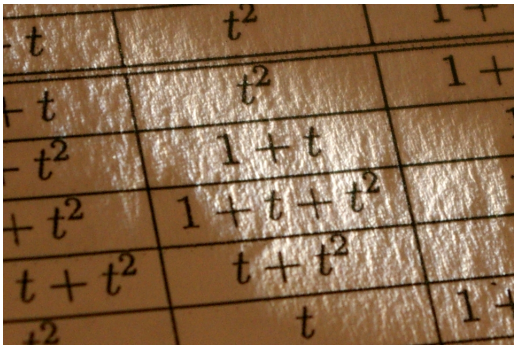
Relaties en Structuren

Frank De Clerck & An De Wispelaere

Bert Seghers
1ste bachelor in de wiskunde
Universiteit Gent



Inhoudsopgave

1 Verzamelingenleer

1.1 Basisnotaties

Verzameling (duidelijk gedefinieerde, verschillende elementen samen)
Singleton, paar, geordend paar, universum, complement
Deelverzameling: kan samenvallen met
Eigenschappen: commutatief - associatief - distributief - De Morgan

1.2 Relaties

Carthetisch product = $A \times B = \{(a,b)||a \in A, b \in B\}$
Meer dan twee verzamelingen: geordende k-tallen
Relatie is deelverzameling van productverzameling
$R_2 \circ R_1$: **na**: eerst R_1 toepassen
$(R_2 \circ R_1)^{-1} = R_1^{-1} \circ R_2^{-1}$

Classificatie van relaties

Naar definitieverzameling

- **Functie**: vertrekt maximum 1 pijl
- **Afbeelding**: vertrekt exact 1 pijl
- **Transformatie**: afbeelding van A naar A

Naar beeldverzameling

- **Injectie**ve relatie A in B: komt hoogstens 1 pijl toe
- **Surjectie**ve relatie A op B: komt minstens 1 pijl toe
- In/Sur**jectie**: in/surjectieve afbeelding
- **Bijectie** van A op B: vertrekt 1 pijl, komt 1 pijl toe (A en B gelijkmachtig)
- Bijectie van A op A: **permutatie**

Naar inhoud

- **Reflexief**: overal lussen of $(x,x) \in R \forall x$
- **Symmetrisch**: ook omgekeerde pijl of $(x,y) \in R \Rightarrow (y,x) \in R \forall x,y$
- **Transitief**: ook samenstelling of $(x,y) \wedge (y,z) \in R \Rightarrow (x,z) \in R \forall x,y,z$

Equivalentierelatie: reflexief, symmetrisch, transitief
Partitie, equivalentieklasse met representant
X gepartitioneerd in $A_1, A_2, ...A_n \Leftrightarrow$
$A_1 \cup A_2 \cup ... \cup A_n = X \wedge A_1 \dot\cup A_2 \dot\cup ... \dot\cup A_n = \varnothing$
Orderelatie: reflexief, antisymmetrisch, transitief

1.3 Getallenverzamelingen en axioma van goede ordening

$\exists \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ met de gekende eigenschappen
Het axioma van de goede ordening:

Als X een nietledige deelverzameling van $\mathbb{Z}$ is met een ondergrens, dan heeft ze een kleinste element.

1.4 Recursieve definities

Recursieve rijvoorschriften definieren u_n voor alle n (bewijs adhv axioma uit ongerijmde).
Als je een recursieve ook absoluut kan schrijven is die ook bepaald voor alle n.

1.5 Inductie

Bewijs met volledige inductie: bewijs voor $k = 1$ en $P(k) \Rightarrow P(k+1)$.
Stelling: Inductiebewijzen zijn geldig, of: Stel $S \subset \mathbb{N}*$ en:

- $1 \in S$
- Voor alle $k \in \mathbb{N}*$ geldt: $k \in S \Rightarrow k+1 \in S$

dan is $S = \mathbb{N}*$. (+Bewijs)

1.6 Ladenprincipe van Dirichlet

Als m objecten moeten verdeeld worden over n laden ($m > n$) dan is er minstens één lade met meer dan één object.

