Groepentheorie

H1

St. 1.1 $a, b \in \mathbb{Z}$ $b > 0$ Dan $\exists! q, r \in \mathbb{Z} : 0 \leq r < b \wedge a = qb + r$

Def 1.3 $a, b \in \mathbb{Z}$ als $\exists q \in \mathbb{Z} : a = qb$, heet a deelbaar door b
notatie $b \mid a$

Prop.
$b \mid a \quad a \mid c \Rightarrow b \mid c$
$b \mid a \quad b \mid c \Rightarrow b \mid a+c \;,\; b \mid a-c$
$b \mid 0 \quad \forall b \in \mathbb{Z}$
$1 \mid a \quad \forall a \in \mathbb{Z}$
$b \mid a \Leftrightarrow |b| \mid |a|$
$b \mid a \quad a \neq 0 \Rightarrow |b| \leq |a|$

Def. 1.5 voor $a, b \in \mathbb{Z}$ is $ggd^{(a,b)} = \max\{z \in \mathbb{Z} : z \mid a, z \mid b\}$ of 1 als dit $\emptyset$ is
voor $S \subset \mathbb{Z}$ is $ggd(S) = \max\{z \in \mathbb{Z} : \forall s \in S : z \mid s\}$ of 1 als dit $\emptyset$ is

Def $a, b \in \mathbb{Z}$ heten relatief priem, onderling ondeelbaar als geldt
$ggd(a,b) = 1$

1.6 (Euclidisch algoritme) voor bepaling $ggd(a,b)$ werkt zo: $a, b \in \mathbb{Z}$
definieer $r_0, r_1, r_2, \ldots$ als volgt (inductief):

$r_0 := |a|$
$r_1 := |b|$
$r_{n+1} := r$, waar $r_{n-1} = qr_n + r$, q, r uniek bepaald zoals in St. 1.1

als $r_N = 0$, stop en $ggd(a,b) = r_{N+1}$

lemma 1.8 $a, b \in \mathbb{Z}$, $b \neq 0$, $a = qb + r$ (q, b, r niet noodzakelijk als in 1.1)
Dan $ggd(a,b) = ggd(b,r)$

St. 1.9 $a, b \in \mathbb{Z}$ en $d = ggd(a,b)$. Dan $\exists x, y \in \mathbb{Z} : xa + yb = d$

1.9 (Uitgebreid Euclidisch algoritme) definieer in 1.9 ook $x_0, x_1, \ldots$
en $y_0, y_1, y_2 \ldots$ door

$q_0, q_1 \dots$ waar q_n zdd $\quad r_{n-1} = q_n r_n + r_{n+1}$

$x_0 = \operatorname{sgn}(a) := \frac{a}{|a|} \qquad y_0 = 0$

$x_1 = 0 \qquad y_1 = \operatorname{sgn}(b) := \frac{b}{|b|}$

$x_{n+1} = x_{n-1} - q_n x_n \qquad y_{n+1} = y_{n-1} - q_n y_n$

als $r_N = 0$, dan $\quad x_{N-1} a + y_{N-1} b = d$

Gevolg 1.11 $a, b \in \mathbb{Z}$, $d = ggd(a,b)$, dan $\{$delers a en b$\} \subset \{$delers d$\}$

Gevolg 1.12 $a, b \in \mathbb{Z} \quad ggd(a,b) = 1 \iff \exists x, y \in \mathbb{Z} : xa + yb = 1$

Gevolg 1.13 $a, b, c \in \mathbb{Z}$, $ggd(a,b) = 1$ Dan $\quad a \mid bc \Rightarrow a \mid c$

Def $p \in \mathbb{Z}$ heet een priemgetal als $\{$delers p$\} = \{1, p\}$ en $p > 1$

St. 1.16 zij p priem, $b, c \in \mathbb{Z}$ dan $\quad p \mid bc \Rightarrow p \mid b \vee p \mid c$

St. 1.17 meer algemeen : $p \mid b_1 b_2 \dots b_n$, $b_1, \dots b_n \in \mathbb{Z}$, dan $\exists_{1 \le i \le n} : p \mid b_i$

St. 1.18 $\forall a \in \mathbb{Z}, a > 0 : \quad a = p_1 p_2 \dots p_t$, $t \ge 0$, p_i priem $\forall 1 \le i \le t$
en dit product is uniek op volgorde van factoren na.

Def p priem, $a \in \mathbb{Z}$: $\quad ord_p(a) := \max\{ n \in \mathbb{Z}_{\ge 0} : p^n \mid a \}$

Gevolg 1.19 $ord_p(ab) = ord_p(a) + ord_p(b)$, $\forall a, b \in \mathbb{Z}$, p priem

Gevolg 1.20 $a, b \in \mathbb{Z}$, $a, b > 0$: $\quad b \mid a \iff \forall p$ priem : $ord_p(b) \le ord_p(a)$

Gevolg 1.21 $a, b \in \mathbb{Z}$, $a, b > 0$: $\quad ggd(a,b) = \prod_{p \text{ priem}} p^{\min\{ord_p(a), ord_p(b)\}}$

Def. 1.23 $a, b \in \mathbb{Z}^{a \neq 0 \neq b}$, is $\quad kgv(a,b) := \min\{ x \in \mathbb{Z}_{\ge 0} : a \mid x, b \mid x \}$
maar als $a = 0 \vee b = 0$; $\quad kgv(a,b) := 0$

St. 1.24 $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$: $\quad kgv(a,b) = \prod_{p \text{ priem}} p^{\max\{ord_p(a), ord_p(b)\}}$

Gevolg 1.24 $a, b, d \in \mathbb{Z}$: $\quad a \mid d$, $b \mid d \Rightarrow kgv(a,b) \mid d$
$a, b, d > 0$

1 OPGAVEN

- $ggd(a,b) \cdot kgv(a,b) = |ab| \quad \forall a,b \in \mathbb{Z}$
- $ggd(a,b) = ggd(a,c) = 1 \Rightarrow ggd(a,bc) = 1 \quad \forall a,b,c \in \mathbb{Z}$
- $ggd(a,b) = 1 \quad a|c \quad b|c \Rightarrow ab|c \quad \forall a,b,c \in \mathbb{Z}$
- $c \cdot ggd(a,b) = ggd(ac,bc) \quad \forall a,b,c \in \mathbb{Z}_{>0}$