

- p1: **Abelse groep:** Verzameling G en binaire bewerking $*$ zodat:
 = groep
 gesloten, associatief, eenheidselement, inverse, commutatief
en commutativiteit: maar in deze cursus: Abelse groep = groep
- p4: **Deelgroep** $H \subset G$ ($H \neq \emptyset$):
 $a+b \in H$ voor $a, b \in H$
 $-a \in H$ voor $a \in H$
- p3: **Cyclische groep:** als $G = \langle a \rangle$ voor een $a \in G$, $a =$ primitief element of $\langle a \rangle = \{m_a n_m \mid m, n \in \mathbb{Z}\}$
 ↳ voortgebracht door a
 ↳ de orde van het element a is de orde van de groep $\langle a \rangle$
 ↳ zo gedefinieerd

- n12: **Ringer:**
 $(R, +)$ is een ring indien: - $(R, +)$ is een groep
 + al voldaan want groep
 - gesloten, associatief, distributief
 ↳ ↳ ↳
 → Indien ook commutatief: commutatieve ring
 → Indien er een $1 \in R$ is waarvoor voor alle $a \in R$: $a \cdot 1 = 1 \cdot a = a$
 = Ring met eenheidselement
- ↳ **Deelring:** Deelverzameling S van R
 ↳ S is deelgroep van additieve groep R
 ↳ $\forall a, b \in S, ab \in S$ (S gesloten onder vermenigvuldiging)
 ↳ comm. ring met eenh. element
- ↳ **Ideal:** deelgroep I in de additieve groep R die gesloten is onder de vermenigvuldiging met elementen van R .
 → $\forall a \in I, \forall b \in R : ab \in I$
- ↳ **Hoofdideal:** $R =$ commutatieve ring met eenheidselement en $a \in R$
 $\Rightarrow aR = \{ab, b \in R\} =$ ideal voortgebracht door a
 = hoofdideal van R

Inhoudsopgave

1. Algebraïsche structuren	1
1.1. Abelse groepen	1
1.1.1. Definitie en basiseigenschappen	1
1.1.2. Deelgroepen	4
1.1.3. Congruentie	5
1.1.4. Groepshomomorfismen en -isomorfismen	7
1.1.5. Cyclische groepen	9
1.2. Ringen	12
1.2.1. Definitie en basiseigenschappen	13
1.2.2. Congruentie	15
1.2.3. Ringhomomorfismen en -isomorfismen	16
1.2.4. Nuldelers en inverteerbare elementen	17
1.3. Integriteitsgebieden en velden	18
1.3.1. Definities en eigenschappen	18
1.3.2. Deelvelden, uitbreidingsvelden en de relatie met vectorruimtes	19
1.4. Veeltermringen	20
1.4.1. Definitie en eerste eigenschappen	21
1.4.2. Deling met rest	23
1.4.3. Nulpunten van een veelterm	25
1.4.4. Veeltermringen modulo een hoofdideaal	26
1.5. Besluit	28
1.6. Opgaven bij hoofdstuk 1	28
2. Veeltermen en rationale expressies	33
2.1. Veeltermen over een veld	33
2.1.1. Definitie en fundamentele eigenschap	33
2.1.2. Deelbaarheid en grootste gemene deler	34
2.1.3. Nulpunten en afgeleiden	43
2.2. Rationale expressies	50
2.2.1. Constructie	50
2.2.2. Splitsen in partieelbreuken	54

2.2.3. Rationale expressies met reële of complexe coëfficiënten	60
2.3. Besluit	64
2.4. Opgaven bij hoofdstuk 2	64
3. Eindige velden	68
3.1. Basiseigenschappen	68
3.2. Existente en uniciteit	69
3.2.1. Mogelijk aantal elementen van een eindig veld	69
3.2.2. Existente	70
3.2.3. Uniciteit	71
3.2.4. Samenvatting	75
3.3. Constructie	75
3.3.1. Algoritme	75
3.3.2. Voorbeeld: het veld met vier elementen	76
3.4. Eigenschappen van de multiplicatieve groep	77
3.5. Alternatieve representatie	81
3.6. Besluit	83
3.7. Opgaven bij hoofdstuk 3	84
4. Voortbrengende functies	87
4.1. Formele machtreeksen	87
4.1.1. Definitie	88
4.1.2. Afgeleiden van formele machtreeksen	90
4.1.3. Substitutie	92
4.1.4. Enkele belangrijke formele machtreeksen	93
4.1.5. Het binomium van Newton als formele machtreeks	94
4.2. Voortbrengende functies	96
4.2.1. Definitie	96
4.2.2. Eigenschappen	97
4.2.3. Toepassingen: een eerste voorbeeld	100
4.3. Exponentieel voortbrengende functies	101
4.3.1. Definitie	101
4.3.2. Eigenschappen	102
4.3.3. Toepassingen: een eerste voorbeeld	103
4.4. De analytische aanpak	105
4.4.1. Waarom nuttig? Een voorbeeld	105
4.4.2. Convergentie van machtreeksen	106
4.4.3. Conclusie	108

4.5.	Het inversieprobleem	109
4.5.1.	Rationale expressies	110
4.5.2.	Algemene inversieformule	112
4.5.3.	Een benadering via singulariteitsanalyse	114
4.6.	Toepassingen van voortbrengende functies	127
4.6.1.	Oplossen van lineaire recurrente betrekkingen	128
4.6.2.	Volle binaire bomen	129
4.6.3.	Bewijs van formule (3.1)	133
4.6.4.	Surjecties	136
4.7.	Besluit	139
4.8.	Opgaven bij hoofdstuk 4	139
5.	Discrete optimalisatie	149
5.1.	Algemene probleemstelling	149
5.2.	Toewijzingsproblemen	150
5.2.1.	Probleemstelling	150
5.2.2.	Vertaling naar een graaf	152
5.2.3.	Toewijzingsalgoritme	153
5.2.4.	Huwelijksstelling	158
5.3.	Een veralgemeening van het toewijzingsprobleem	160
5.3.1.	Probleemstelling	160
5.3.2.	Het Hongaars algoritme: inleiding	161
5.3.3.	Hoe rijen en kolommen manipuleren?	164
5.3.4.	Het Hongaars algoritme	165
5.4.	Besluit	169
5.5.	Opgaven bij hoofdstuk 5	169
A.	Basisbegrippen uit de grafentheorie	172

Inleiding

De cursus *Discrete Wiskunde II* gaat in op een aantal aspecten uit de discrete wiskunde, die nuttig zijn voor (bachelor)studenten in de ingenieurswetenschappen, en dan vooral voor deze in de richtingen Computerwetenschappen en Elektrotechniek. Deze cursus is daarbij een vervolg op de cursus *Discrete Wiskunde I* gedoceerd in de 1ste bachelor Ingenieurswetenschappen. Het is echter niet strikt nodig, zij het wel nuttig, om deze cursus te hebben gevolgd. Het hoogst noodzakelijke wordt in deze cursus herhaald.

We starten deze cursus met een hoofdstuk over algebraïsche structuren. Een algebraïsche structuur is in essentie een verzameling waarop één of twee bewerkingen kunnen worden gedefinieerd die voldoen aan zekere eigenschappen. Achtereenvolgens behandelen we de structuren groepen, ringen en velden. We voeren voor elk van deze structuren het begrip congruentie in, wat ons in latere hoofdstukken toelaat om nieuwe algebraïsche structuren te construeren. Tenslotte definiëren we veeltermen over ringen wat leidt tot een nieuw soort ringen, zogenaamde veeltermringen.

Een tweede hoofdstuk is gewijd aan deze veeltermen en aan rationale expressies gedefinieerd over een veld. Deze algebraïsche structuren vertonen mooie eigenschappen die in se allemaal volgen uit een basiseigenschap, nl. de deling met rest. We zullen in dit hoofdstuk ondermeer uniciteit van de ontbinding van een veelterm in irreducibele veeltermen en van de splitsing van een rationale expressie in partieelbreuken bewijzen.

In een derde hoofdstuk bestuderen we een specifieke categorie van velden, nl. velden met een eindig aantal elementen. Deze velden worden eindige velden of Galoisvelden genoemd. We zullen bewijzen dat een veld met een gegeven aantal elementen enkel kan bestaan als dat aantal elementen een niet-negatieve gehele macht is van een priemgetal. We zullen ook bewijzen dat er zo steeds een veld bestaat en dat het uniek is (bekijken vanuit een algebraïsch standpunt). We gaan dan kort in op de constructie van een eindig veld met een gespecificeerd aantal elementen. Tenslotte zullen we een alternatieve representatie van eindige velden afleiden die gebaseerd is op logaritmes.

De veeltermen behandeld in het tweede hoofdstuk worden vervolgens in een vierde hoofdstuk uitgebreid naar voortbrengende functies (met reële coëfficiënten). In essentie zijn deze voortbrengende functies niets anders dan veeltermen met een oneindig

aantal termen. We zullen echter zien dat deze voortbrengende functies een volledige machinerie op gang brengen die het ons mogelijk maakt om op elegante manier een oneindige rij getallen te bepalen uit relaties tussen deze getallen (zogenaamde recurrente betrekkingen). Het inversieprobleem waarbij de rij getallen uit haar voortbrengende functie (benaderend) moet worden berekend zal ook behandeld worden. Tenslotte tonen we hoe voortbrengende functies kunnen worden gebruikt in een aantal belangrijke toepassingen.

In een laatste hoofdstuk wordt tenslotte een specifiek discreet optimalisatieprobleem behandeld, nl. het zogenaamde toewijzingsprobleem. We zullen ad-hoc algoritmen opstellen om dit soort optimalisatieproblemen op te lossen. De relatie met grafen (o.a. bipartite grafen) zal tevens duidelijk gemaakt worden.

Discrete Wiskunde II: Examen

Academiejaar 2009-2010, eerste examenperiode

Prof. J. Walraevens, titularis · Prof. H. Bruneel, medelesgever

Woensdag 2 juni 2010, 8u30

1. Stel dat twee gehele getallen A en $-B$ ($A > B \geq 0$) gegeven zijn in 9-complement voorstelling in basis 10 met vier cijfers.

Gevraagd:

- (a) Welke waarden kunnen A en B aannemen zodat A en $-B$ geldig kunnen worden voorgesteld d.m.v. bovenstaande voorstelling?
- (b) Stel dat de voorstellingen van A en $-B$ cijfergewijze worden opgeteld (vanaf rechts, met carry naar links). Hoe kan uit het resultaat de 9-complement voorstelling van $A - B$ worden afgeleid?

2. Gegeven een rationaal getal x met kettingbreukvoorstelling $[a_0; a_1, \dots, a_n]$.

Gevraagd: Wat is de kettingbreukvoorstelling van $1/x$?

3. Gegeven $[i]_2 = \{i + 2k, k \in \mathbb{Z}\}$ en $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$. Definieer de aftrekking van $[a]_2$ en $[b]_2$ ($[a]_2, [b]_2 \in \mathbb{Z}_2$) als

$$[a]_2 - [b]_2 = [a - b]_2.$$

Gevraagd: Is $(\mathbb{Z}_2, -)$ een (Abelse) groep? Verklaar uw antwoord.

4. Gegeven de quotiëntringen $\mathbb{C}[x]/(f_1)$ en $\mathbb{C}[x]/(f_2)$, met \mathbb{C} de verzameling der complexe getallen en f_1 en f_2 irreducibele veeltermen in $\mathbb{C}[x]$.

Gevraagd: $\mathbb{C}[x]/(f_1) \cong \mathbb{C}[x]/(f_2)$. Waar of niet waar? Verklaar uw antwoord.

5. Gegeven het eindig veld F_{16} .

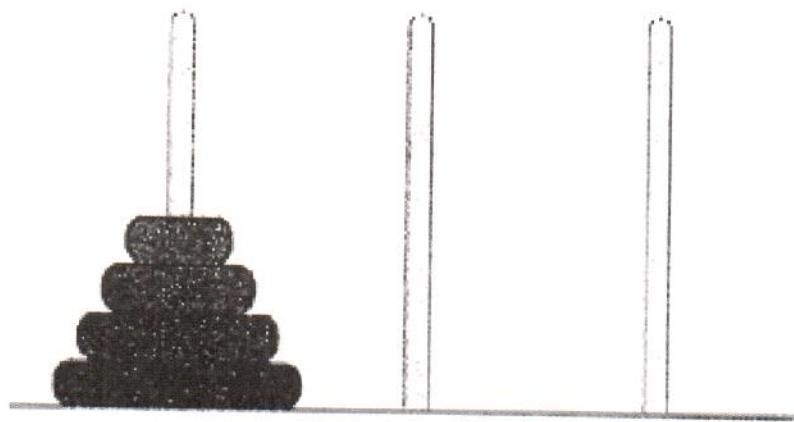
Gevraagd:

- (a) Hoeveel verschillende minimale veeltermen van elementen van F_{16} zijn er?
- (b) Som deze minimale veeltermen op.

