II.2 Gehele getallen

We beginnen met de eigenschappen van de gehele getallen.

Axioma's voor $\mathbb{Z}$

De *gegevens* zijn:

(a) een verzameling $\mathbb{Z}$;
(b) elementen 0 en 1 in $\mathbb{Z}$;
(c) een afbeelding $+\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$, de optelling;
(d) een afbeelding $\cdot\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$, de vermenigvuldiging.

We schrijven meestal ab voor $a\cdot b$.

De optelling voldoet aan de volgende *eigenschappen*:

(Z0) de optelling is *commutatief*: voor alle $a,b\in\mathbb{Z}$ geldt $a+b=b+a$;
(Z1) de optelling is *associatief*: voor alle $a,b,c\in\mathbb{Z}$ geldt $(a+b)+c=a+(b+c)$;
(Z2) 0 is *neutraal* voor de optelling, d.w.z., voor alle $a\in\mathbb{Z}$ geldt $0+a=a$ en $a+0=a$;
(Z3) additieve inversen bestaan: voor alle $a\in\mathbb{Z}$ bestaat er een $b\in\mathbb{Z}$ zodat $a+b=0$.

Uit deze axioma's kunnen we al een belangrijke eigenschap van de optelling in $\mathbb{Z}$ afleiden.

II.2.1 Propositie (Schrappingswet in $\mathbb{Z}$)**.** Zij $a,b,c\in\mathbb{Z}$. Als $a+c=b+c$ dan $a=b$.

Bewijs. Neem aan dat $a+c=b+c$. Wegens **(Z3)** bestaat er een $d\in\mathbb{Z}$ zodat $c+d=0$. We hebben nu

$$a \overset{(\mathbf{Z2})}{=} a+0=a+(c+d) \overset{(\mathbf{Z1})}{=} (a+c)+d$$

en analoog

$$b \overset{(\mathbf{Z2})}{=} b+0=b+(c+d) \overset{(\mathbf{Z1})}{=} (b+c)+d.$$

Maar omdat $a+c=b+c$ volgt nu dat $a=b$, wat we moesten bewijzen. ■

In het bijzonder volgt uit de schrappingswet dat de additieve inversen uit axioma **(Z3)** uniek zijn: als $a+b=0$ en $a+b'=0$, en dus $a+b=a+b'$, dan volgt dat $b=b'$. We zullen voortaan de unieke additieve inverse van a met $-a$ noteren. Dus $-a$ is per definitie het unieke element van $\mathbb{Z}$ waarvoor geldt $a+(-a)=0$.

De vermenigvuldiging in $\mathbb{Z}$ voldoet aan:

(Z4) de vermenigvuldiging is *commutatief*: voor alle $a,b\in\mathbb{Z}$ geldt $ab=ba$;
(Z5) de vermenigvuldiging is *associatief*: voor alle $a,b,c\in\mathbb{Z}$ geldt $(ab)c=a(bc)$;
(Z6) 1 is *neutraal* voor de vermenigvuldiging, d.w.z., voor alle $a\in\mathbb{Z}$ geldt $1\cdot a=a\cdot 1=a$;
(Z7) de *distributieve* eigenschap geldt: voor alle $a,b,c\in\mathbb{Z}$ geldt $a(b+c)=ab+ac$;

De axioma's **(Z0)**–**(Z7)** drukken samen uit dat $(\mathbb{Z},0,1,+,\cdot)$ een *ring* is. Ook de rationale getallen $\mathbb{Q}$ en de reële getallen $\mathbb{R}$ vormen ringen. Maar $\mathbb{N}$ is geen ring want niet alle natuurlijke getallen hebben een additieve inverse in $\mathbb{N}$.

Om $\mathbb{Z}$ te karakteriseren hebben we nog drie axioma's nodig.

(Z8) als $A\subseteq\mathbb{Z}$ voldoet aan

(i) $0 \in A$ en $1 \in A$, en

(ii) als $a \in A$ dan $-a \in A$, en

(iii) als $a, b \in A$ dan $a + b \in A$,

dan $A = \mathbb{Z}$;

(Z9) de verzameling $\mathbb{Z}$ is niet eindig;

(Z10) voor alle $a, b \in \mathbb{Z}$ met $ab = 0$ geldt dat $a = 0$ of $b = 0$.

