

Stellingen en definities

February 29, 2008

1.1 Principe Iedere niet-lege verzameling van niet-negatieve gehele getallen bevat een kleinste element.

1.2 Stelling (Deling met rest) Laat a en b gehele getallen zijn met $b > 0$. Dan bestaan er twee eenduidig bepaalde gehele getallen q en r zodat $a = qb + r$ met $0 \leq r < b$.

1.3 Definitie Laat $a, b \in \mathbb{Z}$. We zeggen: a deelt b als er een getal $c \in \mathbb{Z}$ bestaat zodat $b = ac$.

1.4 Definitie Laat $a, b \in \mathbb{Z}$ en niet beide gelijk aan 0. De grootste gemene deler van a en b , $ggd(a, b)$, is het grootste gehele getal dat zowel a als b deelt. We definiëren $ggd(0, 0) = 0$. We zeggen dat a en b onderling ondeelbaar zijn als $ggd(a, b) = 1$.

1.5 Lemma Zij $a, b \in \mathbb{Z}$, dan geldt:

- i) $ggd(a, b) = ggd(b, a)$
- ii) $ggd(a, b) = ggd(-a, b)$
- iii) $ggd(a, b + xa) = ggd(a, b)$ voor alle $x \in \mathbb{Z}$

1.6 Stelling Zij $a, b \in \mathbb{Z}$, maar niet beide gelijk aan 0. Dan is $ggd(a, b)$ het kleinste positieve element van de verzameling $L = \{ax + by : x, y \in \mathbb{Z}\}$.

1.7 Gevolg De $ggd(a, b)$ kan geschreven worden als een lineaire combinatie van a en b . Dat wil zeggen: er bestaan $x, y \in \mathbb{Z}$ zodat $ggd(a, b) = ax + by$.

1.8 Gevolg Als d een deler van a en b is, dan ook van $ggd(a, b)$.

1.9 Propositie Zij $a, b, c \in \mathbb{Z}$ en $ggd(a, b) = 1$ en $a|bc$. Dan geldt $a|c$.

1.10 Definitie Een getal $p \in \mathbb{N}$ heet een priemgetal als $p > 1$ en als de enige positieve delers van p 1 en p zelf zijn.

1.11 Stelling Er zijn oneindig veel priemgetallen

1.12 Lemma van Euclides Zij $a, b \in \mathbb{N}$ en p een priemgetal. Als $p|ab$, dan $p|a$ of $p|b$.

1.13 Hoofdstelling van de rekenkunde Ieder geheel getal $n > 1$ kan geschreven worden als product van priemgetallen: er bestaan priemgetallen p_1, \dots, p_r zodat $n = p_1 p_2 \dots p_r$. Deze schrijfwijze is eenduidig op de volgorde na.

1.14 Definitie Laat n een positief geheel getal zijn en p een priemgetal. Dan is de orde van n bij p , genoteerd $ord_p(n)$, het aantal factoren $p_i = p$ in de schrijfwijze van 1.13. Voor negatieve n stellen we $ord_p(n) = ord_p(-n)$. Een positief geheel getal n laat zich schrijven als $\prod_{p \in \mathcal{P}} p^{ord_p(n)}$.

1.15 Lemma Een geheel getal $a \neq 0$ deelt b dan en slechts dan als $ord_p(a) \leq ord_p(b)$ voor elk priemgetal p .

1.19 Propositie Het Euclidisch algoritme is een correct algoritme: het stopt na eindig veel stappen en levert als uitkomst de grootste gemene deler.

2.1 Definitie Een equivalentierelatie op een verzameling V is een deelverzameling $R \subset V \times V$ zodat voor alle $a, b, c \in V$ geldt:

- i) $(a, a) \in R$ (reflexief)
- ii) als $(a, b) \in R$, dan ook $(b, a) \in R$ (transitief)
- iii) als $(a, b) \in R$ en $(b, c) \in R$, dan ook $(a, c) \in R$ (transitief)

2.2 Definitie Als een equivalentierelatie is op een verzameling V en $v \in V$ een element, dan heet de deelverzameling $\{w \in V : w \sim v\}$ een equivalentieklasse van v .