6. Gegeven de veeltermen $f = 2x^4 - 4x^3 + 15x^2 - 28x + 7$ en $g = 2x^5 - 4x^4 - 5x^3 + 12x^2 - 3x$ in $\mathbb{R}[x]$.

Gevraagd: $\text{ggd}(f, g)$.

7. Beschouw de welbekende torens van Hanoi. Hierbij zijn i schijven van strikt afnemende grootte (grootste schijf ligt onderaan) gestapeld rond één van drie staven (zie figuur). Bedoeling is om de toren van schijven te 'verplaatsen' naar één van de andere staven in zo weinig mogelijk beurten. In elke beurt wordt vanaf één van de staven de bovenste schijf verplaatst naar één van de andere staven op zo eerst manier dat er nooit een grotere schijf op een kleinere schijf rust.



Noem a_i het totaal aantal beurten dat minimaal nodig is om een toren met i schijven volledig te verplaatsen. We spreken af dat $a_0 = 0$.

Gevraagd:

- Hoeveel zijn a_1 , a_2 en a_3 ?
- Stel een recurrente betrekking (met beginvoorwaarden) op voor de sequentie $\{a_i\}_{i=0}^{\infty}$.
- Bereken de voortbrengende functie f van $\{a_i\}_{i=0}^{\infty}$.
- Bereken de a_i , $i \geq 0$.

8. Stel dat in de uitvoering van het Hongaars algoritme (algoritme 6.3, p. 168-169 in de syllabus) een element $c_{a_i b_j}$ van de kostenmatrix op dat moment (element op de i -de rij, j -de kolom) dubbel bedekt wordt in stap (v)(a).

Gevraagd: Zijn de volgende beweringen waar of niet waar? Verklaar telkens uw antwoord.

- $c_{a_i b_j}$ is noodzakelijkerwijs 0.
- Gesteld dat $c_{a_i b_j} = 0$ is, dan bevat kolom j minstens drie nullen.

Examenvragen Discrete Wiskunde II

Eerste zit 2009-2010

Hey! We proberen hier vragen en antwoorden van examens te verzamelen voor toekomstige generaties in een gezamenlijk document. Dus schrijf je antwoorden/vragen er maar gerust bij en stuur de link door naar medestudenten (hoe meer, hoe beter). Het hoeft niet altijd perfect te zijn, indien er fouten zijn kan iemand anders ze nog altijd verbeteren :).

- Uitleg(op link drukken):
- Voor andere examens (bv: statistiek, analyse 2, meetkunde,...) moedigen wij zeker studenten aan om ook zelf google docs te maken, zie link: Zelf een google doc maken
- Per ongeluk iets te veel gewist? Gebruik ctrl-z of als het niet anders kan File->see revision history. Hij laadt wel zeer traag dus zeker opletten.

Voor andere documenten, check zeker regelmatig :

- Studiehulp v2.0 (beta)

Aantal al gevonden vragen:

Onvolledig/incorrect/onopgelost = headings in het rood.

1) Men stelt de gehele getallen A en $-B$ ($A > B > 0$) voor in een 9-complement voorstelling in basis 10 met 4 cijfers.

Gevraagd:

a) Welke waarden kunnen A en B aannemen zodat A en $-B$ geldig kunnen voorgesteld worden d.m.v. bovenstaande voorstelling?

Het bereik van de voorstelling is: $[-(10^4/2 - 1), 10^4/2 - 1] = [-4999, 4999]$. Uit de extra beperkingen op A en B volgt dan: $A \in [2; 4999]$ en $B \in [1; 4998]$

b) Stel dat de voorstellingen van A en $-B$ cijfergewijze worden opgeteld (vanaf rechts, met carry naar links). Hoe kan uit het resultaat de 9-complement voorstelling van $A - B$ worden afgeleid?

Dit is geval 3 op pag. 13 is de cursus: tel de carry op bij het resultaat (zie schema cursus)

2) Gegeven: De een rationaal getal x met kettingbreukvoorstelling $[a_0; a_1, a_2, \dots, a_n]$.

Gevraagd: Wat is de kettingbreukvoorstelling van $1/x$?

Er zijn 7 gevallen:

$x < -1$: Geen flauw idee (Experimenten brengen geen verduidelijking)

*** aanpassing: een geldige oplossing is $[0; -a_0, -a_1, \dots, -a_n]$ maar volgens definitie 1.20 moeten de a_i ($i \geq 1$) positieve gehele getallen zijn... een alternatieve notatie die dan misschien wel mag is $[-[0; a_0, a_1, \dots, a_n]]$

$x = -1$: De voorstelling blijft gelijk: $[-1]$

$-1 < x < 0$: Ook geen flauw idee

*** aanpassing:zelfde uitleg als voor $x < -1$

$x = 0$: Er is geen kettingbreukvoorstelling van de inverse

$0 < x < 1$: Dan is de oude $a_0 = 0$. Dus kunnen we de kettingbreukvoorstelling inverteren, zodat we krijgen: $[a_1; a_2, a_3, \dots, a_n]$

$x = 1$: De voorstelling blijft gelijk: $[1]$

$x > 1$: Dan is de nieuwe $a_0 = 0$, dus kunnen we alweer inverteren: $[0; a_0, a_1, \dots, a_n]$

3) Gegeven: $[i]_2 : \{i + 2k; k \in \mathbb{Z}\}$ en $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$. Definieer de aftrekking van $[a]_2$ en $[b]_2$ ($[a]_2, [b]_2 \in \mathbb{Z}_2$) als:

$$[a]_2 - [b]_2 = [a - b]_2$$

Gevraagd: Is de groep $(\mathbb{Z}_2, -)$ een (Abelse) groep?

Ja, dit kan nagegaan worden adhv. de groep eigenschappen aan het begin van H2. De commutativiteit, geslotenheid, inverteerbaarheid en het bestaan van het eenheidselement kunnen via de Cayley-tabel geverifieerd worden. Om de associativiteit te controleren moet voor alle mogelijke a , b en c nagegaan worden of $a - (b - c) = (a - b) - c$.

Kennelijk is overigens \mathbb{Z}_2 de enige \mathbb{Z}_n waarvoor dit geldt: dit kan als volgt worden ingezien: als $(\mathbb{Z}_n, -)$ een groep is, geldt wegens associativiteit en eigenschap 2.2 (iii en iv):

$a - (b - c) = a - b + c = (a - b) - c = a - b - c$, zodat $c = -c$, wat inderdaad alleen het geval

is in \mathbb{Z}_2 .

4) Gegeven de quotiëntringen $\mathbb{C}[x]/(f_1)$ en $\mathbb{C}[x]/(f_2)$, met \mathbb{C} de verzameling der complexe getallen en f_1 en f_2 irreducibele veeltermen in $\mathbb{C}[x]$.

Gevraagd: $\mathbb{C}[x]/(f_1) \approx \mathbb{C}[x]/(f_2)$. Waar of niet waar? Verklaar uw antwoord.

Waar. Wegens eigenschap 4.14 is elke veelterm over $\mathbb{C}[x]$ lineair, zodat wegens de opmerking op p. 70 (tussen definitie 2.30 en voorbeeld 2.15) zowel $\mathbb{C}[x]/(f_1)$ als $\mathbb{C}[x]/(f_2)$ isomorf is met $\mathbb{C}[x]$. Aangezien f_1 en f_2 beide isomorf zijn met $\mathbb{C}[x]$, zijn ze ook isomorf met elkaar.

5) Beschouw het veld F_{16} .

a) Hoeveel verschillende minimale veeltermen van elementen van F_{16} zijn er?

Uit de theorie: elke irreducibele veelterm met graad een deler van n is ook een minimale veelterm. Rest nog het berekenen van het aantal veeltermen van graad een deler van n. Volgens formule 3.1 is:

$$1D_1 = 2 \Leftrightarrow D_1 = 2$$

$$2D_2 + 1D_1 = 4 \Leftrightarrow D_2 = 1$$

$$4D_4 + 2D_2 + 1D_1 = 16 \Leftrightarrow D_4 = 3$$

Er zijn dus 6 minimale veeltermen in F_{16} .

b) Som deze minimale veeltermen op.

$$D1 = \{x, x+1\}$$

$$D2 = \{x^2 + x + 1\}$$

$$D4 = \{x^4 + x + 1, x^4 + x^3 + x^2 + x + 1, x^4 + x^3 + 1\}$$

6) Gegeven de veeltermen $f = 2x^4 - 4x^3 + 15x^2 - 28x + 7$ en $g = 2x^5 - 4x^4 - 5x^3 + 12x^2 - 3x$ in $\mathbb{R}[x]$.

Gevraagd: $ggd(f, g)$

We volgen algoritme 4.1 uit de cursus:

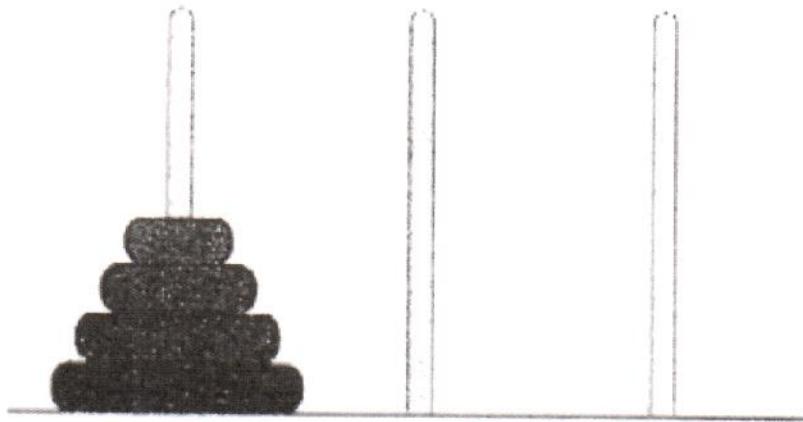
$$2x^5 - 4x^4 - 5x^3 + 12x^2 - 3x = (2x^4 - 4x^3 + 15x^2 - 28x + 7)x + (-20x^3 + 40x^2 - 10x)$$

$$2x^4 - 4x^3 + 15x^2 - 28x + 7 = (-20x^3 + 40x^2 - 10x) \quad (-x/10) + (14x^2 - 28x + 7)$$

$$(-20x^3 + 40x^2 - 10x) \quad = (14x^2 - 28x + 7) \quad (-7x/10) + 0$$

Dus is $ggd(f, g) = x^2 - 2x + 1/2$

7) Beschouw de welbekende torens van Hanoi. Hierbij zijn i schijven van strikt afnemende grootte (grootste schijf ligt onderaan) gestapeld rond één van drie staven (zie figuur). Bedoeling is om de toren van schijven te 'verplaatsen' naar één van de andere staven in zo weinig mogelijk beurten. In elke beurt wordt vanaf één van de staven de bovenste schijf verplaatst naar één van de andere staven op zo een manier dat er nooit een grotere schijf op een kleinere schijf rust.



Noem a_i het totaal aantal beurten dat nodig is om een toren met i schijven volledig te verplaatsen. We spreken af dat $a_0 = 0$.

