II.4 Rationale getallen

We geven axioma's voor $\mathbb{Q}$ en beschrijven kort een constructie van $\mathbb{Q}$ uit $\mathbb{Z}$.

Axioma's voor $\mathbb{Q}$

De *gegevens* zijn:

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

De optelling voldoet aan dezelfde eigenschappen als de optelling in $\mathbb{Z}$:

(Q0) de optelling is *commutatief*: voor alle $a, b \in \mathbb{Q}$ geldt $a + b = b + a$;
(Q1) de optelling is *associatief*: voor alle $a, b, c \in \mathbb{Q}$ geldt $(a+b)+c = a+(b+c)$;
(Q2) 0 is *neutraal* voor de optelling, d.w.z., voor alle $a \in \mathbb{Q}$ geldt $0 + a = a$ en $a + 0 = a$;
(Q3) additieve inversen bestaan: voor alle $a \in \mathbb{Q}$ bestaat er een $b \in \mathbb{Q}$ zodat $a + b = 0$.

Op dezelfde wijze als voor $\mathbb{Z}$ kunnen we hieruit de additieve schrappingswet afleiden.

II.4.1 Propositie (Additieve schrappingswet in $\mathbb{Q}$)**.** Zij $a, b, c \in \mathbb{Q}$. Als $a+c = b+c$ dan $a = b$.

Opnieuw volgt hieruit dat de additieve inversen uniek zijn, en we zullen de additieve inverse van $a \in \mathbb{Q}$ met $-a$ noteren.

De vermenigvuldiging voldoet aan de volgende eigenschappen

(Q4) de vermenigvuldiging is *commutatief*: voor alle $a, b \in \mathbb{Q}$ geldt $ab = ba$;
(Q5) de vermenigvuldiging is *associatief*: voor alle $a, b, c \in \mathbb{Q}$ geldt $(ab)c = a(bc)$;
(Q6) 1 is *neutraal* voor de vermenigvuldiging, d.w.z., voor alle $a \in \mathbb{Q}$ geldt $1 \cdot a = a$ en $a \cdot 1 = a$;
(Q7) de *distributieve* eigenschap geldt: voor alle $a, b, c \in \mathbb{Q}$ geldt $a(b+c) = ab+ac$;

met ander woorden $(\mathbb{Q}, 0, 1, +, \cdot)$ is een ring. Het volgende axioma drukt uit dat we in $\mathbb{Q}$ ook kunnen delen (door elementen verschillend van 0):

(Q8) multiplicatieve inversen bestaan: voor alle $a \in \mathbb{Q}$ met $a \neq 0$ bestaat er een $b \in \mathbb{Q}$ zodat $ab = 1$.

Met kan bewijzen dat multiplicatieve inversen uniek zijn, en we zullen de multiplicatieve inverse van a met $1/a$ of met a^{-1} noteren.

Totnogtoe voldoet ook bijvoorbeeld $\mathbb{R}$ aan de axioma's. Om $\mathbb{Q}$ te karakteriseren hebben we nog twee axioma's nodig.

(Q9) als $A \subseteq \mathbb{Q}$ voldoet aan
(i) $0 \in A$ en $1 \in A$, en
(ii) als $a \in A$ dan $-a \in A$, en
(iii) als $a \in A$ met $a \neq 0$ dan $1/a \in A$, en
(iv) als $a, b \in A$ dan $a + b \in A$ en $ab \in A$;
dan $A = \mathbb{Q}$;
(Q10) de verzameling $\mathbb{Q}$ is niet eindig.

Men kan bewijzen dat de bovenstaande lijst eigenschappen het gegeven $(\mathbb{Q}, 0, 1, +, \cdot)$ uniek bepaalt, in dezelfde zin als we dat voor de natuurlijke getallen hebben gezien.