1.7 Eindige en oneindige verzamelingen

X = eindig $\Leftrightarrow$ er is een bijectie tussen $\mathbb{N}[1, n]$ en X
en oneindig $\Leftrightarrow$ niet eindig.
Stelling: Een niet-ledige verzameling X is oneindig $\Leftrightarrow \exists$ injectie van $\mathbb{N}*$ naar X. (+Bewijs)
Aftelbaarheid van verzamelingen (bijectie met $\mathbb{N}$)
Aftelbaarheid van $\mathbb{Q}$: (+Bewijs met niveaus)
Niet-aftelbaarheid van $\mathbb{R}$: (+Bewijs met cijfers na de komma)

Kardinaalgetallen

Voor eindige verzamelingen: Kardinaalgetal = aantal elementen
Voor aftelbare oneindige: Kardinaalgetal = $\aleph_0$.

1.8 Vereenvoudigd somprincipe

Aantal elementen van unie van disjuncte verzamelingen is som van elementen van respectieve verzamelingen.
Vandaar algemeen ladenprincipe: m objecten over n laden ($m > nr$) $\Rightarrow$ minimum één lade met meer dan r objecten.

2 Logica

3 Telprincipes

3.1 Principe van de dubbele telling

Om kardinaalgetal K van relatie $X \to Y$ te bepalen: K = aantal met $x \in X$ als eerste element = aantal met $y \in Y$ als tweede element. Oefeningen zoals $\mathbb{N}[1, 8]$ met 6 deelverzamelingen

3.2 Eenvoudig inclusie-exclusie principe

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

3.3 Combinatieleer

Variaties	V_n^k	$\frac{n!}{(n-k)!}$
Permutaties	V_n^n	$n!$
Combinaties	C_n^k of $\binom{n}{k}$	$\frac{n!}{(n-k)!k!}$
Herhalingsvariaties	$\bar{V}_n^k$	n^k
Herhalingscombinaties	$\bar{C}_n^k$	$\binom{n+k-1}{k}$

$+\Delta$ van Pascal met bewijs eigenschap Stifel-Pascal

3.4 Toepassingen

Aantal mogelijkheden om n bollen te kiezen waarvan k rode, uit a rode en b blauwe = $\binom{n}{k} a^k b^{n-k}$
Kans = $\frac{1}{(a+b)^n} \binom{n}{k} a^k b^{n-k}$

- **Binomiale kansverdeling** = $\binom{n}{k} p^k q^{n-k}$ met $p + q = 1$
- **Aantal deelverz van een verzameling** ($|K| = n$) is 2^n (+Bewijs)
- **Binomium van Newton** (+Bewijs)

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

- **Veralgemeend inclusie-exclusie principe**

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

met α_i = som van alle mogelijke doorsneden van i verzamelingen. (+Bewijs!)

- **Wanordes**
  Wanorde is een permutatie van een verzameling (bv. $\mathbb{N}[1,n]$) zonder fixelementen.
  Aantal mogelijke wanordes voor $\mathbb{N}[1,n]$:

$$d_n = n! - \alpha_1 + \alpha_2 - \ldots + (-1)^n \alpha_n$$

  dus alle mogelijke permutaties ($n!$) - (permutaties die 1 element fixeren - degene die er 2 fixeren + ...). Hierbij is

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

$$\text{dus} \quad d_n = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \ldots + (-1)^n \frac{1}{n!}\right)$$

  De recursieve formule hiervoor: (+ Bewijs)

$$d_n = (n-1)(d_{n-1} + d_{n-2})$$

3.5 Stirling getallen

Stirling getal $S(n,k)$ = aantal mogelijkheden om een partitie van k niet-ledige deelverzamelingen te maken uit een verzameling van n elementen.
Recursief: $S(n,k) = S(n-1,k-1) + kS(n-1,k)$ (+Bewijs)
Gevolg: # Surjecties van een verzameling met n elementen naar een met k elementen is $k!S(n,k)$.

