Relaties en Structuren

Ludovic Marchand

December 18, 2012

Gebruikte afkortingen: verz $\rightsquigarrow$ verzameling, elt(en) $\rightsquigarrow$ element(en)

1 Elementen van de verzamelingenleer

1.1 Enkele basisbegrippen

Definitie 1.1 *Enkele (deel)verzamelingen van verzamelingen A en B:*
$\rightsquigarrow$ *doorsnede* $[\cap]$, *unie* $[\cup]$, *deelverzameling* $[\subset]$, *(symmetrisch* $[\triangle]$*) verschil* $[\setminus]$

Stelling 1.2 *Stel A, B, C verz, dan gelden volgende eig;*
commutatief $[C]$, *associatief* $[A]$, *distributief* $[D]$, *De Morgan (machten)*

1.2 Relaties

1.2.1 Basisdefinities

Definitie 1.3 *Stel* $a \in A, b \in B$, *dan is het koppel (a,b) (*$\neq$ *(b,a))*

- *Carthesisch product (of productverz): verz* $A \times B := \{(a,b) || a \in A, b \in B\}$
- *Samenst opeenv koppels:* $(a,b) \subset A \times B$, $(b,c) \subset B \times C$ *dan* $(a,c) \subset A \times C$
- *Een relatie is een deelverz (v koppels) van* $A \times B$
- *Stel relatie* $\Re \subset A \times B$, *de inverse relatie is* $\Re^{-1} := \{(b,a) || (a,b) \in \Re\}$
- *Samengestelde relatie* $\Re_2 \circ \Re_1$ $(:= \Gamma)$ *v* $\Re_1 \subset A \times B$ *en* $\Re_2 \subset A \times B$*:*
  $\Gamma := \{(a,c) || \exists\, b \in B : (a,b) \in \Re_1$ *en* $(b,c) \in \Re_2 \quad \rightsquigarrow \quad (\Gamma)^{-1} = \Re_1^{-1} \circ \Re_2^{-1}$
- *Restrictie: stel* $\Re$ *relatie van A nr B,* $C \subset A$ & $D \subset B$ *dan heet*
  $\Re \cap (C \times D)$ *de beperking van* $\Re$ *tot* $(C \times D)$*, genoteerd als* $\Re_{|C \times D}$

1.2.2 Classificatie soorten relaties

naar definitieverzameling

- Een functie f van A nr B : er vertrekt maximum 1 pijl
- Een afbeelding g van A nr B : er vertrekt precies 1 pijl $\rightsquigarrow$ Elke afbeelding is dus een functie
- Een transformatie: afbeelding van A naar A

naar beeldverzameling

- Relatie is injectief $\Leftrightarrow \quad f(a) = f(a') \Rightarrow a = a', \ \forall\, a, a' \in A$
- Relatie is surjectief $\Leftrightarrow \quad \exists\, a \in A : f(a) = b, \ \forall\, b \in B$
- Relatie is bijectief $\Leftrightarrow \quad \exists\, a \in A$ (uniek!) $: f(a) = b, \ \forall\, b \in B$

naar inhoud

- Een relatie $\Re \subset A^2$ is reflexief $\Leftrightarrow \{(x,x)||x \in A\} \subset \Re$
- Een relatie $\Re \subset A^2$ is antireflexief $\Leftrightarrow \{(x,x)||x \in A\} \cap \Re = 0$
- Een relatie $\Re \subset A^2$ is symmetrisch $\Leftrightarrow (x,y) \in \Re \Rightarrow (y,x) \in \Re,\ \forall x,y \in A$
- Een relatie $\Re \subset A^2$ is antisymm $\Leftrightarrow (x,y) \in \Re \Rightarrow (y,x) \notin \Re,\ \forall (x \neq y) \in A$
- Een relatie $\Re \subset A^2$ is transitief $\Leftrightarrow (x,y),(y,z) \in \Re \Rightarrow (x,z) \in \Re,\ \forall x,y,z \in A$

Combinaties

- $\Re \subset A^2$ is een partiële orderelatie $\Leftrightarrow \Re$ reflexief, antisymm en transitief is.
- $\Re \subset A^2$ is een totale orderelatie $\Leftrightarrow \Re$ is partieel en symmetrisch
- $\Re \subset A^2$ is een strikt-orderelatie $\Leftrightarrow \Re$ antireflexief en transitief is.
- $\Re \subset A^2$ is een equivalentierelatie $\Leftrightarrow \Re$ reflexief, symm en transitief is. $\sim$ partitie

1.3 De getallenverzamelingen $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ en $\mathbb{C}$

Leopold Kronecker (1823 - 1891): "*God schiep de* ***natuurlijke getallen*** *en de rest is werk van de mens*"
$\rightsquigarrow$ origineel: "*Die* ***ganzen Zahlen*** *hat der liebe Gott gemacht, alles andere ist Menschenwerk*"

Definitie 1.4 $\mathbb{N} \twoheadrightarrow \mathbb{Z} \twoheadrightarrow \mathbb{Q} \twoheadrightarrow \mathbb{R} \twoheadrightarrow \mathbb{C}$

Axioma 1 *Als $X(\neq \varnothing)$ een deelverzameling is van $\mathbb{Z}, \mathbb{N}$ of $\mathbb{N}^*$, dan bezit X een kleinste element.*

1.4 Het inductieprincipe

Stelling 1.5 *Stel $S \subseteq \mathbb{N}^*$, een deelverz waarvoor een bepaalde uitdrukking waar is en die voldoet aan:*
(1) $1 \in S$ (2) $\forall k \in \mathbb{N}^*$ *: $k \in S$ impliceert $k+1 \in S$*
$\Rightarrow$ *Dan is $S = \mathbb{N}^*$*

1.5 Het ladenprincipe van Dirichlet

Stelling 1.6 *(ladenprincipe Dirichlet):*
Indien m objecten verdeeld moeten worden over n lade, dan zal minstens 1 lade meer dan 1 object bevatten indien er meer objecten zijn dan laden, dus $m > n$

1.6 Eindige, oneindige, aftelbare, niet-aftelbare verzamelingen

Definitie 1.7 *Een verzameling X, zodanig dat er een bijectie bestaat van $\mathbb{N}[1,n]$ naar X, wordt een eindige verz genoemd. We noemen n de orde van X. Elke niet eindige verzameling wordt een oneindige verz genoemd.*

Stelling 1.8 *Elke $X(\neq \varnothing)$ is een oneindige verz $\Leftrightarrow \exists$ injectie van $\mathbb{N}^*$ naar X*

Definitie 1.9 *Een oneindige verz X is aftelbaar, als $\exists$ bijectie van $\mathbb{N}$ (of $\mathbb{N}^*$) op X. Zoniet is X een niet-aftelbare verzameling.*

Stelling 1.10 *$\mathbb{Z}$ is aftelbaar, $\mathbb{Q}$ is aftelbaar maar $\mathbb{R}$ is over-aftelbaar*

Stelling 1.11 *Stel $A \rightarrow \mathbb{N}[1,n]$ bijectie, dan is n het kardinaalgetal van A (not $|A|$)*

1.7 Het somprincipe

Stelling 1.12 *Als $A_i (i = 1 \dots k)$ k 2 aan 2 disjuncte ($\cap = \varnothing$),*
eindige verzamelingen zijn, dan is $|A_1 \cup A_2 \cup \dots \cup A_k| = \sum_{i=1}^{k} |A_i|$

Stelling 1.13 *(ladenprincipe, algemene vorm):*
Indien m objecten over n laden moeten verdeeld worden waarbij $m > nr$, dan is er tenminste één lade die meer dan r objecten bevat.

