Groepen theorie

Luc Veldhuis

7 Februari 2016

Groepen theorie

Definition

Voor a, b in $\mathbb{Z}$ is $d \in \mathbb{Z}$ een grootste gemene deler van a en b als

1. $d|a$ en $a|b$
2. Voor elke e in $\mathbb{Z}$ met $e|a$ en $e|b$ geldt $e|d$
3. $d \geq 0$

$d|a$ betekend 'd deelt a' dus $a = ed$ voor een $e \in \mathbb{Z}$

Opmerking

Als d aan (i) en (ii) voldoet, dan voldoet ook $-d$. $d|a$ betekend $a = fd = (-f)(-d)$ voor een $f \in \mathbb{Z}$ dus $-d|a$. Maar hij is op teken na uniek en dan maakt (iii) een unieke keuze!

Groepen theorie

Bewijs

Namelijk, stel d en d' voldoen allebei aan (i) en (ii), dan geldt $d|a$, $d|b$, $d'|a$, $d'|b$ en dus (met (ii) $e = d'$) volgt $d'|d$. Net zo geldt $d|d'$. Dus er bestaan $x, y \in \mathbb{Z}$ met $d = xd'$ en $d' = yd \rightarrow d = xyd$ en $d(1 - xy) = 0$. Er volgt dat $xy = 1$ of $d = 0$.
Als $d = 0$ dan $d' = yd = 0$.
Als $xy = 1$ dan $x = y = 1$ of $x = y = -1$ want $x, y \in \mathbb{Z}$. Dus $d = d'$ of $d = -d'$

Notatie

Als a, b een ggd hebben, dan schrijf je die als $ggd(a, b)$.

Let op!

Tot nu toe nog geen existentie aangetoond.

Groepen theorie

Merk op

- $ggd(a,0) = d|a$ en $d|0 \leftrightarrow d0 = zd$ voor een $z \in \mathbb{Z}$. Dus (i) in de definitie van ggd is equivalent met $a|d$. Idem (ii) is equivalent met $e|q \to e|d$. $d = |a|$ voldoet aan (i), (ii) en (iii). Dit geldt ook als $a = 0$, dat wil zeggen $ggd(0,0) = 0$.
- Als $a, b \in \mathbb{Z}$ dan is $ggd(a,b) = ggd(a, b+ka)$ voor alle $k \in \mathbb{Z}$ dat wil zeggen ze bestaan allebei en dan zijn ze gelijk of ze betaan geen van beiden. Namelijk, $\{f \in \mathbb{Z}$ met $f|a$ en $f|b\} = \{g \in Z$ met $g|a$ en $g|b+ka\}$. Als $f|a$ en $f|b$ dan ook $f|a$ en $f|b+ka$. Dus LHS $\subseteq$ RHS (Als $a = xf, b = yf$ dan $b + ka = (y+kx)f$)

Definitie

Net zo: RHS $\subseteq$ LHS Uit LHS $=$ RHS volgt de bewering: de definitie van $ggd(a, b)$ hangt alleen af van de verzameling van gemeenschappelijke delers van a en b.

Groepen theorie

Deling met rest

Als $a, b \in \mathbb{Z}$ met $b \neq 0$ dan bestaan er $q, z \in \mathbb{Z}$ met $a = qb + z$ en $0 \leq z < |b|$. De a en r zijn uniek.

Voorbeeld

17 = 2*6 + 5
- 17 = (-3)*6+1

Uitleg

$a = q'b + r'$ met $|r'| \leq \frac{|b|}{r}$
q' en r' zijn misschien niet uniek.

Groepen theorie

Voorbeeld

17 = 3*6+(-1)
Idee: $ggd(17,6) = ggd(17-2*6,6) = ggd(5,6) =$
$ggd(5,6-1) = ggd(5,1) = ggd(5-5,1) = ggd(0,1) = |1| = 1$

Stelling

Voor elke $a, b \in \mathbb{Z}$ bestaat $ggd(a, b)$ en er bestaan $x, y \in \mathbb{Z}$ met $ggd(a, b) = za + yb$.