3.6 Multinomiaalgetallen

Aantal functies van verzameling X met n elementen op verzameling Y met k elementen waarbij ieder element y_i juist het beeld is van n_i elementen van X.

$$\binom{n}{n_1, n_2, \ldots, n_k} = \frac{n!}{n_1! n_2! \ldots n_k!} \qquad (+\text{Bewijs})$$

Multinomiaalstelling

$$(a_1 + a_2 + \ldots + a_k)^n = \sum \binom{n}{n_1, n_2, \cdots, n_k} a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k} \qquad (+\text{Bewijs})$$

4 Getaltheorie

4.1 Basisbegrippen

Deelbaarheid

$$a|b \Leftrightarrow \exists q \in \mathbb{Z} : b = a \cdot q$$

$$\forall a \in \mathbb{N}, b \in \mathbb{Z} : \exists! q, r \in \mathbb{Z} : \quad b = a \cdot q + r \quad \text{met r} \in \mathbb{N}[0, a-1] \quad (+\text{Bewijs})$$

Priemgetallen

Stelling van Euclides: er zijn er oneindig veel. (+Bewijs)

Ontbinden in priemfactoren

Elk getal is te schrijven als een product van priemfactoren (+Bewijs)
Zeef van Eratosthenes

4.2 GGD en KGV

Uitleg **Algoritme van Euclides**
Stelling: Er bestaan gehele m en n zodat $am + bn = ggd(a, b)$. (+Bewijs)
$p | \prod_{i=1}^{n} x_i \quad \Rightarrow \quad p$ deler van ten minste 1 x. (+Bewijs)
Ontbinding in priemfactoren uniek op volgorde na. (+Bewijs)
Elke rationale oplossing van de vergelijking met gehele coëfficiënten

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0$$

is van de vorm p/q met p deler van a_0 en q deler van a_n. Als a_n 1 is, zijn de oplossingen geheel. (+Bewijs)

4.3 De Euler functie

$\Phi(n)$ is aantal natuurlijke getallen lager dan n die onderling ondeelbaar zijn met n.

$$\Phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}) \quad \text{(+Bewijs)}$$

$$\sum_{d|n} \Phi(d) = n \quad \text{(+Bewijs)}$$

4.4 De Mobius functie

$$\mu(d) = \begin{cases} 1 & \text{als} \quad d = 1 \\ (-1)^r & \text{als} \quad d \; r \text{ verschillende priemfactoren heeft} \\ 0 & \text{als} \quad d \text{ een meervoudige priemfactor heeft} \end{cases}$$

$$n \geqslant 2 \Rightarrow \quad \sum_{d|n} \mu(d) = 0 \quad \text{(+Bewijs)}$$

$$f(n) = \sum_{d|n} g(d) \quad \Rightarrow \quad g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d}). \text{ (+Bewijs)}$$

$$\text{Vanzelfsprekend:} \quad \Phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$$

5 Modulorekenen

5.1 Congruenties

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

congruent modulo m is equivalentierelatie met m restklassen
Som en product van congruente getallen is op zich congruent $mod\ m$.

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

Definitie van $+$ $(\oplus)$ en $\times(\otimes)$. Inwendig, commut, assoc, neutr el, distrib, invers el voor de optelling.
Nuldelers! Schrappingswet niet altijd!