2.6 Definitie Een verdeling of partitie van een verzameling V is een collectie niet-lege disjuncte deelverzamelingen $V_i : i \in I$ (met I een of andere indexverzameling) van V zodat hun vereniging gelijk is aan V .

2.7 Propositie Laat V een verzameling zijn met equivalentierelatie \sim . Dan geven de equivalentieklassen een verdeling van V .

2.12 Definitie Laat R een equivalentierelatie op de verzameling V zijn. Een volledig representantensysteem voor R (ook wel een volledig stelsel van representanten) is een deelverzameling $W \subset V$ siw uit iedere equivalentieklasse precies één element bevat.

3.1 Definitie Een groep is een verzameling G voorzien van een bewerking $\circ : G \times G \rightarrow G$ en van een element $e \in G$ zodat aan de volgende eisen is voldaan:

(G1) Voor alle $x, y, z \in G$ geldt: $x \circ (y \circ z) = (x \circ y) \circ z$. (associativiteit)

(G2) Voor alle $x \in G$ geldt: $x \circ e = e \circ x = x$. (eenheidselement)

(G3) Voor alle $x \in G$ is er een element $x^* \in G$ zodat $x \circ x^* = x^* \circ x = e$.

3.2 Definitie Een groep heet commutatief of abels als in G aan de volgende eis voldaan is:

(G4) $x \circ y = y \circ x$ voor alle $x, y \in G$. (commutativiteit)

3.11 Definitie De Euler ϕ -functie $\phi(n)$ wordt voor $n \in \mathbb{Z}, n \neq 0$ gedefinieerd door $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$.

3.15 Definitie Laat G_1 en G_2 groepen zijn. Laat $G_1 \times G_2$ de verzameling van paren (x_1, x_2) zijn met $x_1 \in G_1$ en $x_2 \in G_2$. We definiëren nu de bewerking $(x_1, x_2) \circ (y_1, y_2) = (x_1 y_1, x_2 y_2)$, waarbij in de eerste factor het product in G_1 en in de tweede factor het product in G_2 bedoeld wordt. Deze verzameling is een groep.

3.16 Definitie De orde van een element $a \in G$ is het kleinste positieve getal n waarvoor $a^n = e$ geldt. Is er niet zo een n , dan zeggen we dat de orde van a oneindig is.

3.18 Propositie Zij G een groep en $c \in G$ een element.

i) Als de orde van x oneindig is, dan zijn alle elementen in de rij $(x^k)_{k \in \mathbb{Z}}$ van machten van x verschillend.

ii) Als het element x eindige orde n heeft, dan zijn er precies n verschillende machten van x en er geldt $x^{n+m} = x^m$ voor alle $m \in \mathbb{Z}$.

3.19 Propositie In een groep G is de vergelijking $ax = b$ bij gegeven $a, b \in G$ altijd oplosbaar en heeft precies één oplossing: $x = a^{-1}b$. Ook de vergelijking $xa = b$ is altijd oplosbaar en heeft precies één oplossing: $x = ba^{-1}$.

3.20 Gevolg Laat G een groep zijn en g een willekeurig element. Dan zijn de afbeeldingen $\lambda_g : G \rightarrow G, x \mapsto gx$ en $\rho_g : G \rightarrow G, x \mapsto xg$ bijecties.

4.1 Stelling Zij X een verzameling. Dan is de verzameling $S(X)$ van bijecties $X \rightarrow X$ met als bewerking de samenstelling van afbeeldingen en als eenheidselement de identieke afbeelding een groep.

4.3 Propositie Een isometrie die twee verschillende punten vastlaat is de identiteit of de spiegeling

4.4 Gevolg Een orthogonale afbeelding is een draaiing r_α om de oorsprong of een spiegeling s_l in de lijn l door de oorsprong.