Gevraagd:

a) Hoeveel zijn a_1 , a_2 en a_3 ?

$$a_1 = 1, \quad a_2 = 3 \quad \text{en} \quad a_3 = 7$$

b) Stel een recurrente betrekking (met beginvoorwaarden) op voor de sequentie $\{a_i\}_{i=0}^{+\infty}$.

$$a_{i+1} = 2a_i + 1 \quad \text{met} \quad a_0 = 0$$

c) Bepaal de voortbrengende functie f van $\{a_i\}_{i=0}^{+\infty}$

Sommeren van beide leden van 1 tot $+\infty$ en vermenigvuldigen met x^i levert:

$$f/x - a_0 = 2f + 1/(1-x), \quad \text{zodat:}$$

$$f = \frac{x}{(1-x)(1-2x)} = \frac{1}{1-2x} - \frac{1}{1-x} = \sum_{i=0}^{+\infty} (2x)^i - \sum_{i=0}^{+\infty} x^i = \sum_{i=0}^{+\infty} (2^i - 1) x^i$$

d) Bereken de a_i , $i \geq 0$

$$a_i = 2^i - 1 \quad (\text{Dit kan bewezen worden via inductie of via bovenstaande inversie.})$$

Het bewijs kon ook via een boom die zich op elk niveau in twee splitste en vervolgens tellen we

$$\text{de kosten op per niveau: } \sum_{k=0}^{n-1} 2^k = 2^n - 1$$

→ Zie tekening onderaan dit kan maar niet noodzakelijk... → geeft gewoon setren
takken

- 8) Stel dat in de uitvoering van het Hongaars algoritme (algoritme 6.3, p 168-169 in de syllabus) een element $c_{a,b}$, de kost van de kostenmatrix op dat moment (element op de i -de rij, j -de kolom) dubbel bedekt wordt in stap (v) (a).

Gevraagd: Zijn volgende beweringen waar of niet waar? Verklaar telkens uw antwoord.

- a) $c_{a,b}$ is noodzakelijkerwijs nul.

Vals, zie p. 195 2-de rij, rechts: 5 is dubbel bedekt. Als een element dubbel bedekt is, staan er minstens twee nullen in de kolom van dit element en één nul in de rij van dit element. Dit zegt echter niets over dit element zelf.

- b) Gesteld dat $c_{a,b} = 0$ is, dan bevat de kolom j minstens drie nullen.

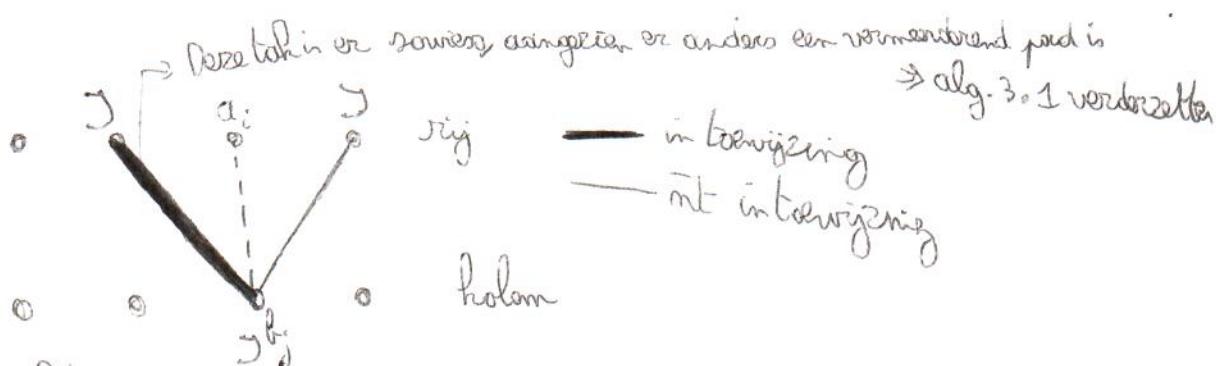
Waar. Bewijs:

Onderstel dat de maximale toekenning $c_{a,b}$ bevat. In dat geval zal, nadat b_j de markering J gekregen heeft in stap (iii) van algoritme 6.3, a_i de markering J krijgen in stap (v) van algoritme 6.3, wat betekent dat de i -de rij in stap (v) (a) van algoritme 6.3, niet bedekt kan worden, zodat $c_{a,b}$ niet dubbel bedekt kan zijn. De optimale toekenning bevat dus niet $c_{a,b}$.

Aangezien b_j in stap (iii) van algoritme 6.1 met J is gemaakteerd, moet b_j via een tak die niet tot de maximale toekenning behoort met een knoop verbonden zijn die met J gemaakteerd is. Deze knoop kan niet a_i zijn, aangezien dan, zoals reeds gezegd, de i -de rij niet bedekt kan worden. b_j is dus zeker met twee knopen verbonden via takken die niet tot de maximale toekenning behoren.

Als in b_j geen tak uit de maximale toewijzing toekomt, volgt uit stap (iv) van algoritme 6.1 dat er een vermeerderend pad gevonden is en en de toewijzing dus niet maximaal is. Dus komt er in b_j een tak toe uit de maximale toewijzing.

Aangezien de andere twee takken die in b_j toekwamen niet tot de maximale toewijzing behoorden, komen er dus minstens 3 takken toe in b_j en is b_j dus minstens met drie verschillende elementen verbonden. Dit manifesteert zich in de kostenmatrix als een kolom met drie nullen.



(a,b) dubbelbedekt en 0, wat is dan nog 0?

↳ i-de rij = bedekt \Rightarrow markering moet zeker N zijn \rightarrow dan rij bedekt

\Rightarrow in bovenstaande tekening moet ook connectie zijn met a_i , zonder dat deze "gebruikt" wordt en markering J heeft: ---
 \Rightarrow 3 takken vanuit $b_j \Rightarrow$ 3 nullen in kolom

Discrete wiskunde II - Examen 2011-2012

Uit VTK Wiki

Examenvragen van Discrete wiskunde II.

Bestanden

Deze pagina heeft nog geen bestanden.

[Bestand kiezen](#) [Geen bestand gekozen](#) [Bestand anoniem uploaden](#)

Examen van 6 juli

1. Eerste vraag

gehalvinduleren niet gezien

Waar/vals + bewijs: als getal deelbaar door 3, dan som cijfers deelbaar door 3 (dit in alle basissen)

Ontvangen van "https://vtk.ugent.be/wiki/Discrete_wiskunde_II_-_Examen_2011-2012"

- Deze pagina is het laatst bewerkt op 6 jul 2012 om 18:14.
- Over VTK Wiki
- //
- studiehulp@vtk.ugent.be

Examen 2010

①/②: Niet gezien

③ Abelse groep wanneer aan volgende eigenschappen voldaan:

1) gesloten onder bewerking

2) associatief

3) eenheidselement

4) inverse

5) commutatief

\hookrightarrow in \mathbb{Z}_2 , dus enkel $[0]_2$ en $[1]_2$

-	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[-1]_2 = [1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

\hookrightarrow Altijd "linkse-bovenste":

$$\begin{array}{c|cc} - & c & d \\ \hline a & a-c & a-d \\ b & b-c & d-b \end{array}$$



\rightarrow Uit Cayleigh-tabel besluiten we: $[0]_2$ is het eenheidselement $\bullet [1]_2 = [1]_2$

+ Associatief:

$$0 - (1 - 1) = 0 - 0 = 0 = (0 - 1) - 1 \stackrel{-1=1}{=} 1 - 1 = 0$$

$$1 - (1 - 1) = 1 - 0 = 1 = (1 - 1) - 1 = 0 - 1 = \stackrel{1}{-1}$$

$$1 - 0 - 0 = (1 - 0) - 0 = 1$$

...

$$\hookrightarrow [1]_2 - [0]_2 = [1]_2 = [0]_2 - [1]_2$$

$$[0]_2 - [0]_2 = [0]_2 = [0]_2 - [0]_2$$

+ Elk element heeft inverse:

$$a - a' = e = a' - a$$

$$[0]_2 - [0]_2 = [0]_2 = [0]_2 - [0]_2$$

$$[1]_2 - [1]_2 = [0]_2 = [1]_2 - [1]_2$$

+ Commutatief: Cayleigh-tabel is symmetrisch rond diagonaal!

$$\Rightarrow a - c = a - d$$

+ Gesloten: Volledige tabel ingevuld: elke bewerking kan

\rightarrow Ja, Abelse groep! Alle 5 eig. aangevold.

\rightarrow Kanenbel in \mathbb{Z}_2 : hier belangrijk dat $-1 = 1$

\rightarrow Stel \mathbb{Z}_3 : $1 - (2 - 1) = 1 - 1 = 0$ en $(1 - 2) - 1 = (-1) - 1 = \stackrel{-1}{-1}$

$$\textcircled{6} \quad f = 2x^4 - 4x^3 + 15x^2 - 28x + 7$$

$$g = 2x^5 - 4x^4 - 5x^3 + 12x^2 - 3x$$

\Rightarrow ggdd?

\rightarrow Algoritme van Euclides:

$$\begin{array}{r} 2x^5 - 4x^4 - 5x^3 + 12x^2 - 3x \\ - 2x^5 - 4x^4 + 15x^3 - 28x^2 + 7x \\ \hline 0 \quad 0 \quad - 20x^3 + 40x^2 - 10x \end{array} \quad \left| \begin{array}{r} 2x^4 - 4x^3 + 15x^2 - 28x + 7 \\ x \end{array} \right.$$

$$\begin{array}{r} 2x^4 - 4x^3 + 15x^2 - 28x + 7 \\ - 2x^4 - 4x^3 + x \\ \hline 0 \quad 0 \quad 14x^2 - 28x + 7 \end{array} \quad \left| \begin{array}{r} -20x^3 + 40x^2 - 10x \\ -\frac{1}{10}x \end{array} \right.$$

$$\begin{array}{r} -20x^3 + 40x^2 - 10x \\ - 20x^3 + 40x^2 - 10x \\ \hline 0 \end{array} \quad \left| \begin{array}{r} 14x^2 - 28x + 7 \\ -\frac{20}{14}x \end{array} \right.$$

$$\Rightarrow \frac{14x^2 - 28x + 7}{\text{Koeff. } (\uparrow)} = \text{ggd}(f, g) = \boxed{x^2 - 2x + \frac{1}{2}}$$

⑦ a)

$$a_1 \quad \underline{\underline{+11}} \quad \stackrel{1}{\rightarrow} \quad \underline{\underline{+1}}$$

$$\Rightarrow d_1 = 1$$

$$a_2 \quad \underline{\underline{+111}} \quad \stackrel{2}{\rightarrow} \quad \underline{\underline{+111}} \quad \stackrel{3}{\rightarrow} \quad \underline{\underline{+111}}$$

$$\Rightarrow a_2 = 3$$

$$a_3 \quad \underline{\underline{+111}} \quad \stackrel{1}{\rightarrow} \quad \underline{\underline{+111}} \quad \stackrel{2}{\rightarrow} \quad \underline{\underline{+111}} \quad \stackrel{3}{\rightarrow} \quad \underline{\underline{+111}} \quad \downarrow 4$$

$$\underline{\underline{+111}} \quad \leftarrow \quad \underline{\underline{+111}} \quad \leftarrow \quad \underline{\underline{+111}} \quad \leftarrow \quad \underline{\underline{+111}}$$

$$\Rightarrow a_3 = 7$$

⑧ a) Wat wordt bedekt?

- Kolommen die overeenkomen met kragen met markering J
- Rijen die overeenkomen met kragen met markering N

↳ Zie oplossing in Google Docs

~~Def~~

↳ + beetje eigen verduidelijkende uitleg

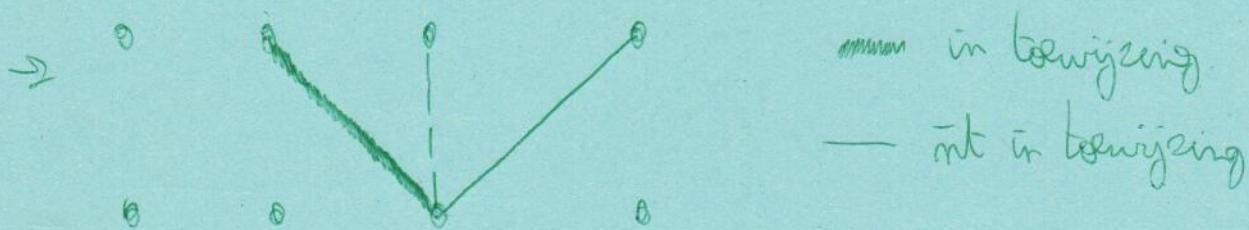
$a_{i,j}$ dubbel bedekt

0) $a_{i,j}$ is noodzakelijk 0.

→ Naast waar is de enige uitzet \hookrightarrow dubbel bedekt

→ Als elem. dubbel bedekt is, staan er minstens 2 nullen in de kolommen
1 mel in de rij. Dit zegt echter niets over dit element zelf.

b) $a_{i,j} = 0 \Rightarrow$ kolom j minstens 3 nullen



$a_{i,j}$ dubbelbedekt en 0 wat dan mag o?

