

# Cykliske grupper og (direkte) produkt af grupper.

**Proposition.** Lad  $G$  være en cyklisk gruppe.

- Så er enhver undergruppe af  $G$  cyklisk.

Antag at  $G$  er endelig og lad  $d$  være et tal, der går op i  $|G|$ .

- Så har  $G$  en entydig undergruppe  $H$  af orden  $d$ .
- $G$  har  $\varphi(d)$  elementer af orden  $d$ .  $H$  består af alle elementer hvis orden går op i  $d$ .

Kan bevises:  $[a]_n \in \mathbb{Z}/n\mathbb{Z}$  har orden

$$\text{ord}([a]_n) = \frac{n}{\gcd(a, n)}.$$

Formuleret mere generelt: Hvis  $G = \langle g \rangle$  er en cyklisk gruppe af orden  $n$  så er

$$\text{ord}(g^i) = \frac{n}{\gcd(i, n)}.$$

**Korollar.** For ethvert positivt helt tal er

$$n = \sum_{d|n} \varphi(d).$$

**Eksempel.** Lad  $p$  og  $q$  være primtal. Så er

- $1 = \sum_{d|1} \varphi(d) = \varphi(1),$
- $p = \varphi(1) + \varphi(p),$  altså  $\varphi(p) = p - 1,$  og
- $pq = \varphi(1) + \varphi(p) + \varphi(q) + \varphi(pq),$  altså  $\varphi(pq) = pq - 1 - (p - 1) - (q - 1) = (p - 1)(q - 1).$

Lad  $G_1, \dots, G_n$  være grupper.

Lad  $G = G_1 \times \dots \times G_n = \{(g_1, \dots, g_n) \mid g_1 \in G_1, \dots, g_n \in G_n\}$ .

Så er  $G$  en gruppe med komposition

$$(g_1, \dots, g_n)(h_1, \dots, h_n) = (g_1h_1, \dots, g_nh_n).$$

$G$  kaldes **produkt gruppen** eller det **direkte produkt** af  $G_1, \dots, G_n$ .

**Lemma.** Lad  $G$  være en gruppe og  $M$  og  $N$  være normale undergrupper af  $G$  med  $M \cap N = \{e\}$ .

Så er  $MN = \{mn \mid m \in M, n \in N\}$  en undergruppe af  $G$  og  $MN$  er isomorf med det direkte produkt  $M \times N$ .

**Proposition 2.8.2.** (med  $r = 2$ )

Lad  $n_1$  og  $n_2$  være positive hele tal med  $\gcd(n_1, n_2) = 1$  og lad  $N = n_1 n_2$ .

Så er  $\tilde{\phi} : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$

som er givet ved  $\tilde{\phi}([x]_N) = ([x]_{n_1}, [x]_{n_2})$

en isomorfi.

Eksistensen af  $\tilde{\phi}^{-1}$  (og metoden til beregning af denne) kaldes den kinesiske restsætning.