4.5 Gevolg Een orthogonale afbeelding is een lineaire afbeelding. Als de determinant $+1$ is, dan is het een draaiing, is de determinant -1 , dan is het een spiegeling.

Definitie Zij $O_2(\mathbb{R}) = \{f : f \text{ is een isometrie en } f((0,0)) = (0,0)\}$ de orthogonale groep.

5.1 Definitie Zij G een groep. Een deelverzameling H van G heet een ondergroep van G als H met de bewerking van G en hetzelfde eenheidselement als G een groep vormt.

5.2 Stelling Zij G een groep en $H \subseteq G$, dan zijn de volgende beweringen equivalent:

- i) H is een ondergroep van G .
- ii) H is niet leeg en met ieder tweetal elementen $x, y \in H$ zitten ook xy en x^{-1} in H .
- iii) H is niet leeg en met ieder tweetal elementen $x, y \in H$ zit ook xy^{-1} in H .

5.4 Lemma Zij S een deelverzameling van een groep G . Dan vormt de verzameling $\langle S \rangle$ die bestaat uit alle eindige producten van elementen $x \in G$ met $x \in S$ of $x^{-1} \in S$ een ondergroep van G .

5.5 Stelling ii) De ondergroepen van \mathbb{Z} zijn $\{0\}$ en de cyclische groepen $d\mathbb{Z} = \{\dots, -2d, -d, -, d, 2d, \dots\}$ met d een positief geheel getal.

i) De ondergroepen van $\mathbb{Z}/n\mathbb{Z}$ zijn de cyclische groepen $\langle \bar{d} \rangle$ met d een positieve deler van n .

5.6 Definitie Zij G en G' twee groepen. Een afbeelding $f : G \rightarrow G'$ heet een homomorfisme als $f(xy) = f(x)f(y)$ voor alle $x, y \in G$.

5.8 Propositie Zij G (resp. G') een groep en e (resp. e') het eenheidselement. Dan geldt voor ieder homomorfisme $f : G \rightarrow G'$:

- i) $f(e) = e'$
- ii) $f(x^{-1}) = f(x)^{-1}$ voor alle $x \in G$.

5.9 Definitie Zij $f : G \rightarrow G'$ een homomorfisme. Dan is de kern van f de deelverzameling van G $\ker f = \{x \in G : f(x) = e'\}$.

5.10 Stelling Als $f : G \rightarrow G'$ een homomorfisme is, dan geldt:

- i) De kern $\ker f$ van f is een ondergroep van G .
- ii) Het beeld van f is een ondergroep van G' .
- iii) De afbeelding f is injectief dan en slechts dan als $\ker f = \{e\}$.

5.11 Propositie i) De samenstelling van twee isomorfismen is weer een isomorfisme.

ii) De inverse afbeelding $f^{-1} : G' \rightarrow G$ van een isomorfisme $f : G \rightarrow G'$ is een isomorfisme.

5.12 Stelling (Chinese reststelling) Laat m en n twee onderling ondeelbare positieve gehele getallen zijn. Dan is de afbeelding $f : \mathbb{Z}/mn\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ met $x(\text{mod } mn) \mapsto (x(\text{mod } m), x(\text{mod } n))$ een isomorfisme.

5.13 Gevolg Laat m en n positieve gehele getallen zijn die onderling ondeelbaar zijn. Laat verder $a, b \in \mathbb{Z}$ gegeven zijn. Dan heeft het stelsel vergelijkingen

$$\begin{cases} x \equiv a(\text{mod } m) \\ x \equiv b(\text{mod } n) \end{cases} \text{ een eenduidige oplossing modulo } mn.$$

6.1 Definitie Een element $\sigma \in S_n$ heet cykel als er k verschillende elementen a_1, \dots, a_k in $\{1, \dots, n\}$ zijn met $\sigma(a_1) = a_2, \sigma(a_2) = a_3, \dots, \sigma(a_{k-1}) = a_k$ en $\sigma(a_k) = a_1$ en bovendien $\sigma(a) = a$ als $a \notin \{a_1, \dots, a_n\}$.

