

Eindige lichamen

1. Karakteristiek van een lichaam

Definitie: Zij $\mathbb{F}$ een lichaam met eenheidselement 1. Als er een natuurlijk getal n bestaat met $\underbrace{1 + 1 + \dots + 1}_n = 0$, dan heet de kleinste $p \in \mathbb{N}$ met deze eigenschap de *karakteristiek* van $\mathbb{F}$.

Als zo'n n niet bestaat, heet $\mathbb{F}$ een lichaam van *karakteristiek* 0.

De lichamen der reële, complexe of rationale getallen zijn lichamen van karakteristiek 0, want in deze lichamen zijn de elementen $n \cdot 1$ voor $n \in \mathbb{N}$ alle verschillend. Dit zijn namelijk juist de natuurlijke getallen, en deze vormen een deelverzameling van $\mathbb{R}$, $\mathbb{C}$ en $\mathbb{Q}$.

Omgekeerd bevat in een lichaam met karakteristiek $p \neq 0$ de verzameling $\{n \cdot 1 \mid n \in \mathbb{N}\}$ juist p elementen, want $p \cdot 1 = 0$, $(p+1) \cdot 1 = 1$, $\dots$, $(2p-1) \cdot 1 = p-1$, $2p \cdot 1 = 0$, $(2p+1) \cdot 1 = 1$ enz.

Voordat we nagaan hoe lichamen met karakteristiek $p \neq 0$ er uit zien, laten we even zien dat het symbool p voor de karakteristiek terecht gekozen is omdat de karakteristiek een priemgetal moet zijn.

Lemma: Zij $\mathbb{F}$ een lichaam met karakteristiek $p \neq 0$. Dan is p een priemgetal.

Bewijs: Stel dat p geen priemgetal is, dan zijn er $a, b > 1$ met $p = a \cdot b$ (het geval $p = 1$ kan niet omdat in een lichaam $1 \neq 0$ moet zijn). Nu geldt $p \cdot 1 = (a \cdot 1)(b \cdot 1) = 0$. Stel dat $a \cdot 1 \neq 0$. Dan is $a \cdot 1$ een inverseerbaar element in $\mathbb{F}$ en er geldt $b \cdot 1 = (a \cdot 1)^{-1}(a \cdot 1)(b \cdot 1) = (a \cdot 1)^{-1} \cdot 0 = 0$. Net zo volgt uit $b \cdot 1 \neq 0$ dat $a \cdot 1 = 0$ moet zijn. Dus is een van $a \cdot 1$ en $b \cdot 1$ gelijk aan 0, in tegenspraak met de minimaliteit van p . $\square$

2. Lichamen met p elementen

Het is duidelijk dat een lichaam van karakteristiek p minstens p elementen bevat, namelijk de elementen $\{n \cdot 1 \mid n = 0, 1, 2, \dots, p-1\}$. We zullen nu nagaan dat deze elementen met de goede definitie van de optelling en vermenigvuldiging inderdaad al een lichaam vormen.

Voorbeelden:

- Voor $p = 2$ definiëren we optelling en vermenigvuldiging van de elementen 0 en 1 door:

$$0+0=0, \quad 0+1=1+0=1, \quad 1+1=0, \quad 0 \cdot 0=0 \cdot 1=1 \cdot 0=0, \quad 1 \cdot 1=1.$$

- Voor $p = 3$ geven we tabellen voor de optelling en vermenigvuldiging aan:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Om aan de hand van deze definities na te gaan dat de optelling en vermenigvuldiging associatief zijn en de vermenigvuldiging distributief over de optelling, zou men in principe alle waarden moeten invullen, dit zijn (omdat er drie getallen bij voorkomen) liefst p^3 mogelijkheden. Bij $p = 2$ kan dat nog, bij $p = 3$ is het al niet meer leuk en voor $p = 5$ zou niemand dit meer vrijwillig doen.

Het is daarom een voor de hand liggende vraag of er niet een makkelijkere manier is, om in te zien dat er lichamen met p elementen bestaan. Zo'n manier bestaat inderdaad, de sleutel hiervoor is het *delen met rest*.

2.1 Delen met rest

Definitie: Zij $n \in \mathbb{N}$ een natuurlijk getal en $x \in \mathbb{Z}$ een willekeurig geheel getal. Dan laat x zich eenduidig schrijven in de vorm

$$x = a + n \cdot b \text{ met } a \in \{0, 1, 2, \dots, n-1\} \text{ en } b \in \mathbb{Z}.$$

Het getal a heet de *rest van x bij delen door n* .

De naam geeft al aan hoe we a en b vinden, namelijk door voor b het gehele deel van de breuk $\frac{x}{n}$ te nemen, preciezer gezegd het grootste gehele getal $\leq \frac{x}{n}$. Dan is a de rest die overblijft.

