

Hoofdstuk 1

Lichamen

Inleiding

In **Lineaire Algebra 1** en **2** heb je al kennis gemaakt met de twee belangrijkste begrippen uit de lineaire algebra: *vectorruimte* en *lineaire afbeelding*. In dit hoofdstuk gaan we die begrippen generaliseren, en wel door toe te staan dat de *scalaires* uit andere objecten bestaan dan de reële en complexe getallen, waartoe ze tot dusverre beperkt waren. De scalaires moeten aan zekere eisen voldoen om de gegeneraliseerde definitie zinnig te maken; zo moet je scalaires kunnen optellen en met elkaar vermenigvuldigen, en moeten er speciale scalaire elementen 1 en 0 zijn. Je krijgt de eigenschappen van vectorruimten terug wanneer je eist dat de scalaires een *lichaam* vormen. Onze eerste taak zal zijn om lichamen te definiëren en er voorbeelden van te geven.

Lichamen

Voor een algemenere definitie van vectorruimte zullen we eigenschappen van de reële getallen bestuderen en proberen in een abstracte definitie te vangen. Vervolgens zullen we kijken naar andere objecten die aan diezelfde eigenschappen voldoen.

De eigenschappen waar we op doelen zijn niet uitsluitend die van de *getallen* zelf, maar ook van de *bewerkingen* die je er op uit kunt voeren: je kunt reële getallen bij elkaar optellen, en je kunt ze met elkaar vermenigvuldigen. Een lichaam zal een verzameling zijn waar we op soortgelijke manier 2 operaties hebben die aan overeenkomstige eigenschappen voldoen. Die eigenschappen zijn dat het niet uitmaakt in welke volgorde je getallen optelt (of vermenigvuldigt), dat er speciale reële getallen zijn (namelijk 0 en 1) die bij optelling of vermenigvuldiging geen effect hebben, en de manier waarop de vermenigvuldiging zich ‘verdeelt’ over de optelling (we maken dat precies in 1.3).

Maar eerst definiëren we preciezer wat een *bewerking* is, omdat we meer algemene operaties willen toestaan dan alleen optelling en vermenigvuldiging.

Definitie 1.1 Als V een verzameling is, geven we met $V \times V$ de verzameling *geordende paren* (v_1, v_2) met $v_1, v_2 \in V$ aan. Een *bewerking* $\cdot$ op een verzameling V is een afbeelding van $V \times V$ naar V . Een bewerking is *commutatief* als $v_1 \cdot v_2 = v_2 \cdot v_1$ voor elk tweetal $v_1, v_2 \in V$, en een bewerking $\cdot$ heet *associatief* als $(v_1 \cdot v_2) \cdot v_3 = v_1 \cdot (v_2 \cdot v_3)$, voor elk drietal v_1, v_2, v_3 .

Met andere woorden: een bewerking voegt aan elk paar elementen van V een derde element toe. Bij een commutatieve bewerking maakt het niet uit in welke volgorde je de bewerking uitvoert en voor een associatieve bewerking maakt het niet uit hoe je de haakjes zet in $v_1 \cdot v_2 \cdot v_3$.

Voorbeelden 1.2 Je kent al heel veel voorbeelden van bewerkingen: we keken al naar de optelling en vermenigvuldiging van reële getallen. Let wel op: bij een bewerking hoort een verzameling. Je kunt niet zeggen dat $+$ een bewerking is, maar wel dat $+$ een bewerking is op de reële getallen (of de gehele getallen, enz.).

- (i) Op een verzameling E die uit slechts één element e bestaat, kun je maar op één manier een bewerking definiëren: $e \cdot e = e$.
- (ii) Optellen vormt een bewerking op de natuurlijke getallen $\mathbb{N}$. Evenzo op de gehele getallen $\mathbb{Z}$, de rationale getallen $\mathbb{Q}$, de reële getallen $\mathbb{R}$ en de complexe getallen $\mathbb{C}$. Dit is in alle gevallen een commutatieve bewerking.
- (iii) Aftrekken is een bewerking op de gehele getallen $\mathbb{Z}$, en op $\mathbb{Q}$, $\mathbb{R}$ en $\mathbb{C}$, maar niet op $\mathbb{N}$. En in geen van deze gevallen is de bewerking commutatief.
- (iv) Delen is een bewerking op de verzameling $\mathbb{Q} \setminus \{0\}$ van rationale getallen die ongelijk aan nul zijn, en evenzo op $\mathbb{R} \setminus \{0\}$ en $\mathbb{C} \setminus \{0\}$. Maar niet op $\mathbb{N} \setminus \{0\}$ en ook niet op $\mathbb{Z} \setminus \{0\}$.
- (v) De gebruikelijke optelling van $n \times n$ matrices is een bewerking op de verzameling $M_n(\mathbb{R})$ van $n \times n$ matrices met reële coëfficiënten. Hetzelfde geldt voor de vermenigvuldiging. Optellen is hier commutatief maar vermenigvuldigen niet!
- (vi) De gebruikelijke optelling en vermenigvuldiging van polynomen vormen bewerkingen op de verzameling $\mathbb{R}[x]$ van polynomen met reële coëfficiënten.
- (vii) Als X een verzameling is, dan kun je aan twee *afbeeldingen* f en g van X naar zichzelf een nieuwe afbeelding $g \circ f$ toevoegen, door $(g \circ f)(x) = g(f(x))$. Deze *samenstelling* $g \circ f$ van de afbeeldingen f en g is zelf ook weer een afbeelding $X \rightarrow X$. Dus is $\circ$ een bewerking op de verzameling afbeeldingen van X naar zichzelf, die we wel met X^X aangeven. Als speciaal geval kun je bijvoorbeeld kijken naar alle functies van $\mathbb{R}$ naar $\mathbb{R}$ (maar de samenstelling kan dan op een deelverzameling gedefinieerd zijn).