Men kan bewijzen dat de bovenstaande lijst eigenschappen het gegeven $(\mathbb{Z}, 0, 1, +, \cdot)$ uniek bepaalt, in dezelfde zin als we dat voor de natuurlijke getallen hebben gezien. Het is niet zo moeilijk te bewijzen dat ieder element van $\mathbb{Z}$ een eindige som van de vorm $1 + \cdots + 1$ is, of -1 maal zo'n som. Dus inderdaad is $\mathbb{Z}$ gelijk aan $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, en **(Z9)** impliceert dat de elementen $0, 1, 2, 3, \ldots$ verschillend zijn. We vinden dus $\mathbb{N}$ terug als deelverzameling van $\mathbb{Z}$, en men kan nagaan dat voor $n, m \in \mathbb{N}$ geldt dat $n +_{\mathbb{N}} m = n +_{\mathbb{Z}} m$ en $n \cdot_{\mathbb{N}} m = n \cdot_{\mathbb{Z}} m$. Later in het college zullen we een rigoureuze constructie geven van $\mathbb{Z}$, uitgaande van $\mathbb{N}$ (zie pagina 36).

Uit bovenstaande axioma's kunnen we alle gebruikelijke rekenregels voor gehele getallen afleiden.

II.2.2 Voorbeeld. Zij $a, b \in \mathbb{Z}$.

(i) Als $a + b = b$ dan $a = 0$;

(ii) $0 \cdot a = 0$;

Bewijs (i) Als $a + b = b$ dan geldt wegens **(Z2)** dat $a + b = 0 + b$ en wegens de schrappingswet volgt nu dat $a = 0$.

(ii) Wegens **(Z2)** geldt $0 + 1 = 1$, dus geldt ook $(0 + 1) \cdot a = 1 \cdot a$. Met de distributiviteit **(Z7)** leiden we af dat $0 \cdot a + 1 \cdot a = 1 \cdot a$, en wegens (i) volgt nu $0 \cdot a = 0$. ∎

Voor meer rekenregels, zie opgave II.2.1.

Aftrekken

De reden om $\mathbb{N}$ uit te breiden tot $\mathbb{Z}$ is dat we voor gehele getallen a en b nu het verschil kunnen definiëren als:

$$a - b = a + (-b).$$

We hebben hiermee een nieuwe operatie op $\mathbb{Z}$ gedefinieerd, aftrekken:

$$- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (a, b) \mapsto a - b.$$

Ongelijkheiden

We definiëren op $\mathbb{Z}$ een ongelijkheid $\leq$ als volgt: voor $n, m \in \mathbb{Z}$ geldt $n \leq m$ dan en slechts dan als $m - n \in \mathbb{N}$. Uitgaande van $\leq$ kan men dan ook $<$, $>$ en $\geq$ definiëren.

Deelbaarheid

Zoals bekend is deling in $\mathbb{Z}$ niet altijd mogelijk: er is geen $x \in \mathbb{Z}$ die aan de vergelijking $5x = 13$ voldoet. Daarentegen heeft de vergelijking $2x = 6$ wel een oplossing binnen $\mathbb{Z}$: neem $x = 3$. Dit leidt tot de volgende definitie:

II.2.3 Definitie. Als de vergelijking $bx = a$ met $a, b \in \mathbb{Z}$ een oplossing $x \in \mathbb{Z}$ heeft dan zeggen we dat a *deelbaar is* door b of dat b een *deler* van a is en schrijven we $b \mid a$. Als b geen deler van a is schrijven we $b \nmid a$.

Delen met rest

Als a niet deelbaar is door b, en $b \neq 0$, dan kunnen we toch proberen a door b te delen, we houden dan wel een rest over.

II.2.4 Definitie. Voor a in $\mathbb{Z}$ definiëren we $|a|$ in $\mathbb{Z}$ door: $|a| = a$ als $a \geq 0$, en $|a| = -a$ als $a < 0$.

II.2.5 Stelling. Voor alle $a, b \in \mathbb{Z}$ met $b \neq 0$ bestaan unieke q en r in $\mathbb{Z}$ zó dat

$$a = q \cdot b + r \text{ en } 0 \leqslant r < |b|.$$

Het getal q heet het *quotiënt* en r heet de *rest* [1] bij deling van a door b. Als $r = 0$ dan schrijven we $q = a/b$.

Bewijs. Laat $a, b \in \mathbb{Z}$ met $b \neq 0$. We definiëren $A \subseteq \mathbb{N}$ door:

$$A = \{n \in \mathbb{N} : \text{ er is een } q \in \mathbb{Z} \text{ met } a = q \cdot b + n\}.$$

In Opgave II.2.9 wordt bewezen dat A niet leeg is (dit is duidelijk als $a \geq 0$, want $a = q \cdot 0 + a$, dus $a \in A$). Volgens Stelling II.1.5 bevat A een kleinste element; we noemen het r.