↳ i-de rij bedekt \Rightarrow markering moet zeker N zijn \Rightarrow Dan rij bedekt

\Rightarrow In horizontale betrekking moet ook connectie zijn met a_i , zonder dat deze "gebruikt" wordt en markering J heeft $\{ \dots \}$ in betrekking
 \Rightarrow 3 takken vanuit bij \Rightarrow 3 nullen in kolom.

6

a) voor Benoiss dat:

$$\ln(f(x)g(x)) = \ln(f(x)) + \ln(g(x)) \text{ m.met } e^{\ln f} \text{ (dan } f \text{ en } g = 1)$$



$$\text{Uit: } \exp(\ln(f(x)g(x))) = \sum_i \frac{\ln(f(x)g(x))^i}{i!}$$

$\lim_{i \rightarrow \infty} \frac{\ln(f(x)g(x))^i}{i!} = \infty$

$$D(\ln(f(x)g(x))) = \frac{1}{f(x)g(x)} \cdot (f'(x)g(x) + f(x)g'(x))$$

$$\text{RL: } D(\ln(f(x)) + \ln(g(x))) = \frac{1}{f(x)} f'(x) + \frac{1}{g(x)} g'(x)$$

$$= \frac{f'(x)g(x)}{f(x)g(x)} + \frac{f(x)g'(x)}{f(x)g(x)}$$

$$= \frac{1}{f(x)g(x)} \cdot (f'(x)g(x) + f(x)g'(x)) \quad \square$$

7)

Discrete wiskunde II - Examen 2012-2013

Uit VTK Wiki

Examenvragen van Discrete wiskunde II.

Bestanden

Deze pagina heeft nog geen bestanden.

[Bestand kiezen](#) [Geen bestand gekozen](#) [Bestand anoniem uploaden](#)

Examen van 29 mei

1. Eerste vraag

$$x = (a_0, a_{-1} \dots a_{-(q-1)} 8) \text{ in basis } 10$$

We willen dit omzetten naar basis 16:

- a) Bestaat er een x waarvoor de omzetting naar basis 16 een oneindig aperiodieke voorstelling oplevert?
- b) Bestaat er een x waarvoor de omzetting naar basis 16 een eindige voorstelling oplevert?
- c) Bij een oneindig periodieke voorstelling, bevat het periodieke gedeelte maximum $10^{(q-1)}$ cijfers.

2. Tweede vraag

$$R = (a + b\sqrt{2}, \text{ met } a \text{ en } b \text{ een element van } \mathbb{Q})$$

- a) Bestaat er een f waar voor er een isomorfisme bestaat tussen R en $\mathbb{Q}[x]/(f)$?
- b) Is R een veld?

3. Derde vraag

Stel je hebt een eindig veld $F(p^n)$. W bevat de elementen van $F(p^n)$ waarvoor de minimale veelterm lineair is.

- a) Hoeveel elementen bevat W ? $\Rightarrow 74$ *Elk irreductibele veld, met deg de telkervan n elementen van V als zijn veld*
- b) Is de algebraïsche structuur die gevormd kan worden met W een veld? *Elk element van V is zijn inverse*

4. Vierde vraag

$$f = x^4 + 1 \text{ en } g = x^5 + x^3 + x^2 + 1$$

- a) Zoek f' en g' van de twee veeltermen in Z_2 . (niet zo moeilijk want dit is gewoon het algoritme van Euclides toepassen)
- b) Zijn f' en g' uniek? (ze zijn opgesteld in Z_2 !)

5. Vijfde vraag

Je hebt ($0 < M < N$) en m,n natuurlijke getallen.

Element a_i is gelijk aan het aantal waarden dat er voor m gevonden kunnen worden zodat $i = m \cdot M$

Element b_i is gelijk aan het aantal waarden dat er voor n gevonden kunnen worden zodat $i = n \cdot N$

Element c_i is gelijk aan het aantal waarden dat er voor het koppel (m,n) gevonden kan worden zodat $i = m \cdot M + n \cdot N$

- a) Stel de voortbrengende functie f op van a_i
- b) Stel de voortbrengende functie g op van b_i
- c) Stel de voortbrengende functie h op van c_i
- d) Geef het specifieke voorschrift van c_i voor M=1 en N=2

6. Zesde vraag

Het algoritme voor het zoeken van een vermeerderend pad aanpassen zodat het algoritme ALLE vermeerderende paden geeft.

Ontvangen van "https://vtk.ugent.be/wiki/Discrete_wiskunde_II_-_Examen_2012-2013"

- Deze pagina is het laatst bewerkt op 5 jul 2013 om 10:54.
- Over VTK Wiki
- //
- studiehulp@vtk.ugent.be

Examen 2012

0

① Niet gezien

② $a + b\sqrt{2}$, $a, b \in \mathbb{Q}$ $R = a + b\sqrt{2}$, met $a, b \in \mathbb{Q}$
 $\sqrt{2} \in R$

a) Bestaat er een waarde of een
isomorfie bestaat tussen $\mathbb{R}[x]/(f)$

b) Is R een veld?

We beginnen met b)

b) $a + b\sqrt{2}$ is invertbaar als $\exists a', b' \in \mathbb{Q} : (a + b\sqrt{2})(a' + b'\sqrt{2}) = 1$

$$\Leftrightarrow aa' + ab'\sqrt{2} + a'b\sqrt{2} + 2bb' = 1$$

$$\Leftrightarrow \begin{cases} aa' + 2bb' = 1 \\ ab' + a'b = 0 \end{cases} \Leftrightarrow \begin{cases} a' = -\frac{ab'}{b} \\ -\frac{a^2b'}{b} + 2bb' = 1 \end{cases} \Leftrightarrow \begin{cases} b' = \frac{1}{2b - \frac{a^2}{b}} = \frac{b}{2b^2 - a^2} \\ a' = -\frac{ab}{2b^2 - a^2} = -\frac{a}{2b^2 - a^2} \end{cases}$$

→ Deze a' en b' bestaan voor alle $a, b \in \mathbb{Q}$.

R is een veld wanneer alle niet-nul elementen invertbaar zijn.
 → ja!

↳ R moet ook commutatieve ring met eenheidselement zijn ...

↳ Eenheidselement: 1 ($a=1, b=0$) $\Rightarrow (a + b\sqrt{2}) \cdot 1 = a + b\sqrt{2}$

↳ Mogen deze echt alledaag bewezen worden?

↳ i) $(a + b\sqrt{2}, +)$ is een groep \rightarrow ja, optelling mag altijd + associatief ...

 (ii) gesloten? ja: $(a + b\sqrt{2})(c + d\sqrt{2})$ heeft altijd uitkomst

 (iii) Associatief? ja

 (iv) distributief? \rightarrow ja

 (v) commutatief \rightarrow ja

→ Eigenlijk lijkt $\mathbb{R}[\sqrt{2}]$ sterk op \mathbb{C} , maar met $(\sqrt{2})^2 = 2$ vs. $i^2 = -1$

⇒ R is een veld

④ $f = x^4 + 1$ $g = x^5 + x^3 + x^2 + 1$ in \mathbb{Z}_2 . a) zoef f en g
b) zijn ze omvek
a) Uitgebreid algoritme van Euclides → Opgelost: in \mathbb{Z}_2 !

$$\begin{array}{ll} i=0 & D_{-1}=0 \end{array}$$

$$t_{-1} = 1$$

$$D_0 = 0$$

$$D_0 = 1$$

$$t_0 = 0$$

$$R_0 = g$$

$$e_1 = f$$

$$i=1 \quad D_1 = 0 - 1 \cdot 0 = 0$$

$$t_1 = 1 - 0 \cdot 0 = 1$$

$$\begin{array}{r} x^5 + x^3 + x^2 + 1 \\ - x^5 \\ \hline x^3 + x^2 + x + 1 \\ = R_2 \end{array} \quad \left| \begin{array}{l} x^4 + 1 \\ x = q_1 \end{array} \right.$$

$$\begin{array}{l} \Rightarrow q_2 = x + 1 \Rightarrow i=3 \\ R_3 = 0 \end{array} \quad \begin{array}{l} \Rightarrow g' = D_2 = 1 \\ f' = t_2 = x \end{array}$$

$$i=2 \quad D_2 = 1 - 0 \cdot q_1 = 1$$

$$t_2 = 0 - 1 \cdot x = -x = x$$

$$\begin{array}{r} x^4 + 1 \\ - x^4 + x^3 + x^2 + x \\ \hline x^3 + x^2 + x + 1 \\ = R_3 \end{array} \quad \left| \begin{array}{l} x^3 + x^2 + x + 1 \\ x = q_2 \end{array} \right.$$

HIER NOG +1!

↳ dan laatste iteratie niet nodig

$$i=3 \quad D_3 = 0 - 1 \cdot x = -x = x$$

$$t_3 = 1 - x \cdot x = 1 - x^2 = x^2 + 1$$

$$\begin{array}{r} x^3 + x^2 + x + 1 \\ - x^3 + x^2 + x + 1 \\ \hline 0 = R_4 \end{array} \quad \left| \begin{array}{l} x^3 + x^2 + x + 1 \\ 1 \end{array} \right.$$

$\Rightarrow i=4$ "a is kopcoëff. van R_3 "

↳ 1 is kopcoëff. van $x^3 + x^2 + x + 1$

$$\Rightarrow g' = D_3 = x$$

$$f' = t_3 = x^2 + 1$$

b) ~~Indien niet in \mathbb{Z}_2 , kan de kopcoëff. nog anders zijn, maar deze kan enkel 1 zijn in \mathbb{Z}_2 .~~

→ FOUT: GGD is uniek maar f' niet begrensd

$$\frac{f - (c_0 + c_1 x + \dots + c_{NM-1} x^{NM-1})}{x^{MN}} = f + \frac{1}{1-x}$$

$$\Leftrightarrow f - (c_0 + c_1 x + \dots + c_{NM-1} x^{NM-1}) = fx^{MN} + \frac{x^{MN}}{1-x}$$

$$\Leftrightarrow f \cdot (1 - x^{MN}) = (c_0 + c_1 x + \dots + c_{NM-1} x^{NM-1}) + \frac{x^{MN}}{1-x}$$

④ d) $c_i = \text{floor}\left(\frac{i}{2}\right) + 1$

1. Algebraïsche structuren

In dit hoofdstuk definiëren we een aantal belangrijke algebraïsche structuren. Deze algebraïsche structuren modelleren veel voorkomende verzamelingen met bijhorende bewerkingen, zoals b.v. de reële getallen met als bewerkingen de optelling en de vermenigvuldiging. Het definiëren in algemene termen laat toe een aantal ‘gekende’ eigenschappen zo algemeen mogelijk op te stellen.

In de eerste paragraaf behandelen we algebraïsche structuren met één bewerking, nl. Abelse groepen. In de volgende twee paragrafen gaan we over naar algebraïsche structuren met twee bewerkingen, nl. ringen in paragraaf 1.2 en de meer specifieke integriteitsgebieden en velden in paragraaf 1.3. We besluiten het hoofdstuk in paragraaf 1.4 met de definitie en een eerste studie van een belangrijk soort ringen, nl. de zogenaamde veeltermringen.

1.1. Abelse groepen = algebraïsche structuren met één bewerking

We starten met een algebraïsche structuur met één bewerking, nl. de zogenaamde Abelse groepen.

1.1.1. Definitie en basiseigenschappen

Definitie 1.1. Een **Abelse groep** (Eng: Abelian group) bestaat uit een verzameling G en een binaire bewerking $*$ op G zodat

- (i) voor alle $a, b \in G$, $a * b \in G$ (G is gesloten onder $*$),
→ men kan de bewerking uitvoeren voor alle elementen van G
- (ii) voor alle $a, b, c \in G$, $a * (b * c) = (a * b) * c$ ($*$ is associatief),
- (iii) er bestaat een $e \in G$ (het eenheidselement of identiteitselement) zodat voor alle $a \in G$, $a * e = a = e * a$,
- (iv) voor alle $a \in G$ bestaat er een $a' \in G$ (de inverse van a) zodat $a * a' = a' * a = e$, en
- (v) opvolgende blz: commutatief

bij bewijs wordt geen commutativiteit gebruikt

→ geldt ook voor algemene groepen, en dus niet enkel
2 voor Abelse

(v) voor alle $a, b \in G$, $a * b = b * a$ ($*$ is commutatief).

Uit deze definitie volgt direct volgende eigenschap.

Eigenschap 1.1. Stel dat $(G, *)$ een Abelse groep is. Dan hebben we:

- (i) G bevat slechts één eenheidselement, en
- (ii) elk element van G heeft slechts één inverse.