2 Elementaire logica

3 Getaltheorie

3.1 Deelbaarheid en ggd

Definitie 3.1 *Deelbaarheid in $\mathbb{Z}$ is een relatie $\varphi \subset \mathbb{Z}\backslash\{0\} \times \mathbb{Z}$ gedefinieerd door*
$(a, b) \in \varphi \Leftrightarrow \exists\, q \in \mathbb{Z} : b = a \cdot q$
waarbij φ deelbaarheidsrelatie, b een a-voud en indien $(a, b) \in \varphi \overset{not}{\to} a|b$

Lemma 3.2 *$\forall a, b, c, m, n \in \mathbb{Z}$ geldt:*

- *$a|b$ en $a|c \Rightarrow a|(b + c)$*
- *$a|b \Rightarrow a|bc$*
- *$a|m$ en $b|n \Rightarrow ab|mn$*

Gevolg 3.3 *Stel $a|b$ en $a|c$, dan $\forall x, y \in \mathbb{Z}$ geldt $a|(bx + cy)$*

Lemma 3.4 *De deelbaarheidsrelatie beperkt tot $(\mathbb{Z} \times \mathbb{Z}) \backslash\{(0, 0)\}$ is reflexief en transitief*

Stelling 3.5 *$\forall a \in \mathbb{Z}\backslash\{0\}, b \in \mathbb{Z} \exists$ unieke q(uotiënt) en r(est) zodanig dat*
$b = a \cdot q + r$ en $0 \leq r < |a|$

Definitie 3.6 *Een getal $c \in \mathbb{Z}$ is een grootste gemene deler van a en b $\Leftrightarrow$*
elke gemene deler van a en b is een deler van c.

Lemma 3.7 *Als a en b twee ggd's zijn van 2 gehele getallen,*
dan geldt $a = b$ of $a = -b$

Definitie 3.8 *De grootste gem deler van a en b is de unieke positieve onder de ggd's van a en b*

Lemma 3.9 *Stel $a, b, q, r \in \mathbb{Z}$, met $a = bq + r$. Dan geldt ggd(a,b) = ggd(b,r)*

$\rightsquigarrow$ (uitgebreid) Algoritme van Euclides.

Stelling 3.10 *Stel $a, b \in \mathbb{Z}$ (niet beide nul) en dat $d = ggd(a, b)$, dan bepaalt*
uitgebreid algoritme, $m, n \in \mathbb{Z}$ zodanig dat $am + bn = d$, tenzij $b|a$
$\rightsquigarrow$ m,n zijn Bézout-coëfficiënten en niet uniek bepaald

Gevolg 3.11

- *Stel ggd(a,b) = 1, dan geldt $a|b \cdot c \Rightarrow a|c$*
- *Stel $a|m$, $b|m$ en ggd(a,b) = 1, dan geldt $a \cdot b|m$*

Definitie 3.12 *Een getal $c \in \mathbb{Z}$ is een kgv van a en b $\Leftrightarrow$ elk gemeen veelvoud van a en b is veelvoud van c.*
Het kgv van a en b is het unieke positieve onder de kgv's van a en b

Stelling 3.13 $\rightsquigarrow$ *nog wat meer eigenschappen van de ggd en het kgv*

- *Stel a,b,c* $\in \mathbb{N}$ *en ac, bc niet beide nul, dan is ggd(ca,cb) = c ggd(a,b)*
- *Stel* $c|a$ *en* $c|b$*, dan is* $c|\frac{ab}{ggd(a,b)}$
- *Stel* $a, b \in \mathbb{N}$*, dan is* $kgv(a,b) \cdot ggd(a,b) = ab$
- *Stel hetzij ab, ac of bc onderling ondeelbaar, dan geldt ggd(a,c) · ggd(b,c) = ggd(ab,c) Bijgevolg is* $ggd(ab,c) = 1 \Leftrightarrow ggd(a,c)$ *en* $ggd(b,c) = 1$*, a,b zijn copriem.*
- *Stel a,b* $\in \mathbb{Z}$ *en* $ax + by = c$*, dan is ggd(a,b)/c*

3.2 Priemgetallen

Definitie 3.14 *Een* $p \in \mathbb{Z}$ *is een priemgetal als p juist 2* ***positieve*** *delers heeft. (1 en zichzelf)* $\rightsquigarrow$ *verdere notatie: p is priemgetal.*

Stelling 3.15 *(Euclides): Deze verz van de priemgetallen is en oneindige verzameling*

Lemma 3.16 *Stel* $p|ab$*, dan* $p|a$ *of* $p|b \quad \forall a, b \in \mathbb{Z}$

Gevolg 3.17 *Indien* $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ *zodanig dat* $p \mid \prod_{i=1}^{n} x_i$*,*
dan is p een deler van tenminste 1 x_i*,* $i \in \mathbb{N}[1,n]$

Stelling 3.18 *(Hoofdstelling van de rekenkunde (Euclides)):*
Elke $n \in \mathbb{N}\backslash\{0,1\}$ *is te schrijven als een product van priemfactoren.*
Op de volgorde na is deze ontbinding uniek.

$\rightsquigarrow$ De zeef van Erasthotenes: veelvouden van p.

3.2.1 Priemelementen in $\mathbb{Z}$

Definitie 3.19 *Een priemelement in* $\mathbb{Z}$ *is ofwel een p ofwel ofwel* $p \cdot (-1)$

Stelling 3.20 *Elke* $z \in \mathbb{Z}\backslash\{-1,0,1\}$ *is te schrijven als product van priemelementen.*
Op de volgorde en het teken na, is deze ontbinding in priemelementen uniek.

Stelling 3.21 *Elke rationale oplossing* x_0 *van de vergelijking:*
$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0$ $a_0, a_n \neq 0$ *is van de vorm* $x_0 = p/q$*,*
voor zekere $p|a_n$ *en* $q|a_0$*. ihb als* $a_0 = 1$ *dan is* $x_0 \in \mathbb{Z}$

3.3 De Eulerfunctie ϱ (Leonhard Euler - 1707-1783)

We noteren $\varrho(n)$ voor het aantal elementen uit $\mathbb{N}[1,n]$ dat copriem is met n.
Indien $n = p$, dan is duidelijk $\varrho(p) = p - 1$
$\rightsquigarrow$ nu 2 lemma's voor algemene n

Lemma 3.22 *stel* $e \geq 1$*, dan geldt* $\varrho(p^e) = p^{e-1}(p-1)$

Lemma 3.23 *stel* $m, n \in \mathbb{N}$ *en* $ggd(m,n) = 1$ *dan is* $\varrho(mn) = \varrho(m)\varrho(n)$

Stelling 3.24 *Stel* $2 \leq n \in \mathbb{N}$ *met priemfactorontbinding* $p_1^{e_1}p_2^{e_2}\ldots p_k^{e_k}$*, dan is*

$$\begin{aligned} \varrho(n) = & \quad n(1-\tfrac{1}{p_1})(1-\tfrac{1}{p_2})\ldots(1-\tfrac{1}{p_k}) \\ = & \quad p_1^{e_1-1}(p_1-1)p_2^{e_2-1}(p_2-1)\ldots p_k^{e_k-1}(p_k-1) \end{aligned}$$

Stelling 3.25 $\forall n \in \mathbb{N}$*, geldt* $\sum_{d|n} \varrho(d) = n$*.*
Hierbij wordt gesomeerd over al de mogelijke delers van n.