Merk op dat dit ook bij negatieve getallen werkt, bijvoorbeeld is b voor $x = -11$ en $n = 5$ het grootste getal ≤ -2.2 , dus -3 en a in dit geval dus 4 .

Notatie: Zij van nu af n een vast gekozen natuurlijk getal. Dan noteren we de rest van $x \in \mathbb{Z}$ bij delen door n met $\overline{x}$.

Voorbeeld: Voor $n = 7$ is $\overline{2} = 2$, $\overline{-1} = 6$, $\overline{37} = 2$ en $\overline{4711} = 0$.

Het volgende lemma geeft aan wanneer twee getallen dezelfde rest bij delen door n geven. Voor $n = 5$ is dit bijvoorbeeld het geval voor de getallen $\dots, -8, -3, 2, 7, 12, 17, 22, \dots$ die alle rest 2 geven.

Lemma: Twee getallen x en y hebben dezelfde rest bij delen door n d.e.s.d.a. het verschil $x - y$ een veelvoud van n is.,

Bewijs: Stel dat x en y dezelfde rest bij delen door n hebben, dan is $x = a + n \cdot b$ en $y = a + n \cdot d$ en dus $x - y = n(b - d)$.

Zij omgekeerd $x - y$ een veelvoud van n , dan is $y = x + n \cdot d$. Voor $x = a + n \cdot b$ is dan $y = a + n(b + d)$ en dus heeft y dezelfde rest als x , namelijk a . $\square$

We definiëren nu de optelling en vermenigvuldiging voor de resten bij delen door n als volgt:

Definitie: Voor $a, b \in \{0, 1, 2, \dots, n-1\}$ zij

$$a + b := \overline{a + b}, \quad a \cdot b := \overline{ab},$$

d.w.z. we tellen de resten bij elkaar op en delen het resultaat weer met rest door n , net zo voor het vermenigvuldigen.

Voorbeelden:

- (i) Zij $n = 10$. Dan is volgens deze definitie $7 + 8 = \overline{15} = 5$ en $7 \cdot 8 = \overline{56} = 6$. In dit geval *vergeten* we gewoon van het resultaat alles behalve het laatste cijfer (omdat we in het tientallige stelsel werken).
- (ii) Zij $n = 11$. Dan is volgens deze definitie $7 + 8 = \overline{15} = 4$ (omdat $15 = 4 + 11$) en $7 \cdot 8 = \overline{56} = 1$ (omdat $56 = 1 + 5 \cdot 11$).

Ga na dat de tabellen die we boven voor lichamen met 2 en 3 elementen hebben gezien juist op deze manier aangemaakt zijn.

2.2 Erfenis van de gehele getallen

Tot nog toe hebben we geen voortgang geboekt, want om associativiteit of distributiviteit aan te tonen, zouden we nog steeds door de waarden heen moeten lopen. Echter, met behulp van het net bewezen lemma kunnen we zien dat we optellen en vermenigvuldigen met het delen met rest mogen verruilen.

Stelling: Voor $x, y \in \mathbb{Z}$ geldt

$$\overline{\overline{x} + \overline{y}} = \overline{x + y} \quad \text{en} \quad \overline{\overline{x} \cdot \overline{y}} = \overline{x \cdot y}$$

d.w.z. $x + y$ geeft bij delen door n dezelfde rest als $\overline{x} + \overline{y}$ en xy geeft bij delen door n dezelfde rest als $\overline{x} \cdot \overline{y}$.

Bewijs: Zij $\overline{x} = a$ en $\overline{y} = c$, d.w.z. $x = a + n \cdot b$ en $y = c + n \cdot d$ voor zekere $b, d \in \mathbb{Z}$. Dan is $x + y = a + c + n(b + d) = \overline{x} + \overline{y} + n(b + d)$, dus verschillen $x + y$ en $\overline{x} + \overline{y}$ alleen maar om een veelvoud van n en hebben dus dezelfde rest bij delen door n .

Verder is $x \cdot y = ac + n(ad + bc) + n^2bd = \overline{x} \cdot \overline{y} + n(ad + bc + nbd)$ en dus verschillen ook xy en $\overline{x} \cdot \overline{y}$ alleen maar om een veelvoud van n . $\square$

Het nut van deze stelling is opmerkelijk: Als we met de resten willen rekenen, kunnen we al het rekenwerk met gewone gehele getallen uitvoeren en pas als laatste stap met rest door n delen. Dit betekent dat alle rekenregels die voor de gehele getallen gelden automatisch ook voor het rekenen met de resten gelden.

Merk op: Omdat we voor $n \geq 2$ de elementen $0 \neq 1$ in de resten bij delen door n terug vinden, voldoet de verzameling $\{0, 1, 2, \dots, n-1\}$ met de boven gedefinieerde bewerkingen rechtstreeks aan de axioma's 1 t/m 7 en 9 van een lichaam.

