n defineres cykel-indexet

$$\zeta_G(x_1, x_2, \ldots, x_n) = \frac{1}{|G|} \sum_{g \in G} \zeta_g(x_1, x_2, \ldots, x_n).$$

Sætning.
To permutationer σ_1 og σ_2 er konjugerede i S_n
(altså: der findes $\tau \in S_n$ som opfylder $\sigma_1 = \tau\sigma_2\tau^{-1}$)
hvis og kun hvis
σ_1 og σ_2 har samme type.

Lad p være et primtal.
En gruppe af orden p^r siges at være en p-gruppe.

Proposition.
Lad G være en gruppe af order $p^r > 1$, der virker på en endelig mængde S.
Så er $|S| \equiv |S^G| \pmod{p}$.

Corollar.
Lad G være en gruppe af order $p^r > 1$.
Så har centeret $Z(G)$ af G orden > 1.

Corollar.
Lad G være en gruppe af order p^2.
Så er G abelsk.
Og enten er $G \cong \mathbb{Z}/p^2\mathbb{Z}$ eller $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Lad p være et primtal.
Lad G være en gruppe af orden $|G| = p^r m$, hvor $p \nmid m$.
En undergruppe H af G, der har orden $|H| = P^r$, siges at være en Sylow p-undergruppe.
Mængden af Sylow p-undergrupper af G betegnes $\mathsf{Syl}_p(G)$.

Sylows sætninger.

1. $\mathsf{Syl}_p(G) \neq \emptyset$

2. Hvis $P, Q \in \mathsf{Syl}_p(G)$ så findes $g \in G$ som opfylder at
$$gPg^{-1} = Q.$$

3. $|\mathsf{Syl}_p(G)|$ går op i m og $|\mathsf{Syl}_p(G)| \equiv 1 \pmod p$.