4 Modulair rekenen

4.1 Congruentie

Definitie 4.1
- *Stel $x_1, x_2 \in \mathbb{Z}$ en $m \in \mathbb{N}^+$,*
  dan zijn x_1 en x_2 congruent modulo $m \Leftrightarrow m|(x_1 - x_2)$, We noteren:

$$x_1 \equiv x_2 \ (mod\ m) \Leftrightarrow x_1 - x_2 = m \cdot t$$

- *De verzameling van de restklassen modulo $m := \mathbb{Z}_m$, neemt men de kleinste representant, dan ontstaat $\mathbb{N}[0, m-1]$; Deze verz is bijectief met $\mathbb{Z}_m$.*

Lemma 4.2 *De relatie congruent modulo m is een equivalentierelatie met m restklassen.*

Stelling 4.3 *Stel $x_1 \equiv x_2 \ (mod\ m)$, $y_1 \equiv y_2 \ (mod\ m)$ $m \in \mathbb{N}^+$ en $x_i, y_i \in \mathbb{Z}$*

$$\text{Dan geldt} \qquad \begin{aligned} x_1 + y_1 &\equiv x_2 + y_2 \ (mod\ m) \\ x_1 y_1 &\equiv x_2 y_2 \ (mod\ m) \end{aligned}$$

$\rightsquigarrow$ *Goed gefeffinieerde optelling en vermenigvuldiging in $\mathbb{Z}_m$*

Lemma 4.4 *Stel $(x_n x_{n-1} \dots x_2 x_1 x_0)_{10}$ de voorstelling is van x in basis 10.*
Dan geldt $x \equiv \sum_{i=0}^{n} x_i \ (mod\ 9)$ $\rightsquigarrow$ *negenproef*

4.2 Optelling en vermenigvuldiging in $\mathbb{Z}_m$

Definitie 4.5
$$\begin{aligned} [x]_m \oplus [y]_m &= [x + y]_m \\ [x]_m \otimes [y]_m &= [x \times y]_m \end{aligned}$$
Met $\otimes$ inwendig, commutatief, associatief en neutraal element
en $\oplus$ zelfde eig, maar $\oplus$ heeft ook nog invers element.
Tenslotte is er nog de distributiviteit van verm tov opt $\rightsquigarrow \mathbb{Z}_m, \oplus, \otimes$ is een ring.

De schrappingswet voor de verm geldt niet in $\mathbb{Z}_m$
Het is mogelijk dat $[a]_m \otimes [b]_m = [0]_m$ terwijl $[a]_m, [b]_m \neq [0]_m$.
Deze klassen met a een echte deler van m, heten nuldelers in $\mathbb{Z}_m$.
Indien $m = p$, dan bezit $\mathbb{Z}_p$ geen nuldelers
not.: $[a]_m \oplus [b]_m \rightarrow$ (a + b) (mod m) en $[a]_m \otimes [b]_m \rightarrow$ ab (mod m).

4.3 Inverteerbare elementen in $\mathbb{Z}_m$

Definitie 4.6 *Een $r \in \mathbb{Z}_m$ wordt inverteerbaar genoemd als $\exists\, x \in \mathbb{Z}_m$*
zodanig dat $rx = 1$ in $\mathbb{Z}_m$, maw indien $rx \equiv 1 \ (mod\ m)$. not. $x = r^{-1}$

Stelling 4.7 *$r \in \mathbb{Z}_m$ is inverteerbaar $\Leftrightarrow ggd(r, m) = 1$.*
ihb is in $\mathbb{Z}_p$, elk element verschillend van 0 inverteerbaar.

Stelling 4.8 *(Stelling van Euler):*

$$y^{\varrho(m)} \equiv 1 \ (mod\ m), \quad als\ ggd(y,m) = 1$$

Gevolg 4.9 *(Kleine stelling van Fermat): Stel $p \nmid y$*

$$\begin{aligned} y^{p-1} &\equiv 1 \ (mod\ p) \\ \Leftrightarrow y^p &\equiv y \ (mod\ p) \end{aligned}$$

Gevolg 4.10 *$\forall n \in \mathbb{N}$ geldt $n^p \equiv n \ (mod\ p)$.*
$\rightsquigarrow n$ en n^5 eidigen steeds op dezelfde letter.

4.4 Lineaire congruenties ($ax \equiv b$(mod m))

Stelling 4.11
- *Als d = ggd(a, m) ∤ b, dan bezit $ax \equiv b$ (mod m) geen oplossingen*
- *Als d | b, dan bezit $ax \equiv b$ (mod m) juist d oplossingen $\in \mathbb{N}[0, m-1]$*
  Opmerking: Is ggd(a, m) = 1, dan is er één oplossing.

Toepassing 4.12 *Oplossingsmethode:*
Indien d een deler is van b, d > 1 (anders geen oplossingen of 1 opl),
moet de congruentie (incl. mod) gedeeld worden door d. Veronderstel dat dit gebeurd is,
dan schrijven we de lin congruentie in de vorm $ax \equiv (b + tm)$ (mod m) met b + tm
een veelvoud van a. De oplossing(en) zijn dan van de vorm $\frac{b+tm}{a}$ (mod m) t ∈ [0, d-1].
⇒ Zo kan men ook lin diophantische vergelijkingen oplossen vd vorm ax + by = c ∈ ℤ adhv stelsels

4.5 De stelling van Wilson en toepassingen

Stelling 4.13 *(Stelling van Wilson): Als p priemgetal, dan*

$$(p-1)! \equiv -1 \pmod{p}$$

Stelling 4.14 *Stel p oneven priem, dan ∃ $a \in \mathbb{Z}_p$ waarvoor*
$a^2 \equiv -1$ (mod p) ⇔ $p \equiv 1$ (mod 4)

4.6 Stelsels lineaire congruenties

Definitie 4.15 *We zoeken oplossingen van de stelsels vergelijkingen vd vorm*

$$a_i x \equiv b_i \pmod{m_i}, \quad i = 1, \ldots, k, \quad ggd(a_i, m_i) | b_i$$

die altijd kunnen herleid worden tot

$$x \equiv b_i \pmod{m_i}, \quad b_i \in \mathbb{N}[0, m_i - 1], \quad i = 1, \ldots, k \tag{1}$$

Stelling 4.16 *(Chinese reststelling): stelsel (1) met* ***ggd(m_i, m_j) = 1 als $i \neq j$***
bezit juist 1 oplossing modulo $M = \prod_{i=1}^{k} m_i$

Toepassing 4.17 *Werkwijze: het bestaat erin een oplossing te zoeken vd vorm*

$$x = \sum_{i=1}^{k} b_i \, m^{(i)} \, y_i, \quad met \, m^{(i)} = \frac{\prod_{j=1}^{k} m_j}{m_i}$$

het stelsel herleid zich dan tot een stelsel vd vorm

$$y_i \, m^{(i)} \equiv 1 \pmod{m_i}, \quad y_i \in \mathbb{N}[0, m_i - 1], \quad i = 1, \ldots, k$$

door het algoritme van Euclides kunnen alle y_i gevonden worden
welke nadien gesubstitueert kunnen worden in x.