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

$$r \text{is de inverse van } x \text{ als } rx \equiv 1 \quad \text{Notatie} : r^{-1}$$

Stelling: Een element r is inverteerbaar modulo $m \Leftrightarrow ggd(r, m) = 1$ (+Bewijs)
Stelling van Euler: $ggd(y, m) = 1 \Rightarrow y^{\Phi(m)} \equiv 1(mod\ m)$ (+ Bewijs)

5.4 Lineaire congruenties

$ax \equiv b\ (mod\ m) \Rightarrow$ zoeken naar $(x, t) \quad ax = b + mt$. Aantal oplossingen:

$ggd(a, m) = 1$	$ggd(a, m) = d$	
$\downarrow$	d deelt b	d deelt b niet
$x = a^{-1}b$	$a'x \equiv b'(mod\ m')$	Geen oplossingen
	d oplossingen in $\mathbb{Z}_m$	

Toepassing: Diofantische vergelijkingen

5.5 Stelling van Wilson

Stelling van Wilson: $(p-1)! \equiv 1$ voor p priem (+Bewijs)
Stelling: $\exists a \in \mathbb{Z}_p : \ a^2 \equiv -1(mod\ p) \Leftrightarrow p \equiv 1 \pmod 4$ (+Bewijs)

5.6 Stelsels lineaire congruenties

Op te lossen met substitutie en parameters k_1, k_2, k_3. Beter: Chinese reststelling.
Chinese reststelling: Het stelsel van k lineaire congruenties

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

met $ggd(m_i, m_j) = 1$, bezit juist 1 oplossing modulo $M = \prod_{i=1}^{k} m_i$. (+Bewijs)
Praktische techniek: zoeken en invullen van y_i in

$$\begin{cases} x \equiv \sum_{i=1}^{k} b_i \cdot y_i \cdot \dfrac{\prod_{j=1}^{k} m_j}{m_i} \end{cases}$$

$$\begin{cases} \dfrac{\prod_{j=1}^{k} m_j}{m_i} \equiv \mathbf{1} \ (mod\ m_i) \end{cases}$$

5.7 Primitieve wortels

$a \in \mathbb{Z}_0, \quad m \in \mathbb{N}_0, \quad ggd(a, m) = 1.$
$\{s \in \mathbb{N} | a^s \equiv 1 \ (mod\ m)\}$ niet ledig, vanwege Euler: $a^{\Phi(m)} \equiv 1 \ (mod\ m)$.
Kleinste element, stel t, waarvoor $a^t \equiv 1 \ (mod\ m)$ = **orde** van a modulo m.
Als $t = \Phi(m)$, dus maximale orde, dan is t een **primitieve wortel** van a modulo m.
Stelling: a heeft orde t modulo m, $ggd(a, m) = 1$. $a^n \equiv 1 \ (mod\ m) \Leftrightarrow n$ veelvoud van t. (+Bewijs)
Gevolg: Orde t altijd deler van $\Phi(m)$. $a^r \equiv a^s \ (mod\ m) \Leftrightarrow r \equiv s \ (mod\ t)$.
Stelling: g prim wortel van $m \Rightarrow$ resten mod m van $g, g^2, \ldots, g^{\Phi(m)}$ zijn DE $\Phi(m)$ getallen uit $\mathbb{N}[1, m-1]$ die copriem zijn met m. (+Bewijs)
Stelling: a heeft orde t mod $m \Rightarrow$ a^k ook orde $t \Leftrightarrow ggd(k, t) = 1$. (+Bewijs)

5.8 Kwadratische congruenties

p is vanaf hier een oneven priemgetal.

$$ax^2 + bx + c \equiv 0 \ (mod\ p)$$

$$\rightarrow x^2 + a^{-1}bx + a^{-1}c \equiv 0 \ (mod\ p)$$

$$\leftrightarrow (x + \frac{a^{-1}b}{2})^2 \equiv \frac{b^2 - 4ac}{4a^2} \quad (mod\ p)$$

$$y^2 \equiv \frac{\delta}{4a^2} \ (mod\ p) \quad \textit{Is delta een kwadraat?}$$

$$\Rightarrow \text{Congruenties van de vorm } \mathbf{x^2 \equiv a \ (mod\ p)}$$

Heeft oplossing $\Rightarrow a$ is kwadratische rest modulo p
Heeft geen oplossing $\Rightarrow a$ is kwadratische niet-rest modulo p.
Stelling: $a \not\equiv 0 \ (mod\ p) \Rightarrow x^2 \equiv a \ (mod\ p)$ heeft juist 2 of geen oplossingen. (+Bewijs) De helft van de getallen uit $\mathbb{N}[1, p-1]$ komt dus $2\times$ voor als oplossing modulo p, de andere helft komt niet voor.