Bewijs

Als $a = b = 0$ dan $ggd(0,0) = 0 = x0 + y0$ voor alle $x, y \in \mathbb{Z}$
Omdat $ggd(a, b) = ggd(b, a)$ mogen we nu aannemen dat $b \neq 0$.
Dan kun je $ggd(a, b)$ en x, y uitrekenen met behulp van het Euclidisch algoritme

Deling met rest

Neem:

$r_{-2} = a,\ r_{-1} = b$

$r_n = r_{n+2} r_{n+1} + r_{n+2}$ voor $n \geq 2$ als $r_{n+1} \neq a$

Deling met rest dus $0 \leq r_{n+2} < |r_{n+1}|$ of $|r_{n+2}| = \frac{|r_{n+1}|}{2}$

$x_{-2} = 1,\ y_{-2} = 0,\ y_{-1} = 1,\ x_v = 0$

Voor $n \geq 2$ $x_{n+2} = x_n - q_{n+2} x_{n+1}$

$y_{n+2} = y_n - q_{n+2} y_{n+1}$

Dan geldt $|r_{-1}| > |r_0| > |r_1| > \cdots > |r_m| > |r_{m+1}| = 0$

$ggd(a, b) = ggd(r_2, r_1) = ggd(r_0, r_{-1}) = ggd(r_1, r_0) =$

$ggd(r_m, r_{m+1}) = |r_m|$

Dus de $ggd(a, b)$ = absolute waarde laatste waarde $\neq 0$

Er geldt $r_n = x_n a + y_n b$ voor $n \geq 2$. (Bewijs met inductie).

$ggd(a, b) = |r_m| = |(-x_m)a + (-y_m)b| of |x_m a + y_m b|$

Groepen theorie

$a = 72, \ b = 20$:

Tabel : Berekening van ggd

n	r_n	x_n	y_n	q_n	berekening
-2	72	1	0		
-1	20	0	1		
0	12	1	-3	3	72 = 3*20+12
1	8	-1	4	1	20 = 1*12+8
2	4	2	-7	1	12 = 1*8+4
3	0				8 = 2*4+0

$ggd(72, 20) = 4 = 2 * 72 - 7 * 20$
Opgave: determinant van vector
$|x_n y_n|$
$|x_{n+1} y_{n+1}|$

Variant met $|r_{n+2}| \leq \frac{|r_{n+1}|}{2}$:

Tabel : Alternative versie ggd

n	r_n	x_n	y_n	q_n	berekening
-2	72	1	0		
-1	20	0	1		
0	-8	1	-4	4	72 = 4*20 -8
1	4	2	-7	-2	20 = (-2)(-8) +4
2	0				-8 = (-2)4+0

Groepen theorie

Equivalentie klassen

Voor $n \geq 2$ $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1} \ldots, \bar{n}\}$
$\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$
$[a]_n = \bar{a} =$ klasse van a modulo n.
$a + \mathbb{Z} = \{a + kn$ met $k \in \mathbb{Z}\}$ deelverzameling van $\mathbb{Z}$
Voor $a, b \in \mathbb{Z}$ geldt $\bar{a} = \bar{b}$ of $\bar{a} \cap \bar{b} = \emptyset$
$\bar{a} = \bar{b} \leftrightarrow n|a - b$

Voorbeeld

$\mathbb{Z}/n\mathbb{Z}$ heeft optellingen en vermenigvuldiging. $\bar{a} + \bar{b} = \overline{(a + b)}$
$\bar{a} * \bar{b} = \overline{(a * b)}$
De bewerkingen zijn wel gedefinieerd dat wil zeggen, onafhankelijk van de gemaakte keuzes.
Uit $\bar{a}$ hebben we een a gekozen. De andere mogelijke keuzes zijn: $a' = a + kn$ met $k \in \mathbb{Z}$ uit $\bar{a}$. $b' = b + kn$ met $k \in \mathbb{Z}$ uit $\bar{b}$.