Opmerking: Indien het stelsel bestaat uit 2 congruenties, dan is x = $b_1 m_2 y_1 + b_2 m_1 y_2$

4.7 Primitieve wortels

Definitie 4.18 *De orde van a modulo m is de kleinste $t \in \mathbb{N}$ waarvoor $a^t \equiv 1 \pmod m$*

Stelling 4.19 *Veronderstel dat ggd(a, m) = 1 en dat a de orde t bezit modulo m,*
dan is $a^n \equiv 1 \pmod m \Leftrightarrow$ als n een veelvoud is van t

Gevolg 4.20 *Stel ggd(a,m) = 1 en a heeft orde t mod m dan*

- *is t een deler van $\varphi(m)$*
- $a^r \equiv a^s \pmod m \Leftrightarrow r \equiv s \pmod t$

Definitie 4.21 *Een primitieve wortel van m is een element $a \in \mathbb{Z}_m$*
waarvoor ggd(a, m) = 1 en waarvan de orde gelijk is aan $\varphi(m)$

Stelling 4.22 *Als g een primitieve wortel is van m, dan zijn de resten modulo m van $g, g^2, \ldots, g^{\varphi(m)}$*
de $\varphi(m)$ natuurlijke getallen uit $\mathbb{N}[1, m-1]$ die copriem zijn met m

Stelling 4.23 *Veronderstel dat a de orde t heeft modulo m (ggd(a, m) = 1), dan*
zal a^k eveneens de orde t modulo m hebben $\Leftrightarrow$ ggd(k, t) = 1

Stelling 4.24 *Elk priemgetal p bezit juist (p - 1) primitieve wortels.*
Indien g een primitieve wortel is van p, dan is de verzameling $\{g^k \pmod p : ggd(k, p-1) = 1\}$,
de verzameling vd primitieve wortels van p.

4.8 Kwadratische congruenties

Definitie 4.25 *Men zoekt een oplossing van $ax^2 + bx + c \equiv 0 \pmod p$*

$$y^2 \equiv \frac{b^2 - 4ac}{4a^2} \pmod p \quad \text{met } y = x + \frac{a^{-1}b}{2}$$

Het hangt er dus vanaf of de noemer vh rechterlid een kwadraat is modulo p.
Vandaar enkel oplossingen van congruenties vd vorm

$$x^2 \equiv a \pmod p \tag{2}$$

Indien (geen) oplossing, dan is a kwadratische (niet-)rest modulo p.

Stelling 4.26 *Stel p een oneven priemgetal en $a \neq 0 \pmod p$, dan*
bezit $x^2 \equiv a \pmod p$ juist 2 of geen oplossingen.
Indien p geen priemgetal kan het ontbonden worden in priemgetallen waardoor meerdere oplossingen

Stelling 4.27 *(Criterium van Euler):*
Stel p een oneven priemgetal en $p \nmid a$ dan heeft (2)

- *2 oplossingen als $a^{\frac{p-1}{2}} \equiv 1 \pmod p$;*
  van de gedaante $x \equiv g^m$ en $x \equiv p - g^m \pmod p$ met g primitieve wortel en $a \equiv g^{2m} \pmod p$
- *0 oplossingen als $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.*

4.9 Het Legendre symbool

Definitie 4.28 $\left[\frac{a}{p}\right] = \begin{cases} 1 & \textit{als } a \textit{ een kwadratische rest modulo } p \textit{ is} \\ 0 & \textit{als } p/a \\ -1 & \textit{als } a \textit{ een kwadratische niet-rest modulo } p \textit{ is} \end{cases}$

Lemma 4.29 *Stel g een primitieve wortel en p een oneven priemgetal, dan*

$$\left[\frac{g^r}{p}\right] = (-1)^r$$

Stelling 4.30 *Het Legendre symbool* $\left[\frac{a}{p}\right]$ *bezit volgende eigenschappen met p,q oneven*

- *Als* $a \equiv b$ *(mod p), dan is* $\left[\frac{a}{p}\right] = \left[\frac{b}{p}\right]$
- $\left[\frac{a^2}{p}\right] = \left[\frac{a}{p}\right]^2$
- $\left[\frac{ab}{p}\right] = \left[\frac{a}{p}\right] \cdot \left[\frac{b}{p}\right]$
- *(Kwadratische wederkerigheidsstelling):*
  als $p \equiv q \equiv 3$ *(mod 4), dan is* $\left[\frac{p}{q}\right] = -\left[\frac{q}{p}\right]$
  zoniet zijn ze gelijk zonder minteken.
- *Indien* $a > p$*, dan is* $\left[\frac{a}{p}\right] = \left[\frac{an+r}{p}\right] = \left[\frac{r}{p}\right]$

Stelling 4.31 *Men kan bewijzen dat* ***elk*** *willekeurig Legendre symbool (p priem) uiteindelijk herleid wordt tot de 2 Legendresymbolen* $\left[\frac{-1}{p}\right]$ *en* $\left[\frac{2}{p}\right]$
Voor deze geldt:

- $\left[\frac{-1}{p}\right] = +1 \Leftrightarrow -1 \equiv a^2 \pmod p \Leftrightarrow p \equiv 1 \pmod 4$
  $\left[\frac{-1}{p}\right] = -1 \Leftrightarrow -1 \not\equiv a^2 \pmod p \Leftrightarrow p \equiv 3 \pmod 4$
- $\left[\frac{2}{p}\right] = +1 \Leftrightarrow p \equiv \pm 1 \pmod 8$
  $\left[\frac{2}{p}\right] = -1 \Leftrightarrow p \equiv \pm 3 \pmod 8$

Indien na uitrekenen $\left[\frac{a}{p}\right] = 1$, dan lost men de congruentie op door de gegeven a te sommeren met p totdat het verkregen getal een kwadraat is zodat men 2 oplossingen vindt voor x.

