Discrete Wiskunde

Bert De Saffel

2017-2018

Inhoudsopgave

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 eerst de inleiding van hoofdstuk 2 (Groepen) gegeven worden.

- **Groep** (symbool = G): Een verzameling elementen die elk met elkaar onderling interageren.
- **Groepstabel**: Een matrix dat interacties voorstelt.

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 . operator uit de wiskunde. Er zijn 4 eigenschappen nodig om een geldige groepstabel te hebben.

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

Een extra, maar niet verplichte eigenschap is **Commutativiteit**. $x \oplus y = y \oplus x$.

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.

- **Generator**: 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 $< 2, 3 >$ ook een generator want $(2 + 2 + 3 + 3 + 3) \mod 12 = 1$.

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

Multiplicatie is geen groepstabel tenzij we de 0 uitsluiten en als de groep n aantal element bevat waarbij n een priemgetal is. Dit wordt duidelijk gemaakt in het onderdeel Priemvelden

Een cyclische groep is een groep dat slechts 1 element heeft als generator.
$i = (29w^i)\%36$
29 = invers element via algemeen algoritme van euclides

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, ...} 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** (**nul**element)
  2. (F\0 , $\otimes$) $\rightarrow$ Multiplicatieve groep met neutraal element **1** (**eenheids**element)
  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\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.

(Z_p, +, .) vormt een veld met nulelement **0** en eenheidselement **1** op voorwaarde dat p een priemgetal is. Dit heet een **priemveld**. Hieruit volgt dat (Z_p\0, .) een cyclische groep is indien p een priemgetal is.

1.2.1 Priemontbinding

_TODO: todo

1.2.2 Algoritme van Euclides

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

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

pi = 3 + 1/(7 + 1/(15))...

1.2.3 Multiplicatieve functies

Euler ϕ

Definitie: Hoeveel getallen kleiner dan x zijn priemgetallen?
Voorbeeld: $90 = 2 * 3^2 * 5$
$\phi(90) = 90 * (1/2) * (2/3) * (4/5) =$ **24**

1.2.4 Möbius μ

Heeft 3 uitkomsten: -1, 0 of 1.

- **0**: Minstens één van de priemfactoren komt meer dan 1 keer voor.
- **-1**: Oneven aantal priemfactoren
- **1**: Even aantal priemfactoren
- $\mu(35) = 1$, want $5 * 7 = evenaantalpriemfactoren$

Möbius Inversie:

- Wordt gebruikt om $\phi(x)$ te berekenen.
- $\phi(x) = \mu(1) * (90/1)$
  $+ \mu(2) * (90/2)$
  $+ \mu(3) * (90/3)$
  $+ \mu(5) * (90/5)$
  $+ \mu(10) * (90/10)$
  $+ \mu(15) * (90/15)$
  $+ \mu(30) * (90/30)$

1.3 Primitieve wortels

Interacties met zichzelf om uiteindelijk 1 uit te komen. Bij de primitieve wortel moet je de *orde* aantal keer interageren met zichzelf om 1 uit te komen
stel $p = 601$ 600 = aantal elementen $600 = 2^3 * 3 * 5^2$
rooster opstellen *_TODO: rooster* $8*3*25 = 600$ is het enige dat als uitkomst 1 mag hebben, zonder computer kan je best enkel de laatste aansluitingen controleren

1.4 Discrete logaritmen

Bepaal index i van het getal x van verzameling p met primitieve wortel w
VB: $p = 401, w = 3, i = 13$

1.4.1 Naïve methode

1.4.2 Baby-step Giant-step

Hoofdstuk 2

Groepen