Delen

De reden om $\mathbb{Z}$ uit te breiden tot $\mathbb{Q}$ is dat we voor rationale getallen a en b met $b \neq 0$ nu ook het quotiënt van a en b kunnen definieren:

$$a/b = a \cdot (1/b).$$

We hebben hiermee een nieuwe operatie op $\mathbb{Q}$ gedefinieerd, delen:

$$/ \colon \mathbb{Q} \times (\mathbb{Q}\backslash\{0\}) \to \mathbb{Q}, \quad (a,b) \mapsto a/b.$$

Constructie van $\mathbb{Q}$

De axioma's voor $\mathbb{Q}$ impliceren dat ieder element van $\mathbb{Q}$ van de vorm a/b is, met $a, b \in \mathbb{Z}$ en $b \neq 0$. Bovendien geldt voor $a, b, a', b' \in \mathbb{Z}$ met $b \neq 0$ en $b' \neq 0$, dat

$$a/b = a'/b' \quad (\text{in } \mathbb{Q}) \quad \Leftrightarrow \quad ab' = a'b \quad (\text{in } \mathbb{Z}).$$

Met andere woorden, de afbeelding $q \colon \mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$ met $q(a,b) = a/b$ is een quotiëntafbeelding voor de equivalentierelatie

$$(a,b) \sim (a',b') \quad \Leftrightarrow \quad ab' = a'b.$$

Dit propositie suggereert dat we $\mathbb{Q}$ uit $\mathbb{Z}$ kunnen *construeren* als $\mathbb{Z}\times(\mathbb{Z}\backslash\{0\})/\sim$. Het is inderdaad mogelijk om uit de optelling en vermenigvuldiging in $\mathbb{Z}$ een optelling en vermenigvuldiging op $\mathbb{Z} \times (\mathbb{Z}\backslash\{0\})/\sim$ te definiëren zodat

$$(\mathbb{Z} \times (\mathbb{Z}\backslash\{0\})/\sim, \overline{(0,1)}, \overline{(1,1)}, +, \cdot)$$

voldoet aan alle axioma's **(Q0)**–**(Q10)**.

$\sqrt{2}$

Het reële getal $\sqrt{2}$ is niet rationaal, nauwkeuriger:

II.4.2 Stelling. Er is geen $x \in \mathbb{Q}$ met $x^2 = 2$.

Bewijs. Stel dat er een $x \in \mathbb{Q}$ is met $x^2 = 2$. Dan zijn er $a, b \in \mathbb{Z}$, met $b \neq 0$ zodat $x = a/b$ en geldt dus

$$a^2 = 2b^2.$$

We mogen aannemen dat $b > 0$ en dat b de kleinst mogelijke noemer is. Merk op dat a noodzakelijk even is, immers als a oneven is dan is ook a^2 oneven, maar $2b^2$ is even. Er is dus een $a' \in \mathbb{Z}$ met $a = 2a'$. Invullen in de bovenstaande identiteit levert dan $4a'^2 = 2b^2$ en dus

$$b^2 = 2a'^2.$$

Op dezelfde manier volgt nu dat $b = 2b'$ voor een $b' \in \mathbb{Z}$, en we vinden een oplossing a'/b' met een kleinere noemer, een tegenspraak. ∎

We zullen later bewijzen dat de vergelijking $x^2 = 2$ wel degelijk een oplossing heeft in $\mathbb{R}$. Een reëel getal wat niet rationaal is heet *irrationaal*.

Opgaven

1. Bewijs uit de axioma's voor $\mathbb{Z}$ dat de relatie

$$(a,b) \sim (a',b') \quad \Leftrightarrow \quad ab' = a'b$$

op $\mathbb{Z} \times \mathbb{Z}\backslash\{0\}$ een equivalentierelatie is.

2. Bewijs dat er geen $x \in \mathbb{Q}$ is zodat $x^2 = 3$.

3. Bewijs dat $\mathbb{F}_2$ (zie opgave II.2.5) voldoet aan axioma's **(Q0)**–**(Q9)**, maar niet aan **(Q10)**.