$a^{\Phi(p)} = a^{p-1} \equiv 1 \ (mod\ p)$, zodat $a^{\frac{p-1}{2}} \equiv \pm 1 \ (mod\ p)$.

Stelling, Criterium van Euler: p oneven priemgetal en $p \mid\mid a \Rightarrow x^2 \equiv a \ (mod\ p)$ heeft 2 oplossingen als $a^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$ en geen oplossingen als $a^{\frac{p-1}{2}} \equiv -1 \ (mod\ p)$ (+Bewijs)

Legendre symbool

Hulpmiddel om $a^{\frac{p-1}{2}}$ niet altijd te moeten uitrekenen:

$$\left[\begin{array}{c} a \\ p \end{array} \right] = \left\{ \begin{array}{rl} 1 & \text{als } a \text{ een kwadratische rest is modulo } p \\ -1 & \text{als } a \text{ geen kwadratische rest is modulo } p \end{array} \right\} = a^{\frac{p-1}{2}}$$

- $a \equiv b \ (mod\ p) \Rightarrow \left[\begin{array}{c} a \\ p \end{array} \right] = \left[\begin{array}{c} b \\ p \end{array} \right]$
- $\left[\begin{array}{c} a^2 \\ p \end{array} \right] = 1$
- $\left[\begin{array}{c} ab \\ p \end{array} \right] = \left[\begin{array}{c} a \\ p \end{array} \right] \cdot \left[\begin{array}{c} b \\ p \end{array} \right]$.
- $\left[\begin{array}{c} p \\ q \end{array} \right] = \left[\begin{array}{c} q \\ p \end{array} \right]$, behalve als $p \equiv q \equiv 3 \ (mod\ 4)$, dan is $\left[\begin{array}{c} p \\ q \end{array} \right] = - \left[\begin{array}{c} q \\ p \end{array} \right]$

6 Groepentheorie

6.1 Definities

Verzameling + bewerking = **structuur** (bv G, f). f beeldt twee elementen van G af op een nieuw element van G, of $f : V \times V \to V; (a, b) \to f(a, b) = a + b = ab$.
Groep = structuur met 3 voorwaarden:
ASSOCIATIEF, EENHEIDSELEMENT e en $\forall a$: INVERS element a^{-1}
Orde van groep: aantal elementen in verzameling. Notatie: $|G|$.
Voorbeelden: $\mathbb{Z}, + \quad \mathbb{Q}, + \quad \mathbb{R}, + \quad \mathbb{C}, + \quad \mathbb{Q}_0, \cdot \quad \mathbb{C}_0, \cdot \quad \mathbb{R}_0, \cdot$
$K_4 \quad \mathbb{Z}_m, \oplus \quad \mathbb{Z}_p \setminus \{0\}, \otimes \quad GL(n, \mathbb{C}), \cdot \quad S_n$
De symmetrische groep S_n bevat (de samenstelling van) alle permutaties van n objecten en heeft dus $n!$ elementen. Bijvoorbeeld S_3: de symmetrieën van een gelijkz Δ.
Eigenschapjes: Linkse en rechtse schrappingswet.
Unieke oplossing voor $xa = b$, nl. ba^{-1}. Voor $ax = b : a^{-1}b$.
Latijns vierkant: (Bewerkings)tabel met in elke rij en kolom $1\times$ ieder element. Niet ieder Latijns vierkant is een geldige Cayleytabel voor een groep, omgekeerd wel.

6.2 Groepmorfismen

Stel groepen $G, \cdot$ en $G', \star$. θ is (homo)morfisme $\Leftrightarrow \theta(a \cdot b) = \theta(a) \star \theta(b) \forall a, b \in G$. Injectief: **monomorfisme**. Surjectief: **epimorfisme**. Bijectief: **iso-**

morfisme. Isomorfisme op zelfde verzameling: **automorfisme**.