We bewijzen dat $0 \leqslant r < |b|$. Neem eens aan dat $r \geqslant |b|$, dan is $s = r - |b| \in \mathbb{N}$ en a is te schrijven als

$$a = q \cdot b + r = q \cdot b + |b| + s = \begin{cases} (q+1) \cdot b + s & \text{als } b > 0 \\ (q-1) \cdot b + s & \text{als } b < 0. \end{cases}$$

Hieruit volgt dat $s \in A$ en omdat $s < r$ kregen we een tegenspraak met de minimaliteit van r.

Dat de getallen q en r uniek zijn wordt aangetoond in Opgave II.2.10. ■

Merk op dat als bij deling van a door b de rest gelijk aan 0 is dan is a deelbaar door b, en omgekeerd, als $b \mid a$ en $b \neq 0$, dan is de rest bij deling van a door b gelijk aan nul.

II.2.6 Voorbeeld. Beschouw $a = -31$ en $b = 5$, dan geldt $-31 = -7 \cdot 5 + 4$; het quotiënt bij deling van -31 door 5 is $q = -7$ en de rest $r = 4$. En, bijvoorbeeld, $12 = (-2) \cdot (-5) + 2$, dus quotiënt en rest bij deling van 12 door -5 zijn -2 en 2, respectievelijk. ▬

II.2.7 Voorbeeld. Beschouw deling door 2; de verzameling $\mathbb{Z}$ valt dan in twee disjuncte deelverzamelingen uiteen: in de verzameling $2\mathbb{Z}$ van alle gehele getallen die deelbaar door 2 zijn, en in de verzameling $2\mathbb{Z} + 1$ van alle gehele getallen die niet deelbaar door 2 zijn (en dus bij deling door 2 de rest 1 hebben)[2].

Analoog, bij deling door $n \in \mathbb{N} \setminus \{0\}$ valt $\mathbb{Z}$ in n disjuncte deelverzamelingen uiteen:

$$\mathbb{Z} = \bigcup_{k=0}^{n-1} n\mathbb{Z} + k,$$

waarbij $n\mathbb{Z} + k$ de verzameling van alle gehele getallen is die bij deling door n de rest k hebben. ▬

Priemgetallen

Een *priemgetal* is een natuurlijk getal $n > 1$ dat alléén 1 en zichzelf als positieve delers heeft. M.a.w., $n \in \mathbb{N}$ is priem precies dan als n precies twee delers heeft. Bijvoorbeeld 2 en 13 zijn priemgetallen maar 15 is geen priemgetal omdat $3 \mid 15$.

[1] De lezer wordt hierbij aangeraden over de hem/haar gebruikte programmeertalen na te gaan of deze definitie, toch echt de enige goede, ook daar van kracht is. Eén van de auteurs heeft eens een hoop tijd verloren doordat in Pascal de rest na deling van -7 door 5 gelijk bleek aan -2 in plaats van 3.

[2] Elementen van $2\mathbb{Z}$ heten *even* en elementen van $2\mathbb{Z} + 1$ heten *oneven* getallen.

II.2.8 Lemma. Elk natuurlijk getal groter dan 1 is deelbaar door een priemgetal.

Bewijs. Zij $k \in \mathbb{N} \setminus \{0,1\}$ en beschouw de verzameling

$$A = \{n \in \mathbb{N} : n > 1 \text{ en } n \mid k\}.$$

Omdat $k > 1$ en $k \mid k$ is $k \in A$ en volgens Stelling II.1.5 bevat A een minimaal element m. Dan moet m een priemgetal zijn want anders is m te schrijven als $m = s \cdot t$ met $s > 1$ en $t > 1$. Hieruit volgt dat $s, t \in A$ en $s, t < m$ wat in tegenspraak is met de minimaliteit van m. ■

Als n een klein natuurlijk getal is dan is het niet moeilijk om na te gaan of n een priemgetal is: we kunnen bijvoorbeeld controleren dat geen natuurlijk getal kleiner dan of gelijk aan $\sqrt{n}$ en groter dan 1 een deler is. Naarmate n groter is wordt het steeds moeilijker want zo'n controle kost, ook met 'supersnelle' computers, te veel tijd. Het komt daarom misschien als een verrassing dat het makkelijk te bewijzen is dat er oneindig veel priemgetallen bestaan.

II.2.9 Stelling. Er zijn oneindig veel priemgetallen.

Bewijs. Neem aan dat $p_1, p_2, \ldots, p_N$ alle priemgetallen zijn. Beschouw het getal

$$K = p_1 \cdot p_2 \cdots p_N + 1.$$

We bewijzen eerst dat geen p_i, $i \leqslant N$ een deler van K is. Dit volgt uit het feit dat, voor elke i, de rest na deling van K door p_i gelijk is aan 1, en niet aan 0.