6.3 Opmerking Twee disjuncte cyclen commuteren.

6.4 Stelling Iedere permutatie $\sigma \in S_n$ is te schrijven als product van disjuncte cyclen. Deze schrijfwijze is eenduidig op de volgorde na.

6.5 Definitie Voor $\sigma \in S_n$ definiëren we het teken $\epsilon(\sigma) \in \{\pm 1\}$ door $\sigma(d) = \epsilon(\sigma)d$. De permutaties met $\epsilon(\sigma) = 1$ heten even, de andere oneven.

6.6 Propositie Het teken definitieert voor $n \geq 2$ een surjectief homomorfisme $\epsilon : S_n \rightarrow \{+1, -1\}$, dus $\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau)$ voor alle $\sigma, \tau \in S_n$.

6.7 Propositie Ieder element uit S_n is een product van verwisselingen.

6.8 Definitie De kern van het tekenhomomorfisme heet de alternerende groep $A_n = \{\sigma \in S_n : \epsilon(\sigma) = 1\}$.

6.9 Stelling De groep A_n wordt voortgebracht door de 3-cyclen.

6.10 Stelling van Cayley Iedere eindige groep G is isomorf met een ondergroep van een symmetrische groep S_n .

6.12 Propositie De symmetriegroep G_T van een tetraëder is isomorf met S_4 .

6.13 Propositie De groep G_I^+ van orthogonale symmetriën (rotaties) van een icosaeëder is isomorf met de alternerende groep A_5 .

7.1 Definitie Laat H een ondergroep van een groep G zijn. Een linkernevenklasse van H is een deelverzameling van de vorm $gH = \{gh : h \in H\}$. Een rechternevenklasse van H is een deelverzameling van de vorm $Hg = \{hg : h \in H\}$.

7.4 Gevolg Zij $f : G \rightarrow G'$ een homomorfisme met $\ker f = H$. Dan geldt voor alle $g \in G$: $f^{-1}(f(g)) = gH = Hg$.

7.5 Definitie De index van een ondergroep H in een groep G is de cardinaliteit van een volledig stelsel van representanten van de linkernevenklassen van H in G . Notatie: $[G : H]$. Als H eindig veel linkernevenklassen heeft dan is $[G : H]$ gewoon het aantal linkernevenklassen.

7.7 Stelling (Lagrange) Zij G een eindige groep en H een ondergroep van G . Dan geldt $\#G = [G : H]\#H$.

7.8 Gevolg Zij G een eindige groep.

- i) De orde $\#H$ van een ondergroep deelt de orde $\#G$ van G .
- ii) De orde van een element $x \in G$ deelt de orde $\#G$ van G .

7.9 Gevolg Iedere eindige groep met als orde een priemgetal p is isomorf met $\mathbb{Z}/p\mathbb{Z}$.

7.10 Gevolg (Kleine stelling van Fermat) Zij p een priemgetal en $a \in \mathbb{Z}$ een getal dat niet deelbaar is door p . Dan geldt $a^{p-1} \equiv 1 \pmod{p}$.

7.11 Gevolg Voor elk priemgetal p en voor elke $a \in \mathbb{Z}$ geldt $a^p \equiv a \pmod{p}$.

8.1 Definitie Laat G een groep zijn en X een verzameling. We zeggen dat G werkt op X

als er een afbeelding $G \times X \rightarrow X$ met $(g, x) \mapsto g \circ x$ gegeven is die voldoet aan

- W1. $e \circ x = x$ voor alle $x \in X$.
- W2. $(gh) \circ x = g \circ (h \circ x)$ voor alle $g, h \in G$ en $x \in X$.

8.1a Definitie Een werking van een groep G op een verzameling X is een homomorfisme $\mu : G \rightarrow S(X)$.

8.4 Definitie Laat G een groep zijn die werkt op een verzameling X . Als x een punt is van X dan heet $Gx = \{gx : g \in G\}$ de baan van x . De stabilisator of isotropiegroep van x is de ondergroep $G_x = \{g \in G : gx = x\}$.

