Mer om abstrakte grupper

Def: La G være en gruppe.
En ikke-tom delmengde $H \subset G$ kalles en undergruppe av G dersom

* $ab \in H$ for alle $a, b \in H$.
* $a^{-1} \in H$ for alle $a \in H$.

Merk: I så fall er H selv en gruppe med den samme binæroperasjon som i G.

Exs: * $\mathbb{Z}$ es un subgrupo de $\mathbb{R}$

* $O(n)$ es un subgrupo de $GL(n, \mathbb{R})$.

* Subgrupos de $S_3 = \{Id, \rho, \rho^2, \mu, \rho\mu, \rho^2\mu\}$:

$\{Id\}$, $\{Id, \rho, \rho^2\}$, $\{Id, \mu\}$, $\{Id, \rho^2\mu\}$, todo S_3.

Def. For et naturlig tall n definerer vi

$$C_n = \{ z \in \mathbb{C} \mid z^n = 1 \}$$

$$= \{ e^{2\pi i k/n} \mid k = 0, \cdots, n-1 \}$$

$$= \{ 1, q, q^2, \cdots, q^{n-1} \},$$

hvor $q = e^{2\pi i/n}$.

Prop: C_n er en undergruppe av $\mathbb{C}^* = \{ z \in \mathbb{C} \mid z \neq 0 \}$

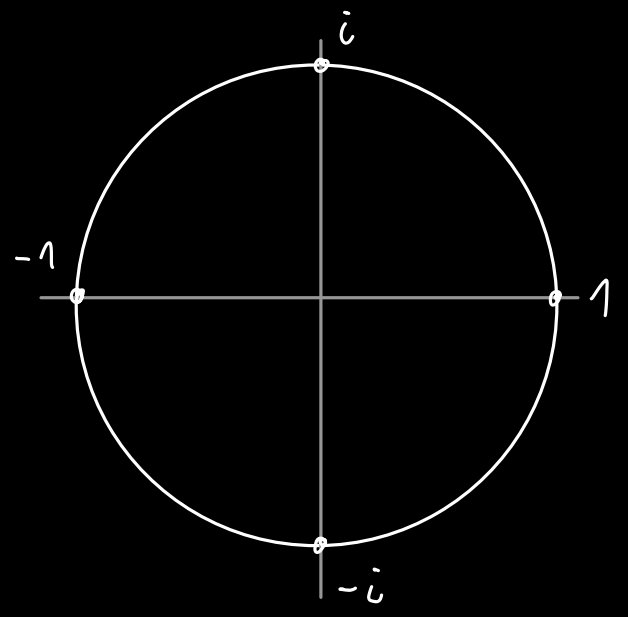
Bevis: La $w, z \in C_n$.

$(wz)^n = w^n z^n = 1 \cdot 1 = 1 \Rightarrow wz \in C_n$

$(w^{-1})^n = (w^n)^{-1} = 1^{-1} = 1 \Rightarrow w^{-1} \in C_n$. //

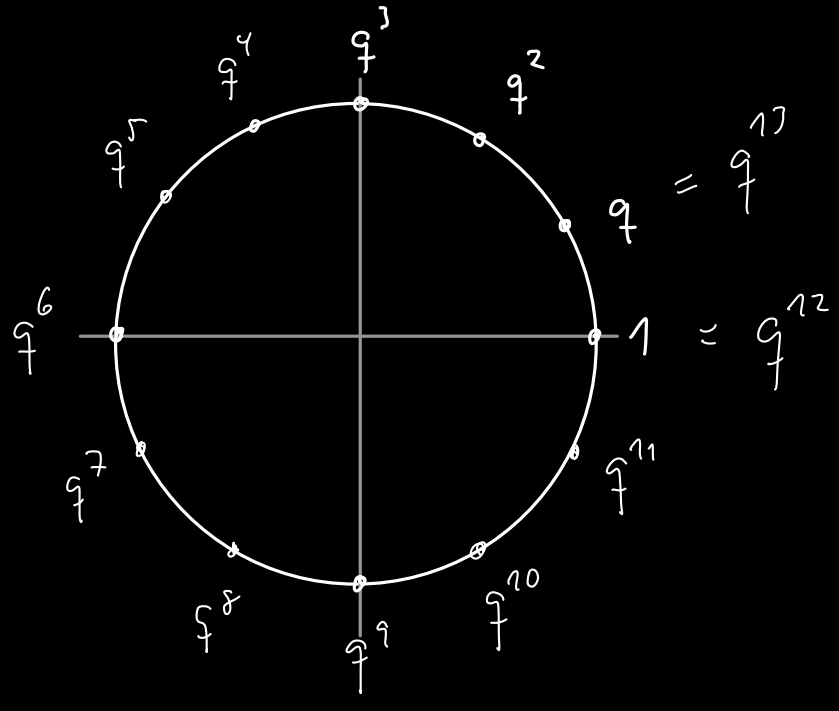
Eks: $n = 4$. $q = e^{2\pi i/4} = e^{\pi i/2} = i$

$i^2 = -1$, $i^3 = i^2 \cdot i = -i$, $i^4 = 1$, $i^5 = i$



$$C_4 = \{1, i, -1, -i\}$$

Eks: $n = 12$. $q = e^{2\pi i/12} = e^{\pi i/6} = \frac{\sqrt{3}}{2} + \frac{i}{2}$



Def: La n være et helt tall, $n > 1$.