5 H5: Inleiding tot de groepentheorie

5.1 Enkele veralgemeningen

Definitie 5.1 *Een binaire bewerking op verz V;* $f: V \times V \to V : (a,b) \mapsto f((a, b))$
vb: additieve, multiplicatieve bewerking op getallenverzamelingen; vb $(2,5) \mapsto (2 +,\cdot\ 5)$

Definitie 5.2 *Een (abelse of commutatieve) groep is een koppel* $(G(verz),\cdot)$
die associatief [A] (, bijkomend commutatief [C]) is, en het neutraal [N] en invers [I] element bevat

Toepassing 5.3 *Stel* $G = \{e,a,b,c\}$*, we definiëren een binaire bewerking* $\Diamond$ *in G adhv Cayley tabel*

$\Diamond$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Deze groep heet de Viergroep van Klein

Lemma 5.4 $\mathbb{Z}_m \backslash \{0\}, \otimes$ *is een abelse groep* $\Leftrightarrow$ *m is priemgetal*

Definitie 5.5 *De orde van een groep is het aantal elementen van de verzameling*

5.2 Enkele eigenschappen

Stelling 5.6 *In een groep G,·*

- *geldt de linkse en rechtse schrappingswet (want inverse bestaat)*
- *is het neutraal en invers element uniek*
- *heeft de vergelijking xa = b juist 1 oplossing, nl* $x = ba^{-1}$

5.3 Groepmorfismen

Definitie 5.7 *Een homomorfisme van G,· in G',×*
is een afbeelding $\theta : G \to G' : a \cdot b \mapsto a \times b$

Definitie 5.8 *Is het homomorfisme θ*

injectief		*monomorfisme*
surjectief	*dan is het meerbepaald een*	*epimorfisme*
bijectief		*isomorfisme*

Een isomorfisme van G,· op zichzelf heet een automorfisme van G,·

Stelling 5.9 *Stel θ, dan is* $\theta(e)$ *en* $\theta(a^{-1})$ *resp het neutraal en invers element in G',×*

5.4 Deelgroepen

Definitie 5.10 *Stel G' ⊂ G een deelverz van G, dan is G',· een deelgroep* $(\leq) \Leftrightarrow$ *G',· is een groep*

Stelling 5.11 *(Criterium voor deelgroepen):*
Stel G' ⊂ G, dan is G',· $\leq$ *G,·* $\Leftrightarrow \forall$ *a,b* $\in$ *G' :* $ab^{-1} \in$ *G'*

Lemma 5.12 *Stel (G',·), (G",·)* $\leq$ *(G,·), dan is*

- *(G',·* $\cap$ *G",·) terug* $\leq$ *(G,·)*
- *(G',·* $\cup$ *G",·) over het algemeen* $\not\leq$ *(G,·)*

Definitie 5.13 *Stel θ is een homomorfisme van G,· in G,×.*

Het beeld van θ	:=	*im(θ)*	:= $\{\theta(x) : x \in G\}$	$\leq G'$
De kern van θ	:=	*ker(θ)*	:= $\{x \in G : \theta(x) = e'\}$	$\leq G$

5.5 Nevenklassen van een deelgroep

Definitie 5.14 *Als H,·* $\leq$ *G,·* $\forall$ $a \in G$, *dan zijn*
$aH = \{ah : h \in H\}$ *en* $Ha = \{ha : h \in H\}$ *resp. linkse en rechtse nevenklassen van H in G*

Stelling 5.15 *Deze linkse resp. rechtse nevenklasse vormt een partitie van G.*

Stelling 5.16 *(Stelling van Lagrange): Stel H* $\leq$ *(eindige groep) G*
dan is de orde van H een deler van de orde van G

Definitie 5.17 *Stel H* $\leq$ *G, het getal* $\dfrac{|G|}{|H|}$ *heet de index van H in G*

5.6 Cyclische groepen

Definitie 5.18 *Stel $D \subset G$, indien elk element van G geschreven kan worden als het product van elementen (+ inverses) uit D, dan zijn de elementen van D de generatoren of voortbrengers van G*

Definitie 5.19 *G is een cyclische groep als het voortgebracht wordt door één element,*

- *G, $\times = \langle x \rangle = \{e, x, x^2, \ldots, x^{m-1}\}$ $m :=$ kleinste $\in \mathbb{N}^+$ waarvoor $x^m = e$*
  Indien $\nexists$ m dan is $\langle x \rangle$ een oneindige groep
- *G, $+ = \langle x \rangle = \{-nx, \ldots, -2x, x, -e, 0, e, x, 2x, \ldots, nx\}$*

Stel $x \in G$, dan brengt x een cyclische groep voort die $\leq G$.
De orde van $\langle x \rangle$ is de orde van x, welke een deler is van de orde van G

Stelling 5.20 *Elke eindige cyclische groep van de orde m is isomorf met $\mathbb{Z}_m, \oplus$*
Elke oneindige cyclische groep is isomorf met $\mathbb{Z}$, +

Gevolg 5.21 *Elke twee cyclische gropeen van dezelfde orde zijn isomorf*

Notatie: cyclische groep van de orde m := C_m, gewoonlijk enkel multiplicatieve bewerking

Stelling 5.22 *Elke eindige groep waarvan de orde een priemgetal is, is een cyclische groep*

Stelling 5.23 *Er bestaan op isomorfismen na juist 2 groepen van de orde 4*

Stelling 5.24 *Stel een cyclische groep $C_n = \langle g \rangle$ van de orde n*
Voor elke d|n is er juist 1 deelgroep van orde d,
bovendien is dit een cyclische groep $\langle g^k \rangle$ met $k = \dfrac{n}{d}$

5.7 Het direct product van groepen

Definitie 5.25 *Stel A, $*$ en B, $\circledcirc$ 2 groepen.*
Definieer een bewerking $\cdot$ op $A \times B$ als volgt $(a_1, b_1) \cdot (a_2, b_2) = (a_1 * a_2, b_1 \circledcirc b_2)$
De groep $A \times B$, $\cdot$ heet het carthesisch product van de groepen A en B

Stelling 5.26 *Stel m,n copriem, dan is $C_m \times C_n \cong C_{mn}$*

5.8 Permutatiegroepen

Definitie 5.27 *Stel $X = \mathbb{N}[1, n]$,*

- *een permutatie van X is een bijectie van X op zichzelf*
- *S_n is dan de groep van alle permutaties op n elementen,*
- *elke deelgroep (met orde m) wordt een permutatiegroep (van orde m) genoemd*
- *Elke permutatie (element) van S_n kan beschreven worden als een stelsel van n betrekkingen van de vorm f(i) = $j \in \mathbb{N}[1, n]$ met $f(i_1) = f(i_2) \Leftrightarrow i_1 = i_2$*

Toepassing 5.28 *Om deze permutaties eenvoudig neer te schrijven maakt men gebruik van de zogenaamde cykelvoorstelling vb: $S_3 = \{(1)(2)(3), (123), (132), (1)(23), (2)(13), (3)(12)\}$*
Merk op dat de volgorde van de cykels geen rol speelt,
maar is binnenin een cykel het eerste element gekozen, dan liggen de andere elementen vast.