6.3 Deelgroepen

Stel G, f een groep. G' is een deelverzameling van G en f' de restrictie van f tot $G' \times G'$. Als G', f' een groep is, dan is dit een **deelgroep**. Deelgroep $\neq \{e\}, \neq G, f$: **Eigenlijke deelgroep**. Notatie *is deelgroep van"*: $<, \leqslant$.
Voorbeelden van deelgroepen: $\mathbb{Z}, + < \mathbb{Q}, + < \mathbb{R}, + < \mathbb{C}, +$ – $\mathbb{Q}_0, \cdot < \mathbb{R}_0, \cdot < \mathbb{C}_0, \cdot$ – $\{e, a\}, \{e, b\}$ en $\{e, c\} < K_4$ – $\{e, \rho, \rho^2\} < S_3$ – $SL(n, \mathbb{C}), \cdot$ met $\det = 1 < GL(n, \mathbb{C}), \cdot$
Doorsnede deelgroepen = deelgroep; unie meestal niet.
Stel θ morfisme $G, \cdot \to G', \star$.
$\theta(G), \star$ is deelgroep van $G', \star$ = beeld = $\mathrm{Im}(\theta)$. $\theta^{-1}(e'), \cdot = \{z \in G | \theta(z) = e'\}, \cdot$ is deelgroep van $G, \cdot$ = kern = $\ker(\theta)$.

6.4 Nevenklassen van een deelgroep

H deelgroep $\Rightarrow aH = \{ah | h \in H\}$ en Ha zijn de linkse en rechtse nevenklassen van H in G.
Stelling: De nevenklassen van H in G vormen een partitie van G. (+Bewijs)
Stelling van Lagrange: H deelgroep van eindige groep $G \Rightarrow |H|$ deelt $|G|$. (+Bewijs)
Index van H in $G = \frac{|G|}{|H|} = [G : H]$.

6.5 Cyclische groepen

Cyclische groep: Als groep element g bevat zodanig dat elk element kan geschreven worden als een macht van g. (g is voortbrengend element; $\langle g \rangle = G$)
Oneindige cyclische groepen (C_∞) en eindige (C_m).
Eindige: $\exists m \in \mathbb{N}_0 : x^m = e$. Stel m: kleinste m waarvoor dit geldt. $\forall k = mq + r$ en $k > m : x^k = x^r,\ r \in \mathbb{N}[0, m-1]$.

$$\langle x \rangle = \{e, x, x^2, \ldots, x^{m-1}\} \qquad |x| = m$$

Stel G willekeurige groep. $x \in G \Rightarrow \langle x \rangle < G$ en is cyclisch. Orde van cyclische groep $\langle x \rangle$ is **orde** van element x. Lagrange $\Rightarrow$ orde van element altijd deler van orde van groep.
Stelling: Elke eindige cyclische groep van orde m is isomorf met $\mathbb{Z}_m, \oplus$. Elke oneindige met $\mathbb{Z}, +$ (+Bewijs)
Toepassingen: Elke eindige groep, orde priem, is cyclisch.
Er bestaan juist 2 groepen van orde 4: K_4 en $Z_4, \oplus$.
Stelling: Stel $G, \cdot$ een eindige groep van orde $n \geqslant 2$. Volgende zijn equivalent: (+Bewijs)

- $G, \cdot$ cyclisch.
- $d|n \Rightarrow x^d = 1$ heeft d oplossingen in $G, \cdot$
- $d|n \Rightarrow G, \cdot$ heeft juist $\Phi(d)$ elementen van orde d.