Bewijs. We bewijzen beide delen afzonderlijk.

- (i) Stel dat G twee eenheidselementen e en e' bevat. Dan hebben we dat

$$e' = e * e' \rightsquigarrow a * e = a = e * a \\ = e,$$

waar we tweemaal gebruik gemaakt hebben van definitie 1.1(iii), éénmaal met e en éénmaal met e' als eenheidselement.

- (ii) We beschouwen een willekeurig element $a \in G$ en veronderstellen dat het twee inverse elementen heeft, nl. a' en a'' . Dan hebben we

$$\begin{aligned} a'' &= a'' * e \\ &= a'' * (a * a') \\ &= (a'' * a) * a' \\ &= e * a' \\ &= a'. \end{aligned}$$

We hebben hier achtereenvolgens gebruikgemaakt van het feit dat e het eenheidselement is in G , dat a' een inverse is van a , van de associativiteit van $*$, dat a'' een inverse is van a en tenslotte nogmaals dat e het eenheidselement is. \square

Veelal wordt de bewerking ' $*$ ' vervangen door ' $+$ ' of ' \cdot '; we spreken dan respectievelijk van de additieve of multiplicatieve notatie. Het eenheidselement wordt dan respectievelijk genoteerd als 0_G of 1_G (of door 0 of 1 als het duidelijk is wat G is), en de inverse van a als $-a$ of a^{-1} . Indien niet gespecificeerd, zullen we vanaf nu de additieve notatie veronderstellen. In deze notatie zullen we i.p.v. over inverse eerder spreken over tegengestelde. Verder noteren we $a + a + \dots + a$ (met n termen) als $n \cdot a$. Merk op dat n hier geen element is van G maar van \mathbb{N} , en dat ' $n \cdot$ ' een verkorte notatie is voor ' n dezelfde termen optellen'. Dit kan uitgebreid worden naar $(-n) \cdot a$, wat eigenlijk $n \cdot (-a)$ betekent. We merken op dat we ' \cdot ' voor twee verschillende bewerkingen gebruiken: zowel voor de groepsbewerking in de multiplicatieve notatie als voor de verkorte notatie voor het optellen van een aantal dezelfde termen wanneer we

de additieve notatie gebruiken. Dit geeft doorgaans geen aanleiding tot verwarring. We zullen ‘·’ trouwens veelal gewoon weglaten. Indien we de multiplicatieve notatie gebruiken, schrijven we voor $a \cdot a \cdot a \cdots \cdot a$ (met n factoren, $n \in \mathbb{N}$) ook wel a^n . Verder schrijven we a^{-n} voor $(a^{-1})^n$.

→ groep 'n Abelse groep zonder
commutativiteit

Naast het begrip ‘Abelse groep’ wordt ook het (algemenere) begrip ‘groep’ gebruikt, wat gedefinieerd wordt door simpelweg eigenschap (v) weg te laten in definitie 1.1. Merk trouwens op dat we in het bewijs van eigenschap 1.1 nergens de commutativiteit gebruikt hebben, zodat uniciteit van eenheidselement en inverse ook voor deze meer algemenere groepen geldt. We zullen het begrip groep in het vervolg van de cursus echter niet meer nodig hebben. Daarom zullen we vanaf nu het begrip ‘groep’ gebruiken om een Abelse groep aan te geven.

Tenslotte wordt de verzameling G soms ook een groep genoemd, waarmee we eigenlijk bedoelen dat de algebraïsche structuur $(G, +)$ een groep is. Er wordt dan impliciet aangenomen dat er een additieve operatie gedefinieerd is op de verzameling en dat aan de groepseigenschappen voldaan is. Dit zal ook gelden voor de algebraïsche structuren die verder in dit hoofdstuk gedefinieerd worden.

Voorbeeld 1.1. De structuren $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ en $(\mathbb{R}, +)$ zijn groepen met eenheidselement 0 en $-a$ tegengestelde van a . $(\mathbb{N}, +)$ is geen groep, aangezien positieve getallen geen tegengestelde hebben in \mathbb{N} .

→ zonder 0, want 0

Voorbeeld 1.2. De structuren $(\mathbb{Q} \setminus \{0\}, \cdot)$ en $(\mathbb{R} \setminus \{0\}, \cdot)$ zijn groepen.

$$\text{Wb. } [3]_4 = 3 + h \cdot 4 \\ \begin{array}{ccccccccc} & 3 & 7 & 11 & 15 & \dots \\ \hline 3 & | & | & | & | & \dots \\ 3 & 3 & 3 & 3 & 3 & \dots \end{array}$$

Voorbeeld 1.3. Definieer, voor $n \in \mathbb{N} \setminus \{0\}$, \mathbb{Z}_n als de verzameling der restklassen modulo n , i.e. $\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$ met $[i]_n = \{i + k \cdot n, k \in \mathbb{Z}\}$. Indien het duidelijk is wat n is, worden de n elementen ook wel gewoon als $[0], \dots, [n-1]$, of zelfs als $0, \dots, n-1$, aangeduid. We definiëren voor deze verzameling de volgende ‘+’-operator: voor alle $[i]_n, [j]_n \in \mathbb{Z}_n$, $[i]_n + [j]_n = [i+j]_n$. Dan is $(\mathbb{Z}_n, +)$ een groep, met $[0]_n$ het eenheidselement en $[-a]_n = [n-a]_n$ het tegengestelde element van $[a]_n$.

Uit definitie 1.1 volgen vrij direct een aantal basiseigenschappen van groepen.

Eigenschap 1.2. Veronderstel een groep G . Dan geldt voor alle $a, b, c \in G$ en $m, n \in \mathbb{Z}$:

- (i) als $a + b = a + c$, dan $b = c$;
- (ii) de vergelijking $a + x = b$ heeft een unieke oplossing $x \in G$;
- (iii) $-(a+b) = (-a) + (-b)$;
- (iv) $-(-a) = a$;

- (v) $(-n)a = -(na) = n(-a);$
- (vi) $(n+m)a = na + ma;$
- (vii) $n(ma) = (nm)a = m(na);$
- (viii) $n(a+b) = na + nb.$

Zie oefeningen

Bewijs. Rechtstreeks uit de definitie van groepen (oefening).

Definitie 1.2. Voor een groep $(G, +)$ kan een nieuwe bewerking gedefinieerd worden, nl. de **aftrekking**. Deze is voor $a, b \in G$ gedefinieerd als

$$a - b = a + (-b). = a - b = a + \begin{matrix} \text{inverse} \\ \text{"tegengestelde" } b \end{matrix}$$

Indien de multiplicatieve notatie gebruikt wordt, definieert men deze bewerking (de deling genaamd) als $a/b = a \cdot b^{-1}$.

Definitie 1.3. De **orde van een groep** $(G, +)$ is gelijk aan het aantal elementen van G indien dit aantal eindig is, en is oneindig indien dit niet zo is.

Merk op dat als de orde van een groep $(G, +)$ eindig is, ze gelijk is aan het kardinaalgetal $|G|$ van de verzameling G .

1.1.2. Deelgroepen

Vervolgens voeren we het begrip deelgroep in.

Definitie 1.4. Stel dat $(G, +)$ een groep is en dat $H \subset G$ ($H \neq \emptyset$) zodat

- (i) $a + b \in H$ voor alle $a, b \in H$, en \rightarrow gesloten
- (ii) $-a \in H$ voor alle $a \in H$. \rightarrow inverse

Dan wordt $(H, +)$ een **deelgroep** (Eng: subgroup) van $(G, +)$ genoemd.

Met andere woorden, H is een deelgroep van G indien H gesloten is onder de ‘+’ operator en het nemen van tegengestelden.

Eigenschap 1.3. Veronderstel een deelgroep $(H, +)$ van de groep $(G, +)$. Dan is $(H, +)$ een groep met 0_G als eenheidselement.

Bewijs. Er kan bewezen worden dat 0_G een element van H is en dat aan de vijf groepseigenschappen voldaan is (oefening).

Voorbeeld 1.4. De groep $(\mathbb{Z}, +)$ is een deelgroep van $(\mathbb{Q}, +)$, die op zijn beurt een deelgroep is van $(\mathbb{R}, +)$.

Veronderstel een groep G . Het is dan duidelijk dat G en $\{0\}$ deelgroepen zijn van G . Enkele interessanter deelgroepen van een gegeven groep volgen uit volgende eigenschap.

Eigenschap 1.4. Stel dat G een groep is, en veronderstel een $m \in \mathbb{Z}$. Dan zijn

- (i) $mG = \{ma, a \in G\}$, en
- (ii) $G\{m\} = \{a \in G, ma = 0\}$,

deelgroepen van G .

Bewijs. Het bewijs wordt gelaten als oefening.

Voorbeeld 1.5. Voor elk geheel getal $m \in \mathbb{Z}$ is $(m\mathbb{Z}, +)$ de deelgroep van $(\mathbb{Z}, +)$ bestaande uit de veelvouden van m . Er geldt dat $m\mathbb{Z} = m'\mathbb{Z}$ als en slechts als $m = \pm m'$. De deelgroep $\mathbb{Z}\{m\}$ is gelijk aan \mathbb{Z} als $m = 0$ en gelijk aan $\{0\}$ als $m \neq 0$.

1.1.3. Congruentie

Met de gehele getallen kunnen we modulorekenen. We rekenen dan met restklassen modulo een positief getal n (zie Discrete Wiskunde I). We veralgemenen dit nu naar algemene groepen.

Definitie 1.5. Veronderstel een groep G en een deelgroep H van G . We zeggen dat twee elementen $a, b \in G$ **gelijk zijn modulo H** (of congruent modulo H), en schrijven $a \equiv b \pmod{H}$, indien

$$\begin{array}{c} \Rightarrow a, b \in G \\ b - a \in H. \end{array}$$

Anders gezegd geldt $a \equiv b \pmod{H}$, indien er een $c \in H$ bestaat zodat $b = a + c$.

De modulo-operator definieert een partitie op G .

Eigenschap 1.5. Veronderstel een groep G en een deelgroep H van G . De congruentierelatie $\cdot \equiv \cdot \pmod{H}$ is een **equivalentierelatie**. We hebben m.a.w. voor alle $a, b, c \in G$ dat

- (i) $a \equiv a \pmod{H}$ (**reflexiviteit**),
- (ii) $a \equiv b \pmod{H} \Rightarrow b \equiv a \pmod{H}$ (**symmetrie**), en
- (iii) $a \equiv b \pmod{H}$ en $b \equiv c \pmod{H} \Rightarrow a \equiv c \pmod{H}$ (**transitiviteit**).

Bewijs. We bewijzen de drie delen afzonderlijk. Ze volgen in essentie uit het feit dat H een deelgroep is van G .

- (i) Aangezien H een deelgroep is van G bevat H het eenheidselement $0 = a - a$ (zie eigenschap 1.3).
- (ii) Indien $b - a \in H$, dan $a - b \in H$, opnieuw omdat H een deelgroep is (zie definitie 1.4). $\rightarrow a \in H$
- $\hookrightarrow a \in H, b \in H \Rightarrow a + b \in H$
- (iii) Uit definitie 1.4 volgt dat als $b - a \in H$ en $c - b \in H$, dan hun som $c - a \in H$. \square

Definitie 1.6. Aangezien $\cdot \equiv \cdot \pmod{H}$ een equivalentierelatie is, verdeelt ze G in equivalentie- of partitieklassen, de **restklassen** van G modulo H genoemd, of ook de **nevenklassen** (Eng: cosets) van G in H . De klasse van $a \in G$ is gegeven als

$$a + H = \{a + b, b \in H\}.$$

\hookrightarrow restklasse

Elk element $a + b$ wordt een **representant van de restklasse** $a + H$ genoemd. De verzameling der restklassen van G modulo H wordt genoteerd als G/H en wordt de **quotiëntverzameling** van G modulo H genoemd.

Voorbeeld 1.6. De modulodefinitie voor de gehele getallen is een speciaal geval van de voorgaande definitie. Neem nl. $G = \mathbb{Z}$ en $H = n\mathbb{Z} = \{n \cdot m, m \in \mathbb{Z}\}$. Inderdaad de restklasse $i + n\mathbb{Z} = \{i + n \cdot m, m \in \mathbb{Z}\} = [i]_n$. M.a.w. $\mathbb{Z}/n\mathbb{Z}$ is niks anders dan \mathbb{Z}_n , de gehele getallen modulo n .