Stelling 5.29 *De samenstelling $\circ$ van permutaties vormt weer een permutatie, die voldoet aan de gewone rekenregels voor de samenstelling van relaties.*
Zo geldt bvb in S_3 dat (1)(23) $\circ$ (123) = (13)(2),
*zo'n samenstelling moet gelezen worden van rechts naar links met $\circ$ = **dan!!***

Definitie 5.30 *Een permutatie van $\mathbb{N}[1,n]$ die 2 elementen verwisselt en de andere elementen fixeert, heet een transpositie van $\mathbb{N}[1,n]$*

Stelling 5.31 *Elke cykel kan worden geschreven als een samenstelling van transposities:*

$$(x_1x_2\dots x_{r-1}x_r) = (x_1x_r)\circ(x_1x_{r-1})\circ\dots\circ(x_1x_3)\circ(x_1x_2)$$

Merk op dat zo'n ontbinding niet uniek is

Stelling 5.32 *(Pariteit van aantal transposities): Stel dat $\alpha \in S_n$ kan worden geschreven als een samenstelling van r en r' transposities. Dan zijn r, r' beide (on)even*

Gevolg 5.33

- *Permutaties zijn in te delen in 2 partities, nl de even of oneven.*
- *De samenstelling van 2 (on)even permutaties is terug even*
- *De alternerende groep, A_n of Alt(n), is de deelgroep van de even permutaties voor de samenstelling*
- *Stel σ oneven permutatie, dan is de nevenklasse σA_n de verzameling vd oneven permutaties*
- *Bijgevolg is $S_n = A_n \cup \sigma A_n$, beide even groot nl orde $\frac{n!}{2}$*

Opmerking: Het epimorfisme $\theta : S_n, \circ \to \{-1,1\}, \cdot : \begin{cases} A_n \to 1 \\ \sigma A_n \to -1 \end{cases}$
wordt de Sign-afbeelding genoemd. Met $\ker(\theta) = A_n$

6 H6 : Ringen, lichamen en velden

6.1 Ringen

Definitie 6.1 *Een ring is een verzameling R, voorzien van 2 binaire bewerking (+, ·) waarvoor geldt: R, + is een abelse groep, · is associatief, · is (links/rechts) distributief tov de optelling*

Definitie 6.2 *Als $R\backslash\{0\}, \cdot$ aan voorwaarde [N] of [C] voldoet, dan wordt $R, +, \cdot$ resp een neutraal-element of een abelse ring genoemd.*

Definitie 6.3

- *Stel R een ring, dan zijn $a, b \in R\backslash\{0\}$ nuldelers $\Leftrightarrow ab = 0$*
  Indien ze bestaan, kan men niet besluiten dat linkse/rechtse schrappingswet geldt.
- *Een ring zonder nuldelers wordt een domein genoemd*
- *Een abelse ring met eenheidselement zonder nuldelers wordt een integriteitsgebeid genoemd*

Definitie 6.4 *Stel $R, +, \cdot$ een ring, dan is een element $u \in R$ een eenheid als het het inverteerbaar element is voor de verm, dus $\Leftrightarrow \exists(unieke)\, v \in R : u \cdot v = v \cdot u = 1$*

Stelling 6.5 *De verzameling U(R) van de eenheden (inverteerbare elementen) van een ring R vormt een groep voor de (restrictie van de) vermenigvuldiging*

Stelling 6.6 *Groep $U(\mathbb{Z}_m), \cdot$ is van de orde $\varphi(m)$*
Groep $U(\mathbb{Z}_p), \cdot$ zal steeds een cyclische groep van de orde $\varphi(p) = p - 1$ zijn

6.2 Lichamen en velden

Definitie 6.7 *Een lichaam is een ring F waarvoor $U(F) = F\backslash\{0\}$ (inverse voor verm)*
Een veld is een commutatief lichaam (invers + comm voor verm)

Stelling 6.8 *(Wedderburn): Een eindig lichaam is een veld*

$\rightsquigarrow$ Formele constructie van $\mathbb{Z}$ naar $\mathbb{Q}$

6.3 Veeltermringen

Definitie 6.9 *Is $a_n = 1$ (de leidende coëfficiënt) ,*
dan spreken we van een monische veelterm of polynoom

Definitie 6.10 *De optelling en vermenigvuldiging in de veeltermring R[x] is gelijk aan die van R*

6.3.1 Veeltermringen over een veld

Stel veeltermcoëfficiënten zijn elementen van het veld $\Bbbk$

Stelling 6.11 *Stel a(x), b(x) $\in \Bbbk[x]$, dan $\exists$ unieke q(x), r(x) $\in \Bbbk[x]$*
waarvoor a(x) = b(x)q(x) + r(x), met graad r(x) < b(x) ihb als r(x) = 0

Definitie 6.12 *Stel a,b,c $\in \Bbbk[x]$ dan*
is c een ggd van a en b $\Leftrightarrow$ elke gemene deler van a en b een deler is van c

Lemma 6.13 *Stel a,b 2 ggd's van 2 elementen in $\Bbbk[x]$, dan geldt $a = u \cdot b$, met $u \in \Bbbk$*

Definitie 6.14 *De ggd van a en b is de unieke monische onder de ggd's van a en b*

$\rightsquigarrow$ Uitgebreid algoritme van Euclides voor veeltermen over $\Bbbk[x]$

Stelling 6.15 *Stel d(x) een ggd van a(x), b(x) $\in \Bbbk[x]$, dan*
$\exists \lambda(x), \mu(x) \in \Bbbk[x] : d(x)(= r_n(x)) = \lambda(x)a(x) + \mu(x)b(x)$

6.3.2 Irreducibele factoren en modulair rekenen

Definitie 6.16 *Een veelterm f(x) $\in \Bbbk[x]$ wordt irreducibel genoemd*
$\Leftrightarrow$ als f(x) = g(x)h(x) impliceert dat g(x) of h(x) $\in \Bbbk$ met f(x) $\notin \Bbbk$

Stelling 6.17 *Stel g(x),h(x) irreducibel, elke f(x) $\in \Bbbk[x]$ (nt const) kan geschreven w als*

$$f(x) = g_1(x)g_2(x)\dots g_r(x) = h_1(x)h_2(x)\dots h_s(x)$$

Bovendien is $r = s$ en $(\forall g_i(x))(\exists$ unieke $h_j(x)) : g_i(x) = \alpha_j h_j(x)$, met $\alpha_j \in \Bbbk$

Stelling 6.18 *(Factorisatiestelling): $(x - \alpha)$ is een factor van $f(x) \Leftrightarrow f(\alpha) = 0 \in \Bbbk$ Deze α's worden de wortels genoemd van de vergelijking f(x) = 0*

Stelling 6.19 *De vergelijking f(x) = 0 bezit ten hoogste zoveel wortels als de graad van f(x)*

Opmerking:

- In $\mathbb{Z}_p[x]$ is er steeds een irreducibele veelterm voor elke graad n
- Modulaire aritmetiek in de ring $\Bbbk[x]$, zie H4

Stelling 6.20 *(Hoofdstelling van de algebra):*
Elke veelterm van graad $n \geq 1$ over $\mathbb{C}$ kan ontbonden worden in precies n lineaire factoren.
Een veld waarin die eig geldt wordt algebraïsch afgesloten genoemd.

