

# Discrete Wiskunde

Bert De Saffel

2017-2018

# Inhoudsopgave

<b>I</b>	<b>Discrete Wiskunde</b>	<b>1</b>
<b>1</b>	<b>Eindige Velden</b>	<b>2</b>
1.1	Proloog . . . . .	2
1.2	Priemvelden . . . . .	4
1.2.1	Priemontbinding . . . . .	5
1.2.2	Algoritme van Euclides . . . . .	5
<b>2</b>	<b>Groepen</b>	<b>6</b>

## **Samenvatting**

Deze tekst vat de theorie van Discrete Wiskunde samen zoals die gegeven werd in het academiejaar 2017-2018.

# Deel I

## Discrete Wiskunde

# Hoofdstuk 1

## Eindige Velden

### 1.1 Proloog

*\_TODO: veel korter schrijven* Vooraleer velden kunnen uitgelegd worden moet er eerst een klein stukje van hoofdstuk 2 (Groepen). Een groep (symbool =  $G$ ) is een verzameling elementen waarvan elk element onderling met elkaar kan werken. Een groepstabel specificeert hoe een bepaalde interactie gebeurt. Een voorbeeld hiervan is het optellen van getallen.

Ter opmerking, het symbool  $\oplus$  stelt het additieve voor en  $\otimes$  stelt het multiplicatieve voor. Dit is een hulpmiddel voor ons zodat we kunnen vergelijken met de  $+$  en  $\cdot$  operator uit de wiskunde. Er zijn 4 eigenschappen nodig om een geldige groepstabel te hebben.

- **Inwendigheid:**  $x \oplus y = \text{element van } G$
- **Associativiteit:**  $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
- **Neutraal Element ( $n$ ):**  $x \oplus n = x$
- **Invers element:**  $x \oplus \bar{x} = n$

Een extra, maar niet verplichte eigenschap is **Commutativiteit**.  $x \oplus y = y \oplus x$ . Een groepentabel is een matrix dat interacties visueel voorstelt. In tabel 1.1 zie je dat 2 en 1, 3 oplevert. De 2 wordt afgelezen op de bovenste rij, en de 1 wordt afgelezen op de linkse kolom.

Enkele begrippen met betrekking tot groepstabel.

Tabel 1.1: Een groepstabel voor de interactie ‘optellen’ in modulo 12

+	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

- **Latijns Vierkant:** Een groepstabel waarvan elk element exact één keer voorkomt in elke rij en kolom (denk aan Sudoku).
- **Isomorfe groepen:** Verschillende groepen die niets met elkaar te maken hebben kunnen isomorf zijn. Dit betekent dat ze identiek zijn na eventuele herlabeling of permutaties van kolommen of rijen.
- **Discrete groepen:** Dit zijn groepen met een eindig aantal elementen. Modulo 12 heeft zo 12 elementen.
- **De orde:** Enerzijds is dit getal het aantal elementen van een groep. Anderzijds is dit het aantal keer dat je een element met zichzelf moet laten interageren om het neutraal element te bekomen. De orde is dus voor elk element verschillend.

Als je de verzameling ‘Modulo 12’ bekijkt heb je 12 elementen. 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 en 11.

- Hoeveel keer moet je 1 met zichzelf optellen om 0 te bekomen? (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 0)  $\rightarrow$  12
- Hoeveel keer moet je 2 met zichzelf optellen om 0 te bekomen? (2, 4, 6, 8, 10, 0)  $\rightarrow$  6

- Hoeveel keer moet je 5 met zichzelf optellen om 0 te bekomen?  $(5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7, 0) \rightarrow 12$

De orde van 1 is dus 12, die van 2 is 6 en die van 5 is ook 12.

Een generator is een element of een combinatie van elementen die, als je die met elkaar laat interageren, alle andere elementen van de groep tegenkomt. In de vorige voorbeelden kan je zien dat zowel 1 als 5 een generator zijn aangezien ze elk element tegenkomen. Je kan ook elementen combineren om een generator te vormen. Zo is  $\langle 2, 3 \rangle$  ook een generator want  $(2 + 2 + 3 + 3 + 3 + 3) \bmod 12 = 1$ . 1 is een generator.

Tot nu toe hebben we enkel additieve groeptabellen gezien. In tabel 1.1 kan je zien dat de groep Modulo 12 voor de bewerking  $\oplus$  een discrete groep is

## 1.2 Priemvelden

Priemvelden is een eerste methode om een cyclische groep te vinden van een bepaalde orde.

- **Veld**: Verzameling  $F$  van elementen  $\{a, b, c, \dots\}$  die onderling interageren via een interactie  $\oplus$  en via een interactie  $\otimes$ .
- **Veldaxioma's**
  1.  $(F, \oplus) \rightarrow$  Een additieve groep met neutraal element **0** (nulelement)
  2.  $(F \setminus 0, \otimes) \rightarrow$  Multiplicatieve groep met neutraal element **1** (eenheidselement)
  3. Distributieve eigenschap:  $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$
- **Eindig veld**: Veld met eindig aantal element  $n$
- Voor elke orde  $n$  is er maximum één enkel eindig veld met orde  $n$
- De multiplicatieve groep  $(F \setminus 0, \otimes)$  van een eindig veld  $(F, \oplus, \otimes)$  is cyclisch

Hoe kan het veld met orde  $n$  geconstrueerd worden met groepstabellen  $(F, \oplus)$  en  $(F, \otimes)$ ?  $\rightarrow$  Alle eindige velden kunnen met behulp van één van twee methodes geconstrueerd worden.

$(\mathbb{Z}_p, +, \cdot)$  vormt een veld met nulelement **0** en eenheidselement **1** op voorwaarde dat  $p$  een priemgetal is. Dit heet een **priemveld**. Hieruit volgt dat  $(\mathbb{Z}_p \setminus 0, \cdot)$  een cyclische groep is indien  $p$  een priemgetal is.

### 1.2.1 Priemontbinding

- **Priemontbinding** → Een geheel getal ontbinden als een product van machten van priemfactoren.  $p_1^{n_1} \cdot p_2^{n_2} \cdot \dots \cdot p_x^{n_x}$ . Dit is uniek voor elk getal.

### 1.2.2 Algoritme van Euclides

- Numerieke uitwerking van het **algoritme van Euclides**:

99		
-84	1 (1 keer in 99 = 1 * 84)	84
15	5 (5 keer in 84 = 5 * 15)	-75
-9	1 (1 keer in 15 = 1 * 9)	9
6	1 (1 keer in 9 = 1 * 6)	-6
-6	2	3
0		



## Hoofdstuk 2

### Groepen