Definitie 1.3 Een *lichaam* is een verzameling V met daarop twee bewerkingen $+$ en $\times$, die voldoen aan:

- [L1] $+$ op V is associatief: $(x + y) + z = x + (y + z)$, voor alle $x, y, z \in V$;
- [L2] er is een (nul)element $0 \in V$ zodanig dat $0 + x = x + 0 = x$ voor alle $x \in V$;
- [L3] bij elke $x \in V$ is er een *tegengestelde* $-x \in V$ zodanig dat $x + (-x) = (-x) + x = 0$;
- [L4] $+$ op V is commutatief: $x + y = y + x$ voor alle $x, y \in V$;
- [L5] $\times$ op V is associatief: $(x \times y) \times z = x \times (y \times z)$, voor alle $x, y, z \in V$;
- [L6] er is een (eenheids)element $1 \in V$ zodanig dat $1 \times x = x \times 1 = x$ voor alle $x \in V$;
- [L7] bij elke $x \in V$ met $x \neq 0$ is er een *inverse* $x^{-1} \in V$ zodanig dat $x \times x^{-1} = x^{-1} \times x = 1$;
- [L8] $\times$ op V is commutatief: $x \times y = y \times x$ voor alle $x, y \in V$;
- [L9] de operatie $\times$ is *distributief* over $+$, dat wil zeggen: $x \times (y + z) = (x \times y) + (x \times z)$ en $(x + y) \times z = (x \times z) + (y \times z)$, voor alle $x, y, z \in V$.

Opmerkingen 1.4 Een lichaam bestaat dus uit een drietal $(V, +, \times)$, namelijk een verzameling V met twee bewerkingen daarop, dat aan een aantal eisen moet voldoen.

In deze definitie hebben we de bewerkingen met $+$ en $\times$ aangegeven, omdat in voorbeelden die we kennen (zoals de reële getallen) dat natuurlijk is. In de meeste voorbeelden die we zullen zien zullen dit ook inderdaad de twee bewerkingen zijn, maar dit is niet altijd zo.

In een lichaam $(V, +, \times)$ definiëren we de *afrekking* van twee elementen nu door $a - b = a + (-b)$, en de *deling* van a door een element $b \neq 0$ door $a/b = a \times b^{-1}$.

In een lichaam kun je dus elk tweetal elementen optellen en aftrekken, vermenigvuldigen en delen (mits je niet door nul deelt).

Om te laten zien dat een verzameling met daarop twee bewerkingen een lichaam is, kun je verifiëren dat aan alle axioma's is voldaan. Soms is het eenvoudig om het volgende te gebruiken.

Definitie 1.5 Als $(V, +, \times)$ een lichaam is en een deelverzameling $U \subset V$ vormt met *dezelfde bewerkingen* ook een lichaam, dan zeggen we dat $(U, +, \times)$ een *deellichaam* van V is. We zeggen wel dat U een deellichaam is van V (en bedoelen dan: met dezelfde bewerkingen).

Wanneer je weet dat $(V, +, \times)$ een lichaam is, en U is een deelverzameling van V , dan is $(U, +, \times)$ een lichaam als $+$, $\times$ een bewerking vormen op U , als de speciale elementen $0, 1$ uit V ook in U zitten, en als voor elke $u \in U$ tegengestelde en inverse (voor $u \neq 0$) die in V bestaan, ook weer in U zitten. De andere eigenschappen gelden dan voor U omdat ze al voor de grotere verzameling V gelden!

Voorbeelden 1.6 We geven de belangrijkste voorbeelden van lichamen.