Het enige wat we nog moeten aantonen, is het bestaan van een multiplicatieve inverse voor iedere $a \neq 0$. Dit geldt echter niet voor ieder natuurlijk getal n , maar alleen maar voor priemgetallen p .

Lemma: Als n geen priemgetal is en a is een echte deler van n (d.w.z. $n = ab$ met $a \neq 1$ en $b \neq 1$), dan heeft a geen multiplicatieve inverse (bij het rekenen met resten bij delen door n).

Bewijs: Stel dat c de multiplicatieve inverse van a is, dan is $\overline{ac} = 1$ en dus $ac = 1 + n \cdot d$. Dan is $1 = ac - nd = ac - abd = a(c - bd)$ en dit kan niet omdat $a > 1$ en a, b, c, d gehele getallen zijn. $\square$

Voorbeeld: Zij $n = 6$, dan heeft 2 geen multiplicatieve inverse. Er geldt namelijk $2 \cdot 0 = 0$, $2 \cdot 1 = 2$, $2 \cdot 2 = 4$, $2 \cdot 3 = 0$, $2 \cdot 4 = 2$, $2 \cdot 5 = 4$. Men ziet duidelijk dat alle producten door 2 deelbaar zijn en dus i.h.b. nooit 1 kunnen zijn.

Stelling: Zij p een priemgetal. Dan heeft iedere rest $\neq 0$ bij delen door p een multiplicatieve inverse.

Bewijs: Zij $a \in \{1, 2, \dots, p-1\}$. Dan geldt natuurlijk dat de grootste gemene deler van a en p gelijk aan 1 is, want p heeft alleen maar de delers 1 en p , en p kan geen deler van a zijn. Er zijn nu twee mogelijkheden om het bewijs te voltooien:

- (i) Als de lezer bekend is met het uitgebreide algoritme van Euclides dan volgt hieruit meteen de bewering. Volgens Euclides bestaan er namelijk getallen c en d zo dat $1 = ac + pd$, en dan is $\overline{ac} = 1$, dus is c de multiplicatieve inverse van a .
- (ii) Zonder gebruik te maken van het algoritme van Euclides werkt de volgende redenering: We bekijken de verzameling $\{\overline{am} \mid m = 0, 1, \dots, p-1\}$ en laten zien dat deze verzameling p elementen bevat, d.w.z. alle resten bij het delen door p . Als dit niet zo was, waren er twee getallen m en k met $\overline{am} = \overline{ak}$. Maar dan is $\overline{am} - \overline{ak} = \overline{a(m-k)} = 0$ en dus is p een deler van $a(m-k)$. Maar p is geen deler van a , dus moet p een deler van $m-k$ zijn, en dit kan alleen maar voor $m = k$.

Omdat $\{\overline{am} \mid m = 0, 1, \dots, p-1\}$ alle resten bij het delen door p bevat, bevat de verzameling i.h.b. de rest 1, dus geldt voor een $m \in \{0, 1, \dots, p-1\}$ dat $\overline{am} = 1$ en dit is de multiplicatieve inverse van a . $\square$

Voorbeeld: Voor $p = 7$ en $a = 3$ is $3 \cdot 0 = 0$, $3 \cdot 1 = 3$, $3 \cdot 2 = 6$, $3 \cdot 3 = 2$, $3 \cdot 4 = 5$, $3 \cdot 5 = 1$ en $3 \cdot 6 = 4$. De producten van 3 met 0 t/m 6 doorlopen dus inderdaad alle waarden van 0 t/m 6 en 5 is de multiplicatieve inverse van 3, omdat hier het product 1 optreedt.

Gevolg/Definitie: Zij p een priemgetal en $\mathbb{F}_p := \{0, 1, \dots, p-1\}$ de verzameling van de resten bij delen door p . Voor $x \in \mathbb{Z}$ zij $\overline{x}$ de rest van x bij delen door p . Dan is $\mathbb{F}_p$ met optelling en vermenigvuldiging gedefinieerd door

$$a + b := \overline{a + b}, \quad a \cdot b := \overline{ab}$$

een lichaam met p elementen.

Opmerking: Er zijn ook eindige lichamen die niet gelijk zijn aan $\mathbb{F}_p$ voor een priemgetal p . Maar ieder eindig lichaam $\mathbb{F}$ van karakteristiek p laat zich opvatten als vectorruimte over $\mathbb{F}_p$ en de elementen van $\mathbb{F}$ laten zich identificeren met elementen van $\mathbb{F}_p^n$, dus met n -tupels van getallen uit $\mathbb{F}_p$.

Er zijn zelfs oneindige lichamen met karakteristiek p , maar die laten we hier helemaal buiten beschouwing.