Groepen theorie

Luc Veldhuis

5 April 2017

Cyklische groepen en ondergroepen

Definition

$x \in G$, G een groep
$\langle x \rangle = \{x^m | m \in \mathbb{Z}\}$ is de ondergroep voortgebracht uit x.
(De kleinste ondergroep van G die x bevat.)

Ondergroep van G

- $\langle x \rangle \neq \emptyset$, $e = x^0 \in \langle x \rangle$
- $x^{m_1}, x^{m_2} \in \langle x \rangle$, $m_i \in \mathbb{Z} \Rightarrow x^{m_1} x^{m_2} = x^{m_1+m_2} \in \langle x \rangle$
- $x^m \in \mathbb{Z} \Rightarrow (x^m)^{-1} = x^{-m} \in \langle x \rangle$

Opmerking

$\langle x^{-1} \rangle = \langle x \rangle$
$\langle x \rangle$ abels, want: $x^{m_1} \cdot x^{m_2} = x^{m_1+m_2} = x^{m_2+m_1} = x^{m_2} \cdot x^{m_1}$
Een ondergroep van de vorm $\langle x \rangle$ heet cyklisch.

Cyklische groepen en ondergroepen

Voorbeeld

- D_{2n}, $n \geq 3 \rightarrow < r >= \{e, r, r^2, \ldots, r^{n-1}\}$, want $r^n = e$
- $S_4 \rightarrow \langle (1\ 2\ 3\ 4) \rangle = \{e, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\}$, want $(1\ 2\ 3\ 4)^4 = e$
- $\mathbb{Z} \rightarrow \langle 3 \rangle = \{3m | m \in \mathbb{Z}\} = 3\mathbb{Z} = \langle -3 \rangle$ ($\mathbb{Z}$ is een optelgroep)
- $\mathbb{F}_5^* = \{\overline{1} = \overline{2^0}, \overline{2} = \overline{2^1}, \overline{3} = \overline{2^3}, \overline{4} = \overline{2^2}\} = \langle 2 \rangle$

Stelling

Als $H = \langle x \rangle$, dan $|x| = |H| = |x|$ (Kan allebei oneindig zijn.)
Ook geldt :

- Als $|x| = n < \infty$, dan is $\langle x \rangle = \{e, x, x^2, \ldots, x^n\}$ allemaal verschillend.
- Als $|x| = \infty$, dan is $\langle x \rangle = \{\ldots, x^{-2}, x^{-1}, e, x^1, x^2, \ldots\}$ allemaal verschillend.

Cyklische groepen en ondergroepen

Bewijs

$e, x, \ldots, x^{n-1}$ zijn verschillend. Stel dat $x^i = x^j$, met $0 \leq i < j \leq n-1$

Dan is $e = x^{-i}x^i = x^{-i}x^j = x^{j-i}$ met $1 \leq j-i \leq n-1$. x heeft orde n, dus tegenspraak. $e, x, \ldots, x^{n-1}$ zijn allemaal verschillend.

Neem nu $m \in \mathbb{Z}$ en $m = qn + r$ met $0 \leq r \leq n-1$, $q \in \mathbb{Z}$ (delen met rest).

Dan: $x^m = x^{qn+r} = (x^n)^q \cdot x^r = e^q x^r = x^r$

Dus $\langle x \rangle = \{x^m | m \in \mathbb{Z}\} \subseteq \{e, x, \ldots, x^{n-1}\} \subseteq \langle x \rangle$

Dus $\langle x \rangle = \{e, x, \ldots, x^{n-1}\}$

Cyklische groepen en ondergroepen

Opmerking

Als $|x| = n < \infty$, dan is $x^{m_1} = x^{m_2}$ voor $m_1, m_2 \in \mathbb{Z} \leftrightarrow m_1 \& m_2$ hebben dezelfde rest, $r \in \{0, 1, \ldots, n-1\}$ bij deling door $n \leftrightarrow n | m_1 - m_2$

Dus $x^{m_1} = x^{m_2} \leftrightarrow n | m_1 - m_2$

$x^m = e \leftrightarrow n | m$

Cyklische groepen en ondergroepen

Stelling

Elk tweetal cyklische groepen met hetzelfde aantal elementen is isomorf

- Als $|x| = |y| = n < \infty$, dan is $\phi : \langle x \rangle \to \langle y \rangle$ een isomorfisme. $x^0 \mapsto y^i$
- Als $|x| = \infty$, dan is $\phi : \mathbb{Z} \to \langle x \rangle$ een isomorfisme: $k \mapsto x^k$

Opmerking

Dus een cyklische groep met $n < \infty$ elementen is isomorf met $\mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \rangle$, ook als $n = 1$

Cyklische groepen en ondergroepen

Bewijs

- ϕ is welgedefinieerd: $x^i = x^j \leftrightarrow n|(i-j) \leftrightarrow y^i = y^j$, want $|x| = |y| = n < \infty$
  Dus elke keuze van exponent van x (mod n) geeft hetzelfde resultaat.
  - ϕ is een homomorfisme: $\phi(x^i \cdot x^j) = \phi(x^{i+j}) = y^{i+j}$
    $\phi(x^i) \cdot \phi(x^j) = y^i y^j = y^{i+j}$
    $\phi(x^i \cdot x^j) = \phi(x^i)\phi(x^j)$ is een homomorfisme.
  - ϕ is surjectief: $\{e, x, \ldots, x^{n-1}\}$ beeldt af op $\{e, y, \ldots, y^{n-1}\} = \langle y \rangle$
  - ϕ is injectief, want $|\langle x \rangle| = |\langle y \rangle| = n < \infty$
- Oefening (je kunt er niet tellen)