- (i) $(\mathbb{R}, +, \times)$: de reële getallen vormen onder optelling en vermenigvuldiging een lichaam. Om dat te bewijzen moet je nagaan dat de eigenschappen L1–9 gelden. De meeste daarvan zijn flauw.
- (ii) $(\mathbb{Q}, +, \times)$: de rationale getallen (breuken) vormen onder optelling en vermenigvuldiging een lichaam.

Hier is het handig om de opmerking over deellichamen te gebruiken: het is duidelijk dat de breuken een deelverzameling van de reële getallen vormen (met $0, 1$ er in) die gesloten is onder het nemen van sommen, producten, tegengestelden, en inversen (van niet-nul elementen)!

- (iii) $(\mathbb{C}, +, \times)$: de complexe getallen vormen onder optelling en vermenigvuldiging een lichaam met $(\mathbb{R}, +, \times)$ als deellichaam.

We definiëren hier de complexe getallen als paren $(a, b) \in \mathbb{R}^2$ van reële getallen die we optellen als vectoren in $\mathbb{R}^2$ en vermenigvuldigen volgens

$$(a, b) \times (c, d) = ((a \times c) - (b \times d), (a \times d) + (b \times c)),$$

gebruik makend van de vermenigvuldiging (en optelling) in $\mathbb{R}$.

Vaak schrijven we $a + bi$ voor (a, b) in $\mathbb{C}$, waarbij dan $i^2 = -1$.

De reële getallen kunnen we dan vereenzelvigen met de deelverzameling van paren $(a, 0)$.

- (iv) De verzameling $V = \{0\}$ met de gewone optelling en vermenigvuldiging vormt een lichaam dat uit maar 1 element bestaat; in het bijzonder is $0 = 1$

in deze ring! Omdat dit speciale geval soms tot complicaties leidt, zullen we het vanaf nu expliciet uitsluiten, en eisen: *de lichamen die wij beschouwen hebben ten minste twee verschillende elementen $0 \neq 1$.*

- (v) De gehele getallen vormen geen lichaam onder optelling en vermenigvuldiging omdat je van $z \in \mathbb{Z}$ geen inverse in $\mathbb{Z}$ kunt vinden, tenzij $z \in \{-1, 1\}$.

Er zijn heel veel belangrijke algebraïsche structuren die bestaan uit een verzameling V , en één of twee operaties die voldoen aan een *deelverzameling* van de axioma's L1–9. Zo is een *groep* een verzameling met een bewerking die voldoet aan L1–3, en een *commutatieve groep* (die meestal *abelse groep* wordt genoemd) voldoet bovendien aan L4. Een *ring met 1* is een verzameling V met operaties $+$ en $\times$ die voldoen aan L1–6 en aan L9; als deze bovendien aan L8 voldoet, is het een *commutatieve ring met 1*. Een lichaam vormt een abelse groep ten opzichte van de optelling $+$, en de elementen die niet nul zijn vormen een abelse groep ten opzichte van de vermenigvuldiging $\times$.

Voorbeeld 1.7 ($\mathbb{Z}/m\mathbb{Z}$) We construeren de commutatieve ring (met 1) $\mathbb{Z}/m\mathbb{Z}$, de *restklassenring modulo m* , als volgt. Laat $m > 1$ een vast natuurlijk getal zijn (de *modulus*). We delen $\mathbb{Z}$ op in restklassen modulo m , namelijk de deelverzamelingen

$$R_i = \{z : z \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : z = i + k \cdot m\}$$

voor $i \in \mathbb{Z}$. Dan is duidelijk dat $R_i = R_j$ wanneer $i - j$ een veelvoud van m is, en dat $R_i \cap R_j = \emptyset$ wanneer $i - j$ geen veelvoud van m is. Dus $R_i = R_j$ of $R_i \cap R_j = \emptyset$. We hebben zo precies m disjuncte restklassen gemaakt, $R_0, R_1, \dots, R_{m-1}$. Vaak geven we de restklasse R_i , waar i zelf in zit, aan met $\bar{i}$. Als i en j in dezelfde restklasse zitten, schrijven we $i \equiv j \pmod{m}$, en zeggen dat i *congruent j modulo m* is. Dus

$$i \equiv j \pmod{m} \iff R_i = R_j \iff \bar{i} = \bar{j} \iff m \mid i - j.$$

We definiëren optelling en vermenigvuldiging van $\bar{i}$ en $\bar{j}$ door $\bar{i} + \bar{j} = \overline{i + j}$ en $\bar{i} \times \bar{j} = \overline{i \times j}$.