We hebben volgende eigenschap wat betreft de aantalen elementen van de verschillende restklassen.

Eigenschap 1.6. Veronderstel een groep G en een deelgroep H van G . Dan heeft elke restklasse modulo H een gelijk aantal elementen, nl. de orde van H . $\rightarrow a + b, b \in H$

elander uelle a
je
heb altijd dezelfde
elementen
optellen
 \Rightarrow gelijke aarde

Bewijs. Het volstaat om een bijectie te vinden tussen H en $a + H$ voor alle $a \in G$. De functie $f_a : H \rightarrow a + H : b \rightarrow a + b$ is zo een bijectie. \square

Uit deze eigenschap volgt de volgende belangrijke eigenschap.

Eigenschap 1.7. (Theorema van Lagrange) Veronderstel G een groep met een eindig aantal elementen en H een deelgroep van G . Dan is de orde van H een deler van de orde van G .

$$\rightarrow a + H = \{a + b, b \in H\} \xrightarrow{\# \text{elementen van}}$$

Bewijs. Aangezien de restklassen van G modulo H partitieklassen vormen, ze allemaal hetzelfde aantal elementen bevatten als de orde van H volgens vorige eigenschap, en H één van de restklassen is, volgt dit direct.

Tenslotte kunnen we een optelling definiëren op G/H en dit wegens volgende eigenschap.

\downarrow
De restklassen van
 b modulo H

\Rightarrow quotiëntverzameling van G modulo H

\hookrightarrow
 \hookrightarrow $0 + H$
 \hookrightarrow $1 + H$
 \hookrightarrow $2 + H$
 \hookrightarrow \vdots
 \hookrightarrow $n + H$
 \hookrightarrow \vdots
 \hookrightarrow $m + H$
 \hookrightarrow \vdots
 \hookrightarrow $b + H$
 \hookrightarrow \vdots
 \hookrightarrow $\text{restklassen van } b$
 \hookrightarrow $\text{orde } H$ is deler v. orde G

Eigenschap 1.8. Veronderstel een groep G en een deelgroep H van G . Dan geldt voor alle $a, a', b, b' \in G$ dat, als $a \equiv b \pmod{H}$ en $a' \equiv b' \pmod{H}$, ook $a + a' \equiv b + b' \pmod{H}$.

Bewijs. Volgt uit het feit dat H een deelgroep is van G (oefening).

Definitie 1.7. Veronderstel een groep G en een deelgroep H van G . We definiëren volgende optelling op de quotiëntverzameling G/H :

$$(a + H) + (b + H) = (a + b) + H.$$

→ som v. 2 restklassen is ook restklasse

Het kan eenvoudig bewezen worden dat $(G/H, +)$ een groep is. We noemen deze de **quotiëntgroep** (Eng: quotient group) van G modulo H .

$\hookrightarrow (G/H, +) \rightarrow a + H, \forall a \in G$

1.1.4. Groepshomomorfismen en -isomorfismen

Definitie 1.8. Veronderstel twee groepen $(G, +)$ en $(G', +)$. Een **groepshomomorfisme** (Eng: group homomorphism) is een functie ρ van G naar G' waarvoor geldt dat $\rho(a + b) = \rho(a) + \rho(b)$ voor alle $a, b \in G$.

→ "bij een groepshomomorfisme maakt het niet uit in welke groep de bewerking wordt uitgevoerd"

Merk op dat in de gelijkheid $\rho(a + b) = \rho(a) + \rho(b)$ de eerste optelling plaatsgrijpt in G terwijl de tweede optelling in G' gebeurt.

Twee verzamelingen spelen een belangrijke rol bij groepshomomorfismen.

Definitie 1.9. Gegeven een groepshomomorfisme $\rho : G \rightarrow G'$. Dan wordt $\rho(G) = \{\rho(a), a \in G\}$ het **beeld** (Eng: image) van ρ genoemd. Verder wordt de **nulruimte** of **kern** (Eng: kernel) van ρ gedefinieerd als $\ker(\rho) = \{a \in G, \rho(a) = 0_{G'}\}$.

Voorbeeld 1.7. Gegeven een groep G en een $m \in \mathbb{Z}$. Dan is $\rho(a) : G \rightarrow G : a \rightarrow ma$ een groepshomomorfisme, want we hebben $m \cdot (a + b) = ma + mb$. Het beeld van dit homomorfisme is mG , terwijl de nulruimte $G\{m\}$ is (zie eigenschap 1.4 voor de definities van deze twee verzamelingen).

Hierna volgen een aantal basiseigenschappen van groepshomomorfismen.

Eigenschap 1.9. Gegeven een groepshomomorfisme ρ van G naar G' , $a, b \in G$ en $n \in \mathbb{Z}$. Dan geldt dat

- (i) $\rho(0_G) = 0_{G'}$,
- (ii) $\rho(-a) = -\rho(a)$,
- (iii) $\rho(na) = n\rho(a)$,

daarvan het beeld $\rho(a)$ is element van G' en $\rho(na)$ is element van G'

- (iv) voor elke deelgroep H van G , $\rho(H) = \{\rho(a), a \in H\}$ een deelgroep is van G' ,
- (v) $\ker(\rho)$ een deelgroep is van G ,
- (vi) $\rho(a) = \rho(b) \Leftrightarrow a \equiv b \pmod{\ker(\rho)}$,
- (vii) ρ is injectief $\Leftrightarrow \ker(\rho) = \{0_G\}$, en
- (viii) voor elke deelgroep H' van G' , $\rho^{-1}(H')$ een deelgroep is van G die $\ker(\rho)$ bevat.

Bewijs. We bewijzen alle delen afzonderlijk.

- (i) We kunnen achtereenvolgens schrijven dat

$$\rho(0_G) = 0_{G'}$$

$$\begin{aligned} \rho(0_G) + 0_{G'} &= \rho(0_G) \\ &= \rho(0_G + 0_G) \\ &= \rho(0_G) + \rho(0_G). \end{aligned}$$

→ welke voorwaarde
maakt niet uit:
zonder hem gedaan

Hieruit volgt het gestelde door gebruik te maken van eigenschap 1.2(i).

- (ii) We kunnen schrijven dat

$$\rho(-a) = -\rho(a)$$

$$\begin{aligned} 0_{G'} &= \rho(0_G) \\ &= \rho(a + (-a)) \\ &= \rho(a) + \rho(-a), \end{aligned}$$

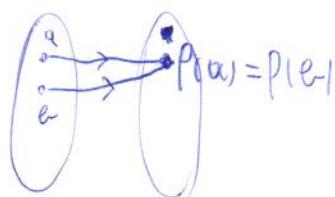
waaruit het gestelde volgt.

elkaar inverse

↳ als $a+b=a+c$, dan $b=c$

- (iii) Voor $n = 0$ volgt dit uit (i). Voor $n > 0$ volgt dit uit de definitie van een groepshomomorfisme door inductie op n . Voor $n < 0$ volgt dit uit het geval $n > 0$, eigenschap 1.2(v) en uit (ii).
- (iv) Stel $a', b' \in \rho(H)$. Dan zijn er $a, b \in H$ zodat $a' = \rho(a)$ en $b' = \rho(b)$. Aangezien H een (deel)groep is, volgt $a+b, -a \in H$ en dus $\rho(a+b), \rho(-a) \in \rho(H)$. Aangezien ρ een groepshomomorfisme is, volgt tenslotte dat $a' + b' = \rho(a) + \rho(b) \in \rho(H)$ en $-a' = -\rho(a) \in \rho(H)$.
- (v) Stel $a, b \in \ker(\rho)$. Dan $\rho(a) = \rho(b) = 0_{G'}$ en aangezien ρ een groepshomomorfisme is, $\rho(a+b) = \rho(-a) = 0_{G'}$. Dus $a+b, -a \in \ker(\rho)$.
- (vi) We hebben achtereenvolgens:

$$\text{ab } \rho(a) = \rho(b);$$



$$\begin{aligned} \rho(a) &= \rho(b) \\ \Leftrightarrow \rho(b) - \rho(a) &= 0_{G'} \\ \Leftrightarrow \rho(b-a) &= 0_{G'} \quad \text{) want groepshomomorfisme} \\ \Leftrightarrow b-a &\in \ker(\rho) \\ \Leftrightarrow a &\equiv b \pmod{\ker(\rho)}. \end{aligned}$$

↳ Definitie 1.5: $a \equiv b \pmod{H}$
indien $b-a \in H$

ρ is injectief $\Rightarrow \ker(\rho) = \{0_G\}$

9

- (vii) Als ρ injectief is, kan er maximum één element uit G $0_{G'}$ als beeld hebben. Volgens (i) is dit 0_G . Als ρ niet injectief is, bestaan er twee verschillende elementen $a, b \in G$ waarvoor $\rho(a) = \rho(b)$. Dus $\rho(a) - \rho(b) = \rho(a - b) = 0_{G'}$ en $\ker(\rho)$ bevat, naast 0_G , het niet-nul element $a - b$.
- (viii) Als $\rho(a), \rho(b) \in H'$ dan $\rho(a + b) = \rho(a) + \rho(b) \in H'$ en $\rho(-a) = -\rho(a) \in H'$. Dus $\rho^{-1}(H')$ is een deelgroep van G . Aangezien $0_{G'} \in H'$ hebben we verder dat $\ker(\rho) \subseteq \rho^{-1}(H')$.
 $\hookrightarrow \{\alpha \in H' : \rho(\alpha) = 0_{G'}\}$

Definitie 1.10. Een bijectief groepshomomorfisme $\rho : G \rightarrow G'$ wordt een **groepsisomorfisme** (Eng: group isomorphism) genoemd. Als zo een groepsisomorfisme bestaat tussen G en G' , dan worden G en G' groepsisomorf genoemd, genoteerd als $G \cong G'$. Als $G = G'$, dan wordt ρ een **groepsautomorfisme** (Eng: group automorphism) genoemd.

Eigenlijk komt een groepsisomorfisme neer op het hernoemen van de elementen; alle structurele eigenschappen van de groep worden behouden.

We zullen de prefix 'groep' meestal weglaten uit de benamingen geïntroduceerd in deze paragraaf. We spreken dan b.v. van een homomorfisme i.p.v. een groepshomomorfisme.

1.1.5. Cyclische groepen

Een interessante subklasse van de groepen zijn de zogenaamde cyclische groepen. Daarvoor definiëren we eerst een specifieke deelgroep van een willekeurige groep G .

Definitie 1.11. Gegeven een groep G en een element $a \in G$. Dan definiëren we volgende deelgroep van G :

$$\langle a \rangle = \{ma, m \in \mathbb{Z}\}.$$

Deze groep wordt de **deelgroep van G voortgebracht door a** (Eng: subgroup of G generated by a) genoemd. Verder definiëren we **de orde van het element a** als de orde van de groep $\langle a \rangle$.
 \hookrightarrow # elementen van

We kunnen nu een cyclische groep definiëren.

Definitie 1.12. Een groep G wordt **cyclisch** (Eng: cyclic) genoemd als $G = \langle a \rangle$ voor een $a \in G$. Het element a wordt een **primitief element of voortbrenger** (Eng: generator) van de cyclische groep G genoemd.

$(\mathbb{R}, +)$ is geen cyclische groep, er bestaat geen getal waarvan je elk getal kan berekenen.
 $\hookrightarrow (\mathbb{R}, +)$ heeft geen kleinste positieve getal

10

\Rightarrow elk elem. v. $(\mathbb{Z}, +)$ kan berekend worden door

Voorbeeld 1.8. De groep $(\mathbb{Z}, +)$ is cyclisch en wordt voortgebracht door 1. Het enige andere primitieve element is -1. Ook de groep $(\mathbb{Z}_n, +)$ is cyclisch en wordt voortgebracht door $[1]_n$. De andere primitieve elementen zijn alle $[m]_n$ waarvoor geldt dat m en n relatief priem zijn (zie ook Discrete Wiskunde I).

$\hookrightarrow m \text{ en } n \text{ onderling ondelbaar} \rightarrow \text{ggd}(m, n) = 1$

Het blijkt dat er eigenlijk geen andere cyclische groepen bestaan dan deze uit dit voorbeeld. M.a.w. cyclische groepen zijn isomorf ofwel met \mathbb{Z} , ofwel met \mathbb{Z}_n voor een zekere $n \in \mathbb{N} \setminus \{0\}$.