6.4 Deelvelden en veldisomorfismen

Definitie 6.21 *Stel $K, +, \cdot$ is een veld, dan is $F \subset K$ een deelveld van $K \Leftrightarrow F, +, \cdot$ is een veld*

Lemma 6.22 *Stel K een veld en $F \subset t$ K een deelveld, dan is K een F-vectorruimte*

Definitie 6.23 *Twee velden F en K zijn isomorf $\Leftrightarrow \exists$ bijectieve afbeelding $\Phi : F \to K$ zodat,*
$\Phi : F, + \to K, +$ respectievelijk $\Phi : F, \cdot \to K, \cdot$
een isomorfisme is tussen beide additieve resp multiplicatieve groepen

6.5 Eindige velden

Definitie 6.24 *De karakteristiek p van een eindig veld is de orde van de additieve deelgroep voortgebracht door 1*

Lemma 6.25 $\mathbb{k}$ *is een eindig veld* $\Leftrightarrow$ *char(*$\mathbb{k}$*) = priemgetal*

Lemma 6.26 *char(eindig* $\mathbb{k}$*) is de kleinste* $p \in \mathbb{Z}^+$ *waarvoor* $p \cdot x = 0, \forall\, x \in \mathbb{k}$

Lemma 6.27 *Een eindig veld heeft steeds orde* p^h*, p een priemgetal,* $h \geq 1$

6.5.1 Constructie van eindige velden $\mathbb{k}_{p^h}$

Toepassing 6.28 *Als h = 1, dan is het veld* $\mathbb{k}_p$ *per definitie* $\mathbb{Z}_p$

- *Vind een irreducibele veelterm f(t)* $\in \mathbb{Z}_p[t]$ *van graad h*
- *Stel* $\mathbb{k}_q$ *gelijk aan* $\{a_0 + a_1 t + a_2 t^2 + \cdots + a_{h-1} t^{h-1} || a_i \in \mathbb{Z}_p\}$
  definieer de gewone optelling en vermenigvuldiging maar nu modulo f(t)

Lemma 6.29 *Stel dat F een eindig veld is van orde* $q = p^h$
$\forall\, h \geq 1$ *bestaat er steeds een irreducibel polynoom over F van graad h*

Stelling 6.30 *Op isomorfismen na bestaat er slechts 1 veld van de orde* $q = p^h$ *met p priem,* $h \geq 1$

6.5.2 Enkele belangrijke stellingen

Stelling 6.31 *Elk element van* $\mathbb{k}^*_{2^h}$ *is een kwadraat,*
terwijl juist de helft van het aantal elementen van $\mathbb{k}^*_{p^h}$*, met* $p \neq 2$*, een kwadraat is*

Stelling 6.32 *In* $\mathbb{k}_q$*, q oneven, is -1 een kwadraat* $\Leftrightarrow q \equiv 1$ *(mod 4)*

6.5.3 Kwadratische vergelijkingen, $ax^2 + bx + c = 0$

lineaire vergelijking ax = b vormt geen moeilijkheden nl x = $a^{-1}b$

Definitie 6.33 *Als char(*$\mathbb{k}_q$*) = p oneven is, stel* $\triangle = b^2 - 4ac$

$\triangle = 0$	$\triangle \neq 0$	$\triangle = d^2$ *met* $(d \in \mathbb{k}^*_q)$
$x = -\dfrac{b}{2a}$	/	$x_{1,2} = \dfrac{-b \pm d}{2a}$

Definitie 6.34 *Als char(*$\mathbb{k}_q$*) = p = 2*
Stel b = 0, dan heeft verg $ax^2 + c = 0$ *als opl* $x = \sqrt{\frac{c}{a}}$
Stel $b \neq 0$*, vermenigvuldig de verg met* $\frac{a}{b^2}$*, stel dan* $y = \frac{ax}{b}$ *en* $\delta = \frac{ac}{b^2}$
zodat de gereduceerde verg $y^2 + y + \delta = 0$ *tevoorschijn komt. Merk op, als s opl* $\Rightarrow$ *s + 1 ook opl*
Tr(z) $= z + z^2 + z^4 + \cdots + z^{2^{h-1}}$*, dan is* $Tr(z)^2 + Tr(z) = 0, \forall\, z \in \mathbb{k}_q$
Als Tr(δ*) = 1* $\Rightarrow$ *geen oplossingen*
Als Tr(δ*) = 0* $\Rightarrow$ *2 oplossingen, nl s en s + 1 met* $k \in \mathbb{k}_q$ *: Tr(k) = 1 en*

$$s = k\delta^2 + (k + k^2)\delta^4 + \cdots + (k + k^2 + k^4 + \cdots + k^{2^{h-2}})\delta^{2^{h-1}}$$

Dit moet dan weer gesubstitueerd worden in de originele vergelijking.
Opmerking: $\mathbb{k}_q = C_0 \cup C_1$ *met* $C_{0,1} = \{t \in \mathbb{k}_q : Tr(t) = 0, 1\}$
Hierbij is $|C_0| = |C_1| = \frac{q}{2}$ *en als h oneven, dan is* $1 \in C_1$ *en kan men stellen k = 1*

7 H7 : Combinatoriek

7.1 Het principe van de dubbele telling

Definitie 7.1 *Stel $S \subset X \times Y$ met $|X| = n$ en $|Y| = m$, dan is*
$r_x(S)/k_y(S)$ het aantal koppels in S die x / y als eerste / tweede element bevatten

Stelling 7.2 $|S| = \sum_{x \in X} r_x(S) = \sum_{y \in Y} k_y(S)$

Gevolg 7.3

- $|X \times Y| = |X| \cdot |Y|$
- *Indien $r_x(S)/k_y(S)$ een constante r / k is, onafhankelijk vd keuze van $x \in X / y \in Y$, dan is*

$$r|X| = k|Y|$$

7.2 Het eenvoudig inclusie-exclusie principe

Stelling 7.4 *(Eenvoudig inclusie-exclusie principe):*

$$|A \cup B| = |A| + |B| - |A \cap B|$$

7.3 Combinatieleer

Het tellen van al dan niet geordende k-tallen (al dan niet met herhaling)

7.3.1 Variaties

Definitie 7.5 *Een variatie van n elementen in groepen van k is een geordend k-tal van k verschillende elementen gekozen uit een gegeven verzameling van n elementen*
notatie totaal aantal variaties: V_n^k of P(n, k)

Opmerking:

- k,n $\in \mathbb{N}$ en k $\leq$ n
- variaties verschillen door de opgenomen elementen en de volgorde ervan

Stelling 7.6 *Er geldt $V_n^k = n(n-1)\cdots(n-(k-1))$ $[= \frac{n!}{(n-k)!}]$*

7.3.2 Permutaties, 0! = 1

Definitie 7.7 *Een permutatie is een variatie van n elementen in groepen van n*
Twee permutaties van n elementen zijn gelijk op de volgorde na
De verzameling van alle permutaties van een verzameling met n elementen noemen we weer S_n

7.3.3 Combinaties, paren/koppels

Definitie 7.8 *Een combinatie van n elementen in groepen van k is een deelverzameling met k elementen uit een gegeven verzameling van n elementen*
notatie totaal aantal combinaties: $\binom{n}{k}$ of C(n, k), deze getallen heten binomaal-getallen/coëfficiënten

Stelling 7.9 *Er geldt $V_n^k = \binom{n}{k} \cdot k!$ $(n, k \in \mathbb{N},\ k \leq n)$*

Gevolg 7.10 $\binom{n}{k} = \frac{V_n^k}{k!} = \frac{n!}{(n-k)!k!}$

Lemma 7.11

- $\binom{n}{k} = \binom{n}{n-k}$
- $\binom{n}{k} = \binom{n}{k-1} \cdot \frac{n-k+1}{k} = \binom{n}{k+1} \cdot \frac{k+1}{n-k}$