To hele tall a, b sies å være kongruent

modulo n, og vi skriver $a \equiv b \pmod{n}$, dersom det finnes et helt tall k slik at

$$a - b = kn,$$

dvs. dersom $a-b$ er delelig med n.

Eks: $11 \equiv 3 \pmod{4}$ fordi

$$11 - 3 = 8 = 2 \cdot 4.$$

Def: Kongruensklassen til a modulo n er definert ved

$$[a] = [a]_n = \{a + kn \mid k \in \mathbb{Z}\}$$

= mengden av alle hele tall som er kongruent med a modulo n.

Observasjon Ethvert helt tall a er kongruent

med nsyaktig ett helt tall b sådan at

$$0 \leq b < n.$$

Altså har vi en disjunkt union

$$\mathbb{Z} = [0]_n \cup [1]_n \cup [2]_n \cup \cdots \cup [n-1]_n.$$

Eks: $n = 2$.

$[0]_2$ = mengden av partall

$[1]_2$ = mengden av oddetall.

Def: $[a]_n + [b]_n = [a+b]_n$.

Merk: Dette er veldefinert fordi

$$(a+kn) + (b+ln) = a+b+(k+l)n$$

$$\equiv a+b \pmod{n}.$$

Def: $\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \dots, [n-1]_n\}$.

: abelsk grupp under addition.

Eks: $n = 12$. I $\mathbb{Z}_{12}$ er

$[8] + [11] = [19] = [19-12] = [7]$.

$[5] + [7] = [12] = [0]$

$\Rightarrow [7] = -[5]$.

Merk: $\underbrace{[1]_n + \dots + [1]_n}_{k \text{ ganger}} = [k]_n$.

Def: En avbildning $\phi: G \to H$ mellom to grupper kalles en homomorfi, dersom

$\phi(gg') = \phi(g) \cdot \phi(g')$ for alle $g, g' \in G$.

Prop: Hvis $\phi : G \to H$ er en homomorfi, så gjelder:

(i) $\phi(e_G) = e_H$, hvor e_G, e_H er enhetselementene i G, H hhv.

(ii) $\phi(g^{-1}) = \phi(g)^{-1}$ for alle $g \in G$.

Bevis: (i) $e_G \cdot e_G = e_G$

$\Rightarrow \phi(e_G) = \phi(e_G) \cdot \phi(e_G)$

$\Rightarrow e_H = \phi(e_G)$.

(ii) $e_G = g g^{-1} \Rightarrow e_H = \phi(e_G) = \phi(g) \cdot \phi(g^{-1})$

$\Rightarrow \phi(g^{-1}) = \phi(g)^{-1}$. //

Def: En homomorfi $\phi : G \to H$ kalles en isomorfi, dersom ϕ er bijektiv, dvs. dersom

det for hver $h \in H$ finn nøyaktig én $g \in G$ slik at $\phi(g) = h$.

Eks: $\mathbb{R}_+ := \{x \in \mathbb{R} \mid x > 0\}$

: gruppe under multiplikasjon

$\exp : \mathbb{R} \to \mathbb{R}_+$, $\exp(x) = e^x > 0$.

$e^{x+y} = e^x \cdot e^y \Rightarrow$ exp er en homomorfi

exp er bijektiv (med $\exp^{-1} = \log$),

altså er exp en isomorfi.

Eks: $\phi : \mathbb{R} \to \mathbb{C}^*$, $\phi(x) = e^{ix} = \cos x + i \sin x$.

$e^{i(x+y)} = e^{ix} \cdot e^{iy}$

$\Rightarrow$ ϕ er en homomorfi.

Eks: For gitt $n > 1$ la $q = e^{2\pi i/n}$.

Da er

$$\phi : \mathbb{Z}_n \to C_n, \quad [k] \mapsto q^k$$

en isomorfi.

Merk: ϕ er vel-definert, fordi

$$q^{k+ln} = q^k \cdot q^{ln}, \quad q^{ln} = (q^n)^l = 1^l = 1.$$
$$= q^k.$$

Def: La G vær en gruppe og $g \in G$.

Undergruppen av G <u>generert</u> av g

er definert ved

$$\langle g \rangle = \{ g^k \mid k \in \mathbb{Z} \}$$
$$= \{ \dots, g^{-2}, g^{-1}, e, g, g^2, \dots \}.$$

Def: En gruppe G kalles <u>syklisk</u> hvis det finnes en $g \in G$ slik at $\langle g \rangle = G$.

<u>Eks</u>: * C_n, $\mathbb{Z}_n$, $\mathbb{Z}$ er sykliske.

* $\mathbb{R}$ er ikke syklisk.

<u>Prop</u> Enhver syklisk gruppe er abelsk.

<u>Bevis</u> $g^k \cdot g^l = g^{k+l} = g^{l+k} = g^l \cdot g^k$. //

<u>Eks</u>: S_3, D_4, $GL_n(\mathbb{R})$ $(n \geq 2)$

er ikke abelske.