Mer om abstrakte grupper (fra 7.2)

Def. For et naturlig tall n definerer vi

$$C_n = \{ z \in \mathbb{C} \mid z^n = 1 \}$$
$$= \{ e^{2\pi i k/n} \mid k = 0, \dots, n-1 \}$$
$$= \{ 1, q, q^2, \dots, q^{n-1} \},$$

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 $w, z \in C_n$.

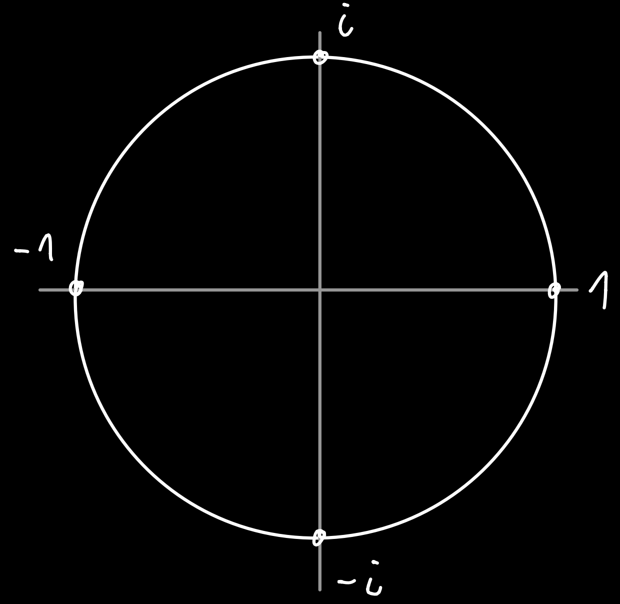
$$(wz)^n = w^n z^n = 1 \cdot 1 = 1 \quad \Rightarrow \quad wz \in C_n$$

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

//

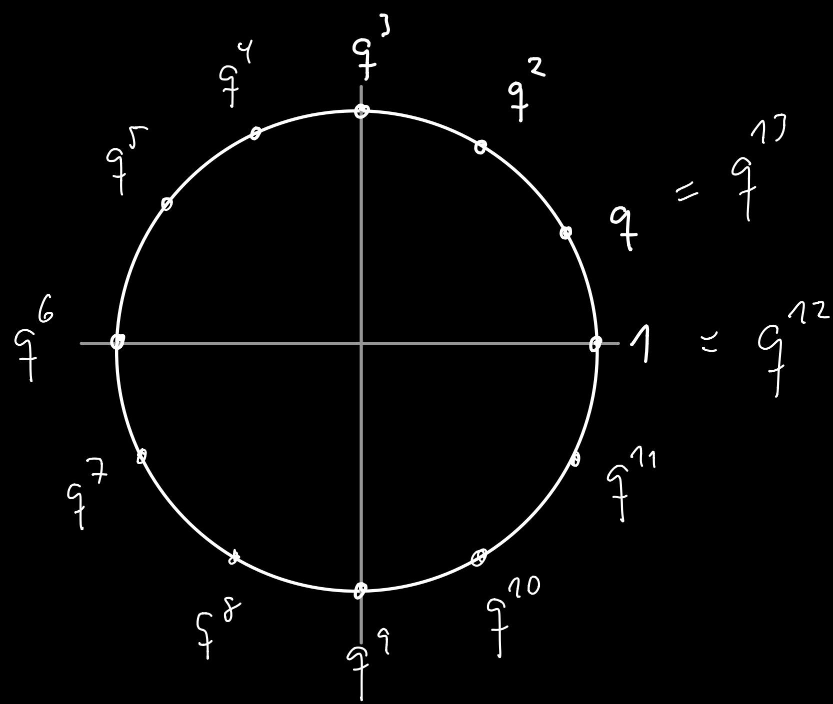
Eks: $n = 4$. $q = e^{2\pi i/4} = e^{\pi i/2} = i$

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



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

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



<u>Def</u>: La n være et helt tall, $n > 1$.

To hele tall a, b sies å være <u>kongruent</u>

<u>modulo n</u>, og vi skriver $a \equiv b \pmod{n}$,

dersom det fins et helt tall k slik at

$$a - b = kn,$$

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

<u>Eks</u>: $11 \equiv 3 \pmod{4}$ fordi

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

Def: <u>Kongruensklassen</u> 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.

<u>Observasjon</u> Ethvert helt tall a er kongruent

med nøyaktig ett helt tall b slik at

$$0 \le b < n.$$

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 odde tall.

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

: abelsk gruppe under addition.

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

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

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

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

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

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

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

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

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

Def: En homomorfi $\phi : G \to H$ kalles en isomorfi, dersom ϕ er bijektiv, dvs. dersom dvs. for hver $h \in H$ finns nøyaktig én

$g \in G$ slik at $\phi(g) = h$.

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

: 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.

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

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

$\Rightarrow \phi$ 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 være 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 syklisk hvis det fins en $g \in G$ slik at $\langle g \rangle = G$.

Eks: C_n, $\mathbb{Z}_n$, $\mathbb{Z}$ er sykliske.

Def: Dersom en gruppe G har kun endelig mange elementer, definerer vi ordenen til G ved

$$|G| = \text{antall elementer i } G.$$

Eks: $|\mathbb{Z}_n| = n$, $|S_3| = 6$, $|D_4| = 8$.

Def: La G være en gruppe og $g \in G$. Ordenen til g er den minste $n \geq 1$ slik at $g^n = e$, hvis en slik n fins.

Ellers sies g å ha <u>uendelig</u> orden.

<u>Eks</u>: $[2] \in \mathbb{Z}_6$ har orden 3, fordi

$2 \cdot [2] = [4] \neq [0]$, ← enhetselementet i $\mathbb{Z}_6$.

$3 \cdot [2] = [6] = [0]$.

<u>Prop</u>: Hvis $g \in G$ har orden n, så har $\langle g \rangle$ nøyaktig n elementer, nemlig

$$\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}.$$

<u>Bevis</u>: (i) La $k \in \mathbb{Z}$. Da fins det hele tall a, b slik at

$$k = a + bn, \qquad 0 \leq a < n.$$

$\Rightarrow \quad g^k = g^a \cdot (g^n)^b = g^a$ fordi $g^n = 1$.

Dette viser at

$$\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}.$$

(ii) La $0 \leq i \leq j < n$ og anta $g^i = g^j$.

Da er $g^{j-i} = e$. Siden $0 \leq j-i < n$,

må $i = j$. Altså er $1, g, g^2, \dots, g^{n-1}$

parvis forskjellige. //

<u>Prop</u>: I en endelig gruppe G har hvert

element endelig orden.

<u>Bevis</u>: La $g \in G$. Elementene

$$e, g, g^2, g^3, g^4, \dots$$

kan ikke alle være forskjellige, så det må finnes hele tall i, j slik at

$$0 \leq i < j \quad \text{og} \quad g^i = g^j.$$

Da er $g^{j-i} = e$, så g har endelig orden. //

Def: La $H < G$ være en undergruppe. Den (venstre) restklassen til et element $g \in G$ er definert ved

$$gH = \{ gh \mid h \in H \}.$$

Eks: $G = \mathbb{Z}$, $H = \mathbb{Z}n = \{ kn \mid k \in \mathbb{Z} \}$,
$n \geq 1$

$[k]_n = k + \mathbb{Z}n = k + H$: restklasse.