Cyklische groepen en ondergroepen

Voorbeeld

Als $|x| = n < \infty$, dan is $\phi : \mathbb{Z}/n\mathbb{Z} \to \langle y \rangle$ met $\overline{i \cdot t} \mapsto y^i$ een isomorfisme

Stelling

Stel $a \in \mathbb{Z}$, $|x| = n < \infty$, dan geldt $|x^a| = \frac{n}{ggd(a,n)}$

Bewijs

Idee: Bepaal alle $m \in \mathbb{Z}$ met $(x^a)^m = e$. De kleinste positive m is dan $|x^a|$.

Cyklische groepen en ondergroepen

Bewijs (vervolg)

$m \in Z : e = (x^a)^m = x^{am} \leftrightarrow n|am$
Schrijf $d = ggd(a, n) \geq 1$, $a = a'd$, $n = n'd$ met $n' \geq 1$
Dan $n'd|a'dm \leftrightarrow n'|a'm$ en $ggd(a', n') = 1$ dus met lemma van Euclides $n'|m$
Dus $(x^a)^m = e \leftrightarrow n'|m$. De kleinste $m \geq 1$ die voldoet is de orde van x^a, $|x^a| = n' = \frac{n}{ggd(a,n)}$

Lemma van Euclides

Als $a, b, c \in \mathbb{Z}$, $a|bc$ en $ggd(a, b) = 1$ dan $a|c$.

Bewijs

Volgens Bézout: $\exists x, y \in \mathbb{Z}$ met $ggd(a, b) = 1 = xa + yb$
Dan $c = xac + ybc$, met $a|xa$ en $a|bc$, dus $a|c$

Cyklische groepen en ondergroepen

Voorbeeld

In $\mathbb{Z}/12\mathbb{Z}$ heeft $\overline{8} \cdot \overline{1}$ orde $\frac{12}{ggd(8,12)} = 3$

Stelling

Zij $H = \langle x \rangle$

- Als $\langle x \rangle = \infty$ dan is $\langle x^a \rangle = \langle x \rangle \leftrightarrow a = \pm 1$
- Als $\langle x \rangle = n < \infty$ dan is $\langle x^a \rangle = \langle x \rangle \leftrightarrow ggd(a, n) = 1$. $\langle x \rangle$ heeft $\phi(n)$ als voortbrenger.

Bewijs

- Oefening ($\langle x \rangle \cong \mathbb{Z}$)
- $\langle x^a \rangle \subseteq \langle x \langle$, want $\#\text{elem}|x^a| = \frac{n}{ggd(n,a)}$, en $\#\text{elem}|x| = n$, dus $\langle x^a \langle = \langle x \langle \leftrightarrow ggd(a, n) = 1$

Cyklische groepen en ondergroepen

Voorbeeld

$\mathbb{Z}/12\mathbb{Z} = \langle T \rangle$ heeft voortbrengers $a \cdot t = \bar{a}$ met $\bar{a} \in (\mathbb{Z}/12\mathbb{Z})^*$, dus $\phi(12) = \phi(2^2 \cdot 3) = \phi(2^2)\phi(3) = 2^{2-1}(2-1)3^{1-1}(3-1) = 4$

Stelling

Elke ondergroep van een cyklische groep is cyklish.
Preciezer: als $H = \langle x \rangle$:

- Als $|x| = \infty (\leftrightarrow |H| = \infty)$, dan zijn de ondergroepen van H 1 op 1 met $a = 0, 1, 2, \ldots$. $a = 0$ geeft $\langle x^a \rangle = \langle e \rangle = \{e\}$
- Als $|x| = n < \infty$, dan zijn de ondergroepen 1 op 1 met de positieve delers van n. $d|n \overset{\text{1-op-1}}{\longleftrightarrow} < x^d >$ ($\frac{n}{d}$ elementen)

Voor het bewijs, zie boek theorem 7 pagina 58.

Cyklische groepen en ondergroepen

Voorbeeld

- $\mathbb{Z}/12\mathbb{Z} = \langle t \rangle$, positieve delers van $12 = 2^2 \cdot 3^1$:
  $\#(2+1)(1+1) = 6$, namelijk $(1, 2, 3, 4, 6, 12)$
  $H = \langle d \cdot t \rangle$

d	1	2	3	4	5	6
	$\langle 1 \cdot t \rangle$	$\langle 2 \cdot t \rangle$	$\langle 3 \cdot t \rangle$	$\langle 4 \cdot t \rangle$	$\langle 5 \cdot t \rangle$	$\langle 6 \cdot t \rangle$
#	$\mathbb{Z}/12\mathbb{Z} = 12$	6	4	3	2	1

- $\mathbb{F} = \langle \overline{2} \rangle$ heeft ook 6 ondergroepen. Vind deze en de voortbrengers.