\hookrightarrow Eigenschap groepshomomorfisme

Eigenschap 1.10. Veronderstel een cyclische groep G . Als G van oneindige orde is, is $G \cong \mathbb{Z}$. Als de orde van G gelijk is aan n ($n \in \mathbb{N} \setminus \{0\}$), dan is $G \cong \mathbb{Z}_n$.

\hookrightarrow groepsisomorf, bijiet groepshomomorf

Bewijs. Aangezien G een cyclisch groep is, bevat hij een primitief element a . Construeren we nu de functie $\rho : \mathbb{Z} \rightarrow G : m \mapsto ma$. Het kan gemakkelijk ingezien worden dat ρ een homomorfisme is. Aangezien a een primitief element is van G moet ρ surjectief zijn. We kunnen nu twee gevallen onderscheiden.

(i) $\ker(\rho) = \{0\}$: uit eigenschap 1.9(vii) volgt dat ρ , naast surjectief, ook injectief is, en dus bijectief. Dus ρ is een isomorfisme en $G \cong \mathbb{Z}$.

(ii) $\ker(\rho) \neq \{0\}$: in dit geval zijn er $m \in \mathbb{Z} \setminus \{0\}$ waarvoor geldt dat $ma = 0$. Noem n het kleinste positieve getal dat hieraan voldoet. Dan volgt dat $G = \{ma, 0 \leq m \leq n-1\}$, aangezien $(m+kn)a = ma$ voor alle $0 \leq m \leq n-1$ en $k \in \mathbb{Z}$. Verder is $m_1a \neq m_2a$ indien $0 \leq m_1 < m_2 \leq n-1$, aangezien anders $(m_1 - m_2)a = 0$, met $0 < m_1 - m_2 < n$ en n is per definitie het kleinste positieve getal waarvoor geldt $na = 0$. Dus G bestaat uit n verschillende elementen. Het is dan gemakkelijk in te zien dat $\hat{\rho} : \mathbb{Z}_n \rightarrow G : [k]_n \mapsto ka$ een isomorfisme is.

Hieruit volgt dat een cyclische groep isomorf is met \mathbb{Z} of met \mathbb{Z}_n (voor een zekere positieve n). De orde van G bepaalt met welke preciesies. \square

De volgende eigenschap voor groepen is een direct gevolg van de vorige.

Eigenschap 1.11. Veronderstel een groep G en een element $a \in G$.

$\hookrightarrow \mathbb{Z}_n$

(i) Als er $m \in \mathbb{N} \setminus \{0\}$ bestaan waarvoor $ma = 0$, dan is de kleinste mogelijke n de orde van a . De andere zijn de gehele veelvouden van deze orde. De deelgroep $\langle a \rangle$ bevat de n verschillende elementen $0 \cdot a, 1 \cdot a, \dots, (n-1) \cdot a$.

\Rightarrow elementen in $\langle a \rangle$

(ii) Als de orde van G eindig is, dan $|G| \cdot a = 0$ en de orde van a deelt $|G|$.

Bewijs. Deel (i) volgt onmiddellijk uit het bewijs van vorige eigenschap met de groep G in dat bewijs gelijk aan $\langle a \rangle$. Deel (ii) volgt uit deel (i) en het theorema van Lagrange (eigenschap 1.7, p. 6). \square

hier: \mathbb{Z}_5

$\hookrightarrow |a| = 5$

$\Rightarrow a^5 = 0 \text{ in } \mathbb{Z}_5$

Hieruit kunnen we nog een aantal eigenschappen voor groepen afleiden.

Eigenschap 1.12. *Gegeven een groep G met orde een priemgetal. Dan is G cyclisch.*

Bewijs. Noem de orde van G p , met p een priemgetal. Neem een $a \in G \setminus \{0\}$ en noem n de orde van a . Aangezien de orde van een element de orde van de groep deelt (zie de vorige eigenschap), is $n = 1$ of $n = p$. Aangezien $1 \cdot a \neq 0$, moet $n = p$ zijn. Dus $G = \langle a \rangle$ en G is cyclisch. \square

Eigenschap 1.13. *Veronderstel een groep G en een element $a \in G$. Stel verder dat er een $e \in \mathbb{N} \setminus \{0\}$ en een priemgetal p bestaan zodat geldt dat $p^e a = 0$ en $p^{e-1} a \neq 0$. Dan is de orde van a gelijk aan p^e .*

Bewijs. Noem m de orde van a . Aangezien $p^e a = 0$ moet $m | p^e$ delen, krachtens eigenschap 1.11(i). Aangezien p priem is moet daarom $m = p^f$ voor een $f \in \{0, \dots, e\}$. Echter, als $f < e$ zou zijn dan geldt dat $p^{e-1} a = 0$, wat in tegenstelling is met de assumpties in de eigenschap. Dus $f = e$ en $m = p^e$. \square

Eigenschap 1.14. *Veronderstel een groep G en elementen $a, b \in G$ waarbij de orde m van a en de orde n van b eindig zijn, en $\text{ggd}(m, n) = 1$. Dan is de orde van $a + b$ gelijk aan mn .*

\rightarrow enkel $\{0\}$ gemeensch.

Bewijs. We bewijzen eerst dat $\langle a \rangle \cap \langle b \rangle = \{0\}$. Veronderstel daarom een $c \in \langle a \rangle \cap \langle b \rangle$. Dan moet de orde van c zowel m als n delen en aangezien $\text{ggd}(m, n) = 1$ moet de orde van c gelijk aan 1 zijn. Dus $c = 0$. \rightarrow werk $l \geq 0$

Noem nu l de orde van $a + b$. Aangezien $l \cdot (a + b) = 0$ geldt er $la = -lb$. Dus $la \in \langle b \rangle$ en aangezien uiteraard $la \in \langle a \rangle$, ook $la \in \langle a \rangle \cap \langle b \rangle$. Dus $la = 0$ en m deelt l . Op een gelijkaardige manier bekomen we dat n ook l deelt. Aangezien $\text{ggd}(m, n) = 1$ deelt het product mn l ook (een getal is steeds ontbindbaar in priemfactoren). Het is verder duidelijk dat $mn(a + b) = 0$ aangezien m en n de ordes van respectievelijk a en b zijn, en dus is mn deelbaar door l . Als twee natuurlijke getallen deelbaar zijn door elkaar zijn ze gelijk, en dus geldt dat mn de orde van $a + b$ is. $\exists mn = l$ \square

We hebben in dit laatste bewijs een aantal eigenschappen gebruikt van elementaire getaltheorie voor natuurlijke getallen. We zullen deze eigenschappen ook bewijzen in de context van veeltermen in hoofdstuk 2.

We voeren nog een belangrijk begrip in.

\rightarrow $\begin{cases} m \cdot a = 0 \\ \langle a \rangle \end{cases}$

Definitie 1.13. *We noemen de **exponent** van een groep G het kleinste natuurlijke getal m verschillend van 0 waarvoor geldt dat $mG = \{0\}$. M.a.w. de exponent is het kleinste natuurlijke getal m verschillend van 0 waarvoor geldt dat $ma = 0$ voor alle $a \in G$. Als er zo geen m bestaat, stellen we de exponent per definitie gelijk aan 0.*

blyft!
m-hagr
wont m-hagr
alle abs v. den
van b)
↳ deswommen
orde op
= brantle

Enkele basiseigenschappen van de exponent van een groep zijn de volgende.

Eigenschap 1.15. Veronderstel dat G een groep is met exponent m . Dan geldt:

- (i) Als $kG = \{0\}$ voor een $k \in \mathbb{Z}$ dan geldt dat k deelbaar is door m ;
- (ii) Als de orde van G eindig is, deelt m die orde; \rightarrow de exponent
- (iii) Als $m \neq 0$, dan is, voor elk element $a \in G$, de orde van a eindig en een deler van m ;
- (iv) Als G cyclisch is, dan is $m = 0$ als de orde van G oneindig is, en is m gelijk aan de orde van G als die orde eindig is.

Bewijs. Het bewijs wordt gelaten als oefening.

Uit deze basiseigenschappen volgt al dat er verbanden bestaan tussen de exponent van een groep enerzijds en zijn orde en de orde van zijn elementen anderzijds. Dit kan nog meer geëxpliciteerd worden in het geval van een eindige groep.

Eigenschap 1.16. Veronderstel een eindige groep G met exponent m . Dan bevat G een element van orde m .

Bewijs. Als $m = 1$ dan $G = \{0\}$ en 0 heeft orde 1. Dus veronderstel in het vervolg $m > 1$. We ontbinden m in priemfactoren: $m = \prod_{i=1}^r p_i^{e_i}$, met p_i priemgetallen en $r, e_i \in \mathbb{N} \setminus \{0\}$. We bewijzen eerst dat er voor elke $i = 1, \dots, r$ een $a_i \in G$ bestaat zodat $(m/p_i)a_i \neq 0$. Veronderstel nl. dat er voor een zekere i voor alle $a \in G$ geldt dat $(m/p_i)a = 0$. Dan is m niet het kleinste natuurlijke getal verschillend van 0 waarvoor geldt dat $ma = 0$ voor alle $a \in G$, in tegenstelling met het feit dat m de exponent is van G .

Dus voor elke $i = 1, \dots, r$ bestaat er een $a_i \in G$ zodat $(m/p_i)a_i \neq 0$. Dan volgt uit eigenschap 1.13 dat de orde van het element $(m/p_i)a_i$ gelijk is aan $p_i^{e_i}$, en dit voor elke $i = 1, \dots, r$. Tenslotte volgt uit eigenschap 1.14 dat het element $\sum_{i=1}^r (m/p_i)a_i$ orde m heeft. \square

Volgende belangrijke eigenschap volgt dan quasi direct.

Eigenschap 1.17. Een eindige groep G is cyclisch als en slechts als zijn orde gelijk is aan zijn exponent.

Bewijs. Dit volgt uit eigenschappen 1.15(iv) en 1.16. \square

$$\begin{aligned} &\hookrightarrow \mathbb{Z}_3 : \{0, 1, 2\} \\ &\hookrightarrow \mathbb{Z}_3, 1 = 0 \\ &\text{4 operatoren} \end{aligned}$$

1.2. Ringen = algebraïsche structuren met twee bewerkingen

We gaan nu over naar algebraïsche structuren met twee bewerkingen. De meest algemene structuur die we zo beschouwen zijn de zogenaamde ringen.

$$\begin{array}{ccc} 0,4 & 0,5 & 0,6 \\ 1 & 2 & 3 \end{array}$$

$$\hookrightarrow 0,53? \rightsquigarrow 2 + \frac{3-2}{10} \cdot 3 = 2 + \frac{1}{10} \cdot 3 = 2,3 = 2,3 \quad 13$$

1.2.1. Definitie en basiseigenschappen

Definitie 1.14. De structuur $(R, +, \cdot)$ is een **ring** (Eng: ring) indien de volgende voorwaarden voldaan zijn:

- (i) $(R, +)$ is een groep,
- (ii) voor alle $a, b \in R$, $a \cdot b \in R$ (R is gesloten onder \cdot),
- (iii) voor alle $a, b, c \in R$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (\cdot is associatief), en
- (iv) voor alle $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ en $(b + c) \cdot a = b \cdot a + c \cdot a$ (\cdot is distributief t.o.v. $+$).

We schrijven vaak kortweg R om de ring $(R, +, \cdot)$ aan te duiden.

Indien daarenboven

- (v) voor alle $a, b \in R$, $a \cdot b = b \cdot a$ (\cdot is commutatief),

dan noemt men R een **commutatieve ring**.

Indien naast (i)-(iv)

- (v') er een element $1 \in R$ is, zodat, voor alle $a \in R$, $a \cdot 1 = 1 \cdot a = a$ (1 is het eenheidselement voor \cdot),

dan noemt men R een **ring met eenheidselement**.

Net als een deelgroep kunnen we ook het begrip deelring invoeren.

Definitie 1.15. Een deelverzameling S van een ring R wordt een **deelring** (Eng: subring) van R genoemd indien

- (i) S een deelgroep van de additieve groep R is, en
- (ii) voor alle $a, b \in S$, $a \cdot b \in S$ (S is gesloten onder de vermenigvuldiging).

Eigenschap 1.18. Veronderstel een deelring $(S, +, \cdot)$ van de (commutatieve) ring $(R, +, \cdot)$. Dan is $(S, +, \cdot)$ een (commutatieve) ring.

Bewijs. De ringeigenschappen zijn gemakkelijk te bewijzen (oefening).