Nu is $\mathbb{Z}/m\mathbb{Z}$ de verzameling van de m restklassen modulo m met deze optelling en vermenigvuldiging. Niet alle elementen (ongelijk 0) hebben een inverse in $\mathbb{Z}/m\mathbb{Z}$ tenzij m een priemgetal is. Voor een priemgetal p is de ring $\mathbb{Z}/p\mathbb{Z}$ wel een lichaam dat uit precies p verschillende elementen bestaat. Zo'n eindig lichaam $\mathbb{Z}/p\mathbb{Z}$ wordt ook wel met $\mathbb{F}_p$ aangegeven.

Later zullen we zien dat voor elke *macht* $q = p^k$ van een priemgetal p er een eindig lichaam $\mathbb{F}_q$ van q elementen bestaat (en voor geen enkel ander natuurlijk getal). Bovendien is er in essentie maar één zo'n lichaam. Let wel op: als $k > 1$ is, dan is $\mathbb{Z}/p^k\mathbb{Z}$ geen lichaam (want de restklasse $\bar{p}$ heeft er bijvoorbeeld geen inverse in). Om een lichaam van p^k elementen te maken moeten we een ingewikkeldere constructie maken.

Huiswerkopgaven I

♠ **Huiswerk I-1.** Veronderstel dat de verzameling R gegeven is met bewerkingen $+$ en $\times$.

- (i) Laat zien dat als $R, +$ aan [L2] voldoet, het element 0 uniek is.
- (ii) Laat zien dat als $R, +, \times$ een lichaam vormt (die niet noodzakelijk commutatief is), er geldt dat $0 \times r = r \times 0 = 0$, dat $-1 \times r = r \times -1 = -r$, en dat $r \times (-s) = (-r) \times s = -(r \times s)$ voor alle $r, s \in R$. Houd in elke stap bij welke eigenschap je gebruikt!

♠ **Huiswerk I-2.** Laat V een verzameling zijn met daarop een bewerking die we met $\cdot$ aangeven. Veronderstel dat deze bewerking associatief is, dus

$$\forall x, y, z \in V : (x \cdot y) \cdot z = x \cdot (y \cdot z).$$

- (i) Laat zien dat dan ook geldt:

$$\forall x, y, z, a \in V : ((x \cdot y) \cdot z) \cdot a = (x \cdot y) \cdot (z \cdot a).$$

- (ii) Bewijs dat als $\cdot$ ook commutatief is, er geldt:

$$\forall x, y, z \in V : (x \cdot y) \cdot z = y \cdot (z \cdot x).$$

Het is eenvoudig (maar vervelend) om te laten zien dat matrixvermenigvuldiging van 2×2 matrices van rationale getallen een associatieve bewerking is; dus $\times$ is een associatieve bewerking op $M_2(\mathbb{Q})$.

- (iii) Laat door een tegenvoorbeeld zien dat $\times$ geen commutatieve bewerking is op $M_2(\mathbb{Q})$.
- (iv) Laat zien dat voor een verzameling met een associatieve bewerking *niet* altijd geldt:

$$\forall x, y, z \in V : (x \cdot y) \cdot z = y \cdot (z \cdot x).$$

♠ **Huiswerk I-3.** Laat E een eindige, niet-lege verzameling zijn. Laat $P(E)$ de *machtsverzameling* van E zijn, dat is de verzameling waarvan de elementen de *deelverzamelingen* van E zijn.

- (i) Voor elk tweetal deelverzamelingen A, B van E definiëren we

$$A + B = (A \cup B) \setminus (A \cap B);$$

dus $A + B$ bestaat uit elementen van E die wel in de vereniging maar niet in de doorsnede van A en B zitten. Laat zien dat dit een bewerking op $P(E)$ geeft.

- (ii) Laat zien dat deze bewerking $+$ op $P(E)$ commutatief is.
- (iii) Laat zien dat er een element 0 van $P(E)$ bestaat zodat $A + 0 = A$.
- (iv) Laat zien dat bij elke A in $P(E)$ een A^{-1} bestaat zodat $A + A^{-1} = 0$, met de 0 uit (iii).
- (v) Maak twee plaatjes van drie elkaar snijdende cirkels die drie deelverzamelingen A, B, C van E voorstellen. Elementen van A liggen dan binnen de eerste cirkel, van $A \cap B$ in het stuk waar A en B overlappen, enz. Geef door arcering in het eerste plaatje aan waar $(A + B) + C$ zit, en in het tweede waar $A + (B + C)$. Is $+$ associatief op $P(E)$?

♠ **Huiswerk I-4.** Maak een opteltabel en een vermenigvuldigingstabel voor $\mathbb{Z}/7\mathbb{Z}$, en leg uit hoe je aan deze tabellen de eigenschappen L2, L3, L4, L6, L7 en L8 afleest.