Stelling 7.12 *(Stifel-Pascal):*
$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$

$\rightsquigarrow$ recursiviteit van binomiaalgetallen $\rightarrow$ Driehoek van Pascal (Blaise Pascal 1623-1662)

7.3.4 Herhalingsvariaties

Definitie 7.13 *Een herhalingsvariatie van n elementen in groepen van k is een geordend k-tal elementen uit een verzameling van n elementen*
notatie totaal aantal herhalingsvariaties: $\overline{V_n^k}$ *of* $\overline{P(n,k)}$

Stelling 7.14 *Er geldt* $\overline{V_n^k} = n^k$ *met k,n* $\in \mathbb{N}$

7.3.5 Herhalingscombinaties

Definitie 7.15 *Een herhalingscombinatie van n elementen in groepen van k is een niet-geordend k-tal elementen, gekozen uit een verzameling van n elelementen*
notatie totaal aantal herhcombinaties: $\overline{\binom{n}{k}}$ *of* $\overline{C(n,k)}$

Stelling 7.16 $\overline{\binom{n}{k}} = \binom{n+k-1}{k}$

Samenvatting:

	zonder terugplaatsen	*met terugplaatsen*
ongeordend	$\binom{n}{k}$	$\binom{n+k-1}{k}$
geordend	$n(n-1)\cdots(n-k+1)$	n^k

7.4 Toepassingen op combinatieleer

7.4.1 De binomiale kansverdeling

Definitie 7.17 *De binomiale kansverdeling: f(n, p, k) = B(n, p) =* $\binom{n}{k} p^k (1-p)^{n-k}$

"Wat is de kans dat we uit een verzameling van n voorwerpen waarvan er n_1 *de eigenschap p hebben en* n_2 *de eig q(:=1-p) hebben* $(n_1 + n_2 = n)$*, er juist k elementen uitnemen met de eigenschap p, waarbij het gekozen voorwerp telkens teruggeplaatst wordt.*

7.4.2 Het aantal deelverzamelingen van een verzameling

Stelling 7.18 *Een verzameling X van n elementen bezit* 2^n *deelverzamelingen*

7.4.3 Het binomium van Newton

Stelling 7.19 *Stel* $n \geq 1$*, dan geldt voor elke 2 getallen a en b*

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

7.4.4 Het veralgemeend inclusie-exclusie principe

Stelling 7.20 *(inclusie-exclusie of zeeprincipe): Als $A_1, A_2, \ldots, A_n$ eindige verzamelingen zijn*

$$|A_1 \cup A_2 \cup \cdots \cup A_n = \alpha_1 - \alpha_2 + \alpha_3 - \cdots + (-1)^{n-1}\alpha_n$$

met α_i = de som van de kardinaalgetallen van al de mogelijke doorsneden met i verzamelingen A_i

7.5 De Stirling getallen

Definitie 7.21 *Het Stirling getal S(n, k) (van de tweede soort) is per definitie het aantal mogelijkheden waarop men een verzameling X met n elementen kan schrijven als een disjuncte unie van k niet-ledige deelverzamelingen*

Stelling 7.22 *Het Stirling getal S(n, k) met $1 \leq k \leq n$ wordt recursief gedefinieerd door*

- *S(n, 1) = 1*
  S(n, k) = S(n - 1, k - 1) + kS(n - 1,k) $(2 \leq k \leq n-1)$
  S(n, n) = 1

$\rightsquigarrow$ driehoek van de Stirling getallen vd tweede soort

Gevolg 7.23 *Het aantal surjecties van een verzameling X (|X| = n) naar een verzameling Y (|Y| = k) is gelijk aan k!S(n, k)*

7.6 Multinomiaalgetallen (veralgemening binomiaalgetallen)

Definitie 7.24 *Het multinomiaalgetal is het aantal functies van $X(|X| = n)$ op $Y(|Y| = k)$, zodanig dat y_i het beeld is van n_i elementen uit X*

$$\binom{n}{n_1, n_2, \ldots, n_k} \qquad \text{Merk op dat : } \binom{n}{n_1, n_2} = \binom{n}{n_1}$$

Stelling 7.25 *Voor elke verzameling $n, n_1, \ldots, n_k \in \mathbb{N}^+$ waarvoor $\sum_{i=1}^{k} n_i = n$ is*

$$\binom{n}{n_1, n_2, \ldots, n_k} = \frac{n!}{n_1! n_2! \cdots n_k!}$$

Stelling 7.26 *(Multinomiaalstelling): Voor elke $n, k \in \mathbb{N}^+$ geldt*

$$\left(\sum_{i=1}^{k} a_i\right)^n = \sum \binom{n}{n_1, n_2 \cdots, n_k} a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k}$$

Hierbij wordt in het rechterlid de som genomen over al de mogelijke k-tallen van natuurlijke getallen $(n_1 \ldots, n_k)$ waarvoor $\sum_{i=1}^{k} n_i = n$

7.7 Enkele toepassingen in de algebra

7.7.1 De Möbiusfunctie, August Ferdinand Möbius 1790-1868

Definitie 7.27 *De Möbiusfunctie μ is een functie van $\mathbb{N}\backslash\{0\}$ naar de verz $\{-1, 0, 1\}$*

$$\mu(d) = \begin{cases} 1 & \text{als } d = 1 \\ (-1)^r & \text{als } d \text{ een product is van } r \text{ verschillende priemgetallen} \\ 0 & \text{als } d \text{ een meervoudige priemfactor bezit} \end{cases}$$

Stelling 7.28 *Voor elke $n \geq 2$ zal de som van de waarden $\mu(d)$, genomen over alle delers van n, gelijk zijn aan 0 maw $\sum_{d|n} \mu(d) = 0$*

Stelling 7.29 *(inversieregel): Stel g functie met definitiegebied* $\mathbb{N}\backslash\{0\}$*, en dat*

$$f(n) = \sum_{d|n} g(d)$$

dan kan g omgekeerd verkregen worden uit f door

$$g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})$$

Gevolg 7.30 *Aangezien* $\sum_{d|n} \varphi(d) = n$ *zal* $\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$
Ook geldt $\mu(mn) = \mu(m)\mu(n) \quad \forall(m,n) : ggd(m,n) = 1$

7.7.2 Groepen

Stelling 7.31 *Stel* $G, \cdot$ *een eindige groep van orde* $n \geq 2$*,*
volgende eigenschappen zijn gelijkwaardig

- $G, \cdot$ *is een cyclische groep*
- *Als* $d|n$*, dan bezit* $x^d = 1$ *precies d oplossingen in* $G, \cdot$
- *Als* $d|n$*, dan bezit* $G, \cdot$ *juist* $\varphi(d)$ *elementen van de orde d*

Gevolg 7.32 *Als* C_n *een cyclische groep is die voortgebracht wordt door g, dan wordt* C_n *eveneens voortgebracht door* g^k *met ggd(k, n) = 1*

7.7.3 Eindige velden

Stelling 7.33 *Indien* $\mathbb{k}_q$ *een eindig veld is met karakteristiek p,*
dan is de groep $\mathbb{k}_q^*, \cdot$ *een cyclische groep van de orde q - 1*