Voorbeeld 1.9. De additieve (deel)groepen \mathbb{Z} , \mathbb{Q} en \mathbb{R} uit voorbeeld 1.1, p. 3 zijn tevens (deel)ringen met de vermenigvuldiging als tweede bewerking.

Voorbeeld 1.10. Definieer de vermenigvuldiging in \mathbb{Z}_n als volgt: voor alle $[i]_n, [j]_n$, $[i]_n \cdot [j]_n = [i \cdot j]_n$. De structuur $(\mathbb{Z}_n, +, \cdot)$ is dan een ring.

Ook voor ringen kunnen een aantal basiseigenschappen eenvoudig bewezen worden.

Eigenschap 1.19. Veronderstel een ring R en $a, b \in R$. Dan geldt:

- (i) R bevat maximaal één eenheidselement (voor de vermenigvuldiging);
- (ii) $0_R \cdot a = a \cdot 0_R = 0_R$;
- (iii) $a(-b) = (-a)b = -(ab)$;
- (iv) $(-a)(-b) = ab$.

Bewijs. Rechtstreeks uit de definitie van ringen (oefening).

We nemen in het vervolg aan dat $1 \neq 0$. Dit sluit enkel de ring uit met slechts één element (ook wel de triviale ring genaamd).

Definitie 1.16. De karakteristiek van een ring R is gedefinieerd als de exponent van de onderliggende additieve groep $(R, +)$.

Eigenschap 1.20. Veronderstel een ring R met eenheidselement. Dan is de karakteristiek van R gelijk aan de orde van 1 in de additieve groep $(R, +)$ als die orde eindig is, en gelijk aan 0 als die orde oneindig is.

Bewijs. Er geldt voor $m \in \mathbb{Z}$ en een $a \in R$ dat

$$\begin{aligned} ma &= m \cdot (1 \cdot a) \\ &= (m \cdot 1) \cdot a. \end{aligned}$$

Hieruit en uit eigenschap 1.19(ii) volgt dat als $m \cdot 1 = 0$ dan $ma = 0$ voor alle $a \in R$. Omgekeerd geldt uiteraard ook dat als $ma = 0$ voor alle $a \in R$ dan $m \cdot 1 = 0$. Dus als de orde van 1 oneindig is, is de exponent van R 0 en anders zijn de orde van 1 en de exponent van R gelijk. \square

De karakteristiek is dus de kleinste $m \in \mathbb{N} \setminus \{0\}$ waarvoor geldt dat $m \cdot 1 = 0$, of is 0 als er zo geen m is.

Definitie 1.17. Veronderstel een commutatieve ring R en $a, b \in R$. We zeggen dat b a deelt, of ook, dat a deelbaar is door b, indien er een $c \in R$ bestaat zodat $a = bc$. Het element b wordt een **deler** van a genoemd en we schrijven $b|a$.

Het binomium van Newton, algemeen bekend voor de reële getallen, geldt ook voor algemene commutatieve ringen.

Eigenschap 1.21. (Binomium van Newton) Veronderstel een commutatieve ring R , twee elementen $a, b \in R$ en een natuurlijk getal n . Dan geldt

$$(a + b)^n = \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i,$$

met de binomiaalcoëfficiënt $\binom{n}{i}$ gedefinieerd als

$$\binom{n}{i} = \frac{n!}{i!(n-i)!}.$$

Bewijs. Via inductie op n (oefening).

Merk op dat de binomiaalcoëfficiënt een natuurlijk getal is en geen element van de ring.

1.2.2. Congruentie

Net zoals in een groep kunnen we ook in een commutatieve ring met eenheidselement modulorekenen. We voeren daartoe eerst het begrip **ideaal** in.

Definitie 1.18. Veronderstel een commutatieve ring R met eenheidselement. Een **ideaal** (Eng: ideal) van R is een deelgroep I van de additieve groep R die gesloten is onder de vermenigvuldiging met elementen van R . M.a.w. voor alle $a \in I$ en $b \in R$ geldt dat $ab \in I$. \rightarrow element $\overset{\text{deelgroep}}{\underset{I}{\in}}$ van $I \cdot$ element $v. R =$ element $v. I$

Voorbeeld 1.11. Gegeven een $n \in \mathbb{Z}$. Dan is $n\mathbb{Z} = \{nm, m \in \mathbb{Z}\}$ een ideaal van de ring \mathbb{Z} .

Dit voorbeeld kan uitgebreid worden naar meer algemene ringen.

Definitie 1.19. Veronderstel R een commutatieve ring met eenheidselement en $a \in R$. Dan is $aR = \{ab, b \in R\}$ een ideaal, het **ideaal voortgebracht door a** (Eng: ideal generated by a). Het wordt ook een **hoofdideaal** (Eng: principal ideal) van R genoemd. \rightarrow dus voor ideaal geldt dat voor een (beperkte) deelgroep, hoofdideaal: $\forall b \in R$ \exists ^{voortgebr} element a

Aangezien een ideaal een deelgroep van de additieve groep R is, kunnen we de definitie van congruentie voor groepen overnemen voor idealen. M.a.w. $a \equiv b \pmod{I}$ als en slechts als $b - a \in I$. De reden waarom we dit beperken tot idealen (i.p.v. tot meer algemene deelringen van R) is omdat we voor idealen een vermenigvuldiging kunnen definiëren op de quotiëntverzameling R/I .

Eigenschap 1.22. Veronderstel een commutatieve ring R met eenheidselement, een ideaal I van R , en elementen $a, a', b, b' \in R$. Als $a \equiv b \pmod{I}$ en $a' \equiv b' \pmod{I}$, dan ook $aa' \equiv bb' \pmod{I}$. \rightarrow dus dan $bb' - aa' \in I$

Bewijs. We moeten bewijzen dat $bb' - aa' \in I$. We hebben dat er $c, c' \in I$ zodat $b = a + c$ en $b' = a' + c'$. Dan is $bb' - aa' = ac' + a'c + cc'$. Aangezien I een ideaal is zijn de drie termen in het rechterlid elementen van I . En dus ook het linkerlid. \square

$$\begin{aligned} &\therefore "a \in I, b \in R" \\ &\rightarrow ab \in I \quad \text{Vrij} \\ &\rightarrow \text{product uitdrukking in } I \end{aligned}$$

Op de quotiëntverzameling modulo I kunnen we dus niet enkel een optelling, maar ook een vermenigvuldiging definiëren. Dit leidt tot volgende definitie.

Definitie 1.20. Veronderstel een commutatieve ring R met eenheidselement en een ideaal I van R . Op de quotiëntverzameling R/I definiëren we een optelling en vermenigvuldiging:

$$(a + I) + (b + I) = (a + b) + I,$$

$$(a + I) \cdot (b + I) = (a \cdot b) + I.$$

Het kan bewezen worden dat $(R/I, +, \cdot)$ een commutatieve ring met eenheidselement is. We noemen deze de **quotiëntring** (Eng: quotient ring) van R modulo I .

In het speciaal geval van een hoofdideaal passen we de notatie aan in navolging van modulorekenen bij de gehele getallen.

Definitie 1.21. Indien het hoofdideaal $I = aR$ het ideaal is voortgebracht door een element $a \in R$, dan schrijven we $[b]_a$ i.p.v. $b + aR$, spreken we van de quotiëntring R modulo a i.p.v. R modulo aR , en noteren we $R/(a)$ i.p.v. R/aR .

1.2.3. Ringhomomorfismen en -isomorfismen

Vervolgens bespreken we de uitbreiding van de begrippen homo- en isomorfismen naar een ringcontext.

Definitie 1.22. Veronderstel twee ringen $(R, +, \cdot)$ en $(R', +, \cdot)$. Een **ringhomomorfisme** (Eng: ring homomorphism) is een functie ρ van R naar R' waarvoor geldt dat

- (i) $\rho(a + b) = \rho(a) + \rho(b)$ voor alle $a, b \in R$, en
- (ii) $\rho(a \cdot b) = \rho(a) \cdot \rho(b)$ voor alle $a, b \in R$. \rightarrow Ring, dus moet \circ ...

Definitie 1.23. Een bijectief ringhomomorfisme $\rho : R \rightarrow R'$ wordt een **ringisomorfisme** (Eng: ring isomorphism) genoemd. Als zo een ringisomorfisme bestaat tussen R en R' , dan worden R en R' ringisomorf genoemd, genoteerd als $R \cong R'$. Als $R = R'$, dan wordt ρ een **ringautomorfisme** (Eng: ring automorphism) genoemd.

Eigenlijk komt een ringisomorfisme - net zoals een groepsisomorfisme - enkel neer op het hernoemen van de elementen. We zullen overigens veelal spreken van een ‘isomorfisme’ aangezien meestal duidelijk is wat we er precies mee bedoelen, een groeps- of een ringisomorfisme. Idem voor een homomorfisme.

1.2.4. Nuldelers en inverteerbare elementen

We besluiten deze sectie met de definitie van twee soorten interessante elementen van ringen en bewijzen zekere verbanden tussen beiden.

Definitie 1.24. Veronderstel een commutatieve ring R en $a \in R \setminus \{0\}$. We noemen a een **nuldeler** indien er een $b \in R \setminus \{0\}$ bestaat zodat $ab = 0$.

Voorbeeld 1.12. In \mathbb{Z}_4 is $[2]_4$ een nuldeler, want $[2]_4 \cdot [2]_4 = [0]_4$.

Eigenschap 1.23. (Schrappingswet) Veronderstel een commutatieve ring R en $a \in R$ noch nul, noch een nuldeler. Dan geldt voor alle $b, c \in R$ dat $ab = ac$ impliceert dat $b = c$.

Bewijs. De vergelijking $ab = ac$ leidt tot $a(b - c) = 0$. Aangezien $a \neq 0$ en aangezien a geen nuldeler is, volgt $b - c = 0$ en dus $b = c$. \square

↳ de o.a niet van b-c kaner, want is geen nuldeler

Definitie 1.25. Veronderstel een commutatieve ring R met eenheidselement. Een element $a \in R$ wordt **inverteerbaar** of **regulier** genoemd indien er een $b \in R$ bestaat zodat $ab = 1$.

Eigenschap 1.24. Veronderstel een commutatieve ring R met eenheidselement en een element $a \in R$. Indien a inverteerbaar is, is a geen nuldeler.

Bewijs. Indien er een b zou bestaan zodat $a \cdot b = 0$ dan zou vermenigvuldiging van beide leden met a^{-1} leiden tot $b = 0$. Daaruit volgt dat a geen nuldeler kan zijn. \square

↳ a.a⁻¹.b = 0.a⁻¹ = 0 \Rightarrow 1.b = 0 \Rightarrow b = 0

Indien a inverteerbaar is, kan a dus geen nuldeler zijn. Het omgekeerde is echter niet noodzakelijk waar, zoals volgend voorbeeld aangeeft. \rightarrow het niet omdat het niet inverteerbaar is, dat het een nuldeler is

Voorbeeld 1.13. De ring $(\mathbb{Z}, +, \cdot)$ bevat geen nuldelers. Toch zijn enkel de elementen -1 en 1 inverteerbaar. $\hookrightarrow \mathbb{Z} = \text{gehele getallen} : 1 \cdot 1 = 1, -1 \cdot -1 = 1$, maar $2 \cdot \frac{1}{2} \neq 1$

We hebben wel de volgende belangrijke eigenschap.

Eigenschap 1.25. Veronderstel een **eindige** commutatieve ring R met eenheidselement. Indien $a \in R \setminus \{0\}$ geen nuldeler is, is a inverteerbaar. \rightarrow gaat niet tegen. voor 1.13, want R moet eindig zijn: \mathbb{Z} is ipo- \mathbb{Z}

Bewijs. We moeten bewijzen dat een willekeurige niet-nuldeler a ($\neq 0$) een inverse heeft. Beschouw de producten $a \cdot r \in R$ voor alle $r \in R$. Indien $r_1 \neq r_2$, dan is $ar_1 \neq ar_2$. Dit volgt rechtstreeks uit de schrappingswet (eigenschap 1.23). Aangezien er $|R|$ verschillende mogelijkheden zijn voor r (met $|R|$ het aantal elementen in R), zijn er ook $|R|$ verschillende mogelijkheden voor ar . Aangezien R eindig is, wil dit zeggen dat 1 ook één van de mogelijkheden van ar is. Er bestaat bijgevolg een $r \in R$, zodat $ar = 1$, en deze r is de inverse van a . \square