8.6 Propositie Als G op X werkt, dan levert de afbeelding $g \mapsto gx$ een bijectie $G/Gx \leftrightarrow GX$ tussen de linkernevenklassen van G_x en de punten van de baan van X en dus $\#Gx = [G : G_x]$.

8.7 Lemma Laat G een groep zijn die op een verzameling X werkt. Dan geldt $G_{gx} = gG_xg^{-1}$.

8.8 Definitie Een punt $x \in X$ met $Gx = \{x\}$ onder een werking van G heet een vast punt of dekpunt. De verzameling vaste punten wordt genoteerd met X^G .

8.9 Propositie Laat p een priemgetal zijn en G een groep waarvan de orde een macht van p is. Als G op een verzameling X werkt, dan geldt de congruentie $\#X^G \equiv \#X \pmod{p}$.

8.10 Stelling (Cauchy) Laat G een eindige groep zijn en p een priemgetal dat de orde van G deelt. Dan bevat G een element van orde p .

9.1 Definitie-Stelling Een ondergroep H van een groep G heet een normaaldeeler als aan één van de volgende drie equivalente eigenschappen voldaan is:

- i) $ghg^{-1} \in H$ voor alle $g \in G$ en $h \in H$.
- ii) $gHg^{-1} = H$ voor alle $g \in G$.
- iii) $gH = Hg$ voor alle $g \in G$.

9.7 Stelling Met de bewerking $g_1N \circ g_2N = g_1g_2N$ wordt G/N een groep. De afbeelding $\phi : G \rightarrow G/N$ met $g \mapsto gN$ is een surjectief homomorfisme met kern N .

9.9 Stelling Laat G een groep zijn met centrum $Z(G)$ zodat $G/Z(G)$ cyclisch is. Dan is G abels.

9.10 Stelling Laat G een groep zijn en N een normaaldeeler van G . De ondergroepen van G/N zijn precies de ondergroepen $H/N = \{hN : h \in H\}$.

9.11 Stelling Laat G een groep zijn en N een normaaldeeler van G . Dan is G/N abels dan en slechts dan als N de commutatorondergroep $[G, G]$ bevat.

9.12 Propositie Laat G een eindige groep zijn en laat p de kleinste priem zijn die de orde van G deelt. Een ondergroep H van G met index $[G : H] = p$ is een normaaldeler.

10.1 Homomorfiestelling Laat $f : G \rightarrow G'$ een homomorfisme van een groep G naar een groep G' zijn. Laat N een normaaldeler van G zijn met $N \subseteq \ker f$. Dan is er een eenduidig bepaald homomorfisme $h : G/N \rightarrow G'$ zodat $h(gN) = f(g)$ voor alle $g \in G$.

10.2 Eerste isomorfiestelling Laat $f : G \rightarrow G'$ een homomorfisme van groepen zijn. Dan geldt $G/\ker f \cong f(G)$.

10.4 Propositie Laat $f : G \rightarrow A$ een homomorfisme zijn van een groep G naar een abelse groep A . Dan is er een eenduidig bepaald homomorfisme $h : G_{ab} = G/[G, G] \rightarrow A$ zodat $f = h\phi$.

10.5 Tweede isomorfiestelling Laat N een normaaldeler van G zijn en H een ondergroep. Dan is er een isomorfisme $H/(H \cap N) \cong HN/N$.

10.7 Stelling Laat N en N' normaaldelers van een groep G zijn met $N \subset N' \subset G$. Iedere normaaldeler van G/N is van de vorm M/N met M een normaaldeler van G met $N \subset M \subset G$. In het bijzonder is N'/N een normaaldeler van G/N en er geldt $(G/N)/(N'/N) \cong G/N'$.

10.8 Stelling Laat H een ondergroep zijn van G met index $[G : H] = n$. Dan is er een normaaldeler $N \subseteq H$ waarvan de index $[G : N]$ een deler is van $n!$.