Omdat 2 één van de p_i is, geldt $K \geq 3$. Volgens Lemma II.2.8 is K deelbaar door een priemgetal p. Maar dan moet p ongelijk zijn aan elk van de p_i. Dit is een tegenspraak: we hebben aangenomen dat $p_1, p_2, \ldots, p_N$ *alle* priemgetallen waren. ■

Opgaven

1. Bewijs direct uit de axioma's voor $\mathbb{Z}$, dat voor alle $a, b \in \mathbb{Z}$ geldt:
(a) $-(a+b) = (-a) + (-b)$;
(b) $-0 = 0$;
(c) $-(ab) = (-a) \cdot b$;
(d) $(-a) \cdot (-b) = a \cdot b$;
(e) $(-1) \cdot a = -a$;
(f) $-(-a) = a$.

2. Bewijs dat $1 \neq 0$. (Hint: gebruik axioma **(Z9)**).

3. Bewijs de multiplicatieve schrappingswet: als $a, b, c \in \mathbb{Z}$ en $c \neq 0$, en als $ac = bc$ dan $a = b$. (Hint: gebruik axioma **(Z10)**).

✯ **4.** Bewijs dat axioma **(Z10)** volgt uit de axioma's **(Z0)**–**(Z9)**.

5. Laat zien dat de verzameling $\mathbb{F}_2$ met twee verschillende elementen $\{0,1\}$, en met de operaties $+$ en $\cdot$ gedefinieerd door $0+0=0$, $0+1=1+0=1$, $1+1=0$, $0 \cdot 0 = 1 \cdot 0 = 0 \cdot 1 = 0$ en $1 \cdot 1 = 1$ voldoet aan de axioma's **(Z0)**–**(Z8)** voor $\mathbb{Z}$.

6. Bewijs dat voor alle $a, b, c \in \mathbb{Z}$ geldt
   (a) als $a \mid b$ en $a \mid c$ dan $a \mid (b + c)$;
   (b) als $a \mid b$ dan $ac \mid bc$;
   (c) als $a \mid b$ dan $a \mid bc$;
   (d) als $a \mid b$ en $b \mid c$ dan $a \mid c$.

✯ **7.** Bewijs dat voor alle $a, b \in \mathbb{Z}$ geldt dat als $a \mid b$ en $b \mid a$ dan $a = \pm b$;

✍ **8.** Bewijs of weerleg: voor alle $a, b, c \in \mathbb{Z}$ geldt dat als $a \mid bc$, dan $a \mid b$ of $a \mid c$.

9. Bewijs, onder de aannamen van Stelling II.2.5, dat er een q in $\mathbb{Z}$ is met $a - qb \geq 0$.

✍ **10.** Bewijs dat de getallen q en r in Stelling II.2.5 uniek zijn.

✍ **11.** Laat a en b natuurlijke getallen zijn en neem aan dat $a = qb + r$ met $q, r \in \mathbb{Z}$ en $0 \leqslant r < b$. Vind het quotiënt en de rest bij deling van $-a$ door b en verklaar je antwoord.

12. Laat Ω een verzameling zijn, en R de verzameling van alle functies $f\colon \Omega \to \mathbb{F}_2$ (zie opgave II.2.5). Voor $f, g \in R$ definiëren we $f+g$ en fg in R door $(f+g)\colon x \mapsto f(x)+g(x)$ en $fg\colon x \mapsto f(x)g(x)$. Voor iedere $A \subseteq \Omega$ definiëren we de *karakteristieke functie* 1_A van A door: $1_A(x) = 1$ als $x \in A$ en $1_A(x) = 0$ als $x \notin A$.
   (a) Laat zien dat de afbeelding $\mathcal{P}(A) \to R$, $A \mapsto 1_A$ een bijectie is.
   (b) Laat zien dat voor alle $A, B \in \mathcal{P}(A)$ geldt dat $1_{A\cap B} = 1_A 1_B$.
   (c) Laat zien dat voor alle $A, B \in \mathcal{P}(A)$ geldt dat $1_A + 1_B = 1_{(A\cup B)\setminus(A\cap B)}$.
   (d) Laat zien dat voor alle $A, B \in \mathcal{P}(A)$ geldt dat $1_{A\cup B} = 1_A + 1_B + 1_A 1_B$, en $1_{\Omega\setminus A} = 1_\Omega + 1_A$.
   (e) Doe nu opnieuw de sommen in sectie I.2 waarin identiteiten tussen verzamelingen moeten worden bewezen, maar nu door te rekenen met de gebruikelijke regels voor optelling en vermenigvuldiging in R (merk op dat $f^2 = f$ voor alle f in R).