Groepen theorie

Luc Veldhuis

21 Februari 2016

Groepen theorie

Herhaling

(G,*) groep $\Leftrightarrow$ G verzameling, $* : G \times G \to G$ bewerking die voldoet aan de voorwaarden:

- Associatief: $a * (b * c) = (a * b) * c$
- $\exists$ Neutraal element $e \in G$ $a * e = e * a = a$
- $\exists$ inverse elementen $\forall a \in G$ $\exists a^{-1} \in G$: $a * a^{-1} = a^{-1} * a = e$

Gevolg

- Het neutrale element is uniek. Als e' een ander neutraal element is, dan $e = e * e' = e' * e = e'$.
- Het inverse element is uniek, namelijk als b een ander inverse element van a is, dan geldt $b = b * e = b * (a * a^{-1}) = (b * a) * a^{-1} = e * a^{-1} = a^{-1}$.
- $(a^{-1})^{-1} = a$ want $a^{-1} * (a^{-1})^{-1} = e = (a^{-1})^{-1} * a^{-1}$ maar inverse element is uniek.
- $(a * b)^{-1} = b^{-1} * a^{-1}$. Want $(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b = b^{-1} * b = e = \cdots = (a * b) * (b^{-1} * a^{-1})$
- $a_1, \ldots, a_n \in G \Rightarrow a_1 * \cdots * a_n$ is gedefinieerd zonder haakjes.

Conventie

- In een groep $(G, *)$ laten we ook vaak de bewerking vervallen. $(G, *) = G$ en we schijven ab in plaats van $a * b$.
- Als $*$ een commutatieve bewerking is, dan schijven we e als 0, $a * b$ als $a + b$ en a^{-1} als$-a$ en $a - b$ als $a + (-b)$.

Stelling

Op een groep G geldt:

$au = av \Leftrightarrow u = v$

$ub = vb \Leftrightarrow u = v$

Bewijs

$\Leftarrow$ duidelijk

$\Rightarrow$

$au = av$

$a^{-1}(au) = a^{-1}(av)$

$(a^{-1}a)u = (a^{-1}a)v$

$eu = ev$

$u = v$

$ub = vb$ op een soortgelijke manier

Definitie

- In een groep G laat $x \in G$ en $n \in \mathbb{N}$
  $x^n = e$ als $n = 0$
  $x^n = x * \cdots * x$ als $n > 0$
  $x^n = x^{-1} * \cdots * x^{-1}$ als $n < 0$
- Als G commutatief is, dan
  $nx = 0$ als $n = 0$
  $nx = x + \cdots + x$ als $n > 0$
  $nx = (-x) + \cdots + (-x)$ als $n < 0$
  Daarmee geldt $x^n x^m = x^{n+m}$
  $x^n y^n = (xy)^n$
  $nx + mx = (n + m)x$
  $nx + ny = n(x + y)$

Definitie

Zij G een groep, $x \in G$
x heeft orde $n \geq 1$ als $x^n = e$ en $x^m \neq e$, $0 < m < n$ De orde van x wordt ook genoteerd als $|x| \in \mathbb{N}$

Opmerking

- x heeft orde $1 \Rightarrow x = e$
- Als $|x| = n$ dan is $\{x^m : m \in \mathbb{Z}\} = \{e, x, x^2, \ldots, x^{n-1}\}$. De verzameling heeft de eindige grootte n.
- Als $x^n \neq e$ voor alle $n \in \mathbb{N}$ dan $|x| = \infty$

Voorbeeld

- $\mathbb{R}$ is een groep onder optelling. Elk element $x \neq 0$ heeft een oneindige orde, $|x| = \infty$
- $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ is een groep onder vermenigvuldiging. Elk element $x \neq 1$ heeft orde ∞.
- $\mathbb{Z}/m\mathbb{Z}$ is een groep onder optelling. Elk element x heeft orde $|x| \leq m$
  $|x| = m$ alleen als m priem.
  Waarbij $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$
- $(\mathbb{Z}/m\mathbb{Z})^* = \{\overline{a} \in \mathbb{Z}/m\mathbb{Z} : \exists \overline{b} : \overline{b}\overline{a} = \overline{a}\overline{b} = \overline{1}\} = \{\overline{a} \in \mathbb{Z}/m\mathbb{Z} : ggd(a, m) = 1\}$

Voorbeeld

$\mathbb{Z}/12\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}\}$ Ordes:
$1, 12, 6, 4, 3, 12, 2, 12, 3, 4, 6, 12$

Opmerking

$|x| = 12 = m$ zijn priem

Voorbeeld

$(\mathbb{Z}/15\mathbb{Z})^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}$
$\phi(15) = \phi(3)\phi(5) = (3-1)(5-1) = 8$
$|\overline{7}| = 4 \rightarrow \overline{7777} = \overline{49} = \overline{47} = \overline{137} = \overline{91} = \overline{1}$