Stelling: $C_n = \langle g \rangle$ heeft voor elke deler d van n een deelgroep van orde d. Dit is de cyclische groep voortgebracht door $g^{\frac{n}{d}}$. (+Bewijs)

6.6 Direct product van groepen

$A, \star$ en $B, \circ$ groepen. Bewerking $\cdot$ op $A \times B$:

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \star a_2, b_1 \circ b_2)$$

$A \times B, \cdot$ is een groep, orde $|A| \cdot |B|$, direct of carthesisch product.
Voorbeeld: $C_2 \times C_3 \cong C_6; C_2 \times C_2 \cong K_4$, niet cyclisch!
Stelling: $ggd(m, n) = 1 \Rightarrow C_m \times C_n \cong C_{m \cdot n}$ (+Bewijs)

6.7 Elementair abelse groepen

Elementair abelse groep = eindige, commutatieve groep, orde $\neq 1$, zodat elk element dezelfde orde p heeft.
Lagrange: p is een deler van de orde n. p is altijd een priemgetal, want anders bestaat er voor elke deler d van p een deelgroep C_d, voortgebracht door $x^{\frac{p}{d}}$. We nemen G' cyclische deelgroep van G ($\cong \mathbb{Z}_p$). Indien $G \backslash G' \neq \varnothing$, bestaat er een element van $G \backslash G'$, dat weer een deelgroep G'' voortbrengt ($\cong \mathbb{Z}_p$). Het direct product $G' \times G''$ heeft orde p^2 en is isomorf met een deelgroep van G. Indien de rest nog altijd niet ledig, bestaat er een element dat G''' zal voortbrengen en $G' \times G'' \times G'''$ is dan isomorf met een deelgroep van orde p^3. Na een eindig aantal stappen is de hele groep G geconstrueerd. Elke elementair abelse groep G is dus isomorf met het direct product van h cyclische groepen van orde p en is de orde van G altijd p^h.

6.8 Permutatiegroepen

S_n: groep van alle permutaties van verz met n elementen, van $\mathbb{N}[1, n]$. Elke deelgroep van S_n is een **permutatiegroep**. Een element van een permutatiegroep is een permutatie, een f, die een bijectie is van $\mathbb{N}[1, n]$ op zichzelf. Voorbeeld:

$$f(1) = 2, f(2) = 4, f(3) = 5, f(4) = 2, f(5) = 3 \qquad \text{of} \qquad f = (124)(35)$$

Bij cykelvoorstelling kan men cykels met lengte 1, dus fixelementen weglaten als de verzameling waarover gepermuteerd wordt duidelijk is. Samenstelling met $\circ$: uitvoeren van rechts naar links.

Even en oneven permutaties

Transpositie: permutatie die 2 elementen van plaats wisselt en de rest fixeert. Men kan iedere permutatie herschrijven als combinatie van transposities of van andere permutaties, maar telkens ligt de pariteit vast: het aantal cykels is altijd even, ofwel oneven.
Stelling: 1 permutatie is te schrijven in r en r' transposities $\Rightarrow$ r en r' zijn beide even of beide oneven. (+Bewijs)
Samenstelling van twee even of oneven permutaties: terug even. Permutaties zijn in te delen in de partitie even - oneven permutaties. De even vormen een deelgroep en de oneven de nevenklasse voor S_n, beide met orde $\frac{n!}{2}$. De deelgroep der even permutaties is $\mathrm{Alt}(n)$ of A_n, de alternerende groep.
Sign-afbeelding: het epimorfisme $S_n, \circ \to \{1, -1\}, \cdot$ die de oneven permutaties afbeeldt op -1 en A_n op 1.

7 Ringen, lichamen en velden

7.1 Ringen

Ring: verzameling R met twee bewerkingen in vaste volgorde, notatie $R, +, \cdot$

$$R, +, \cdot \text{ is een ring} \Leftrightarrow \begin{cases} R, + \text{ is een abelse groep} \begin{cases} \text{Associatief} \\ \text{Neutraal element } 0 \\ \text{Invers element} \\ \text{Commutatief} \end{cases} \\ R\backslash\{0\}, \cdot \text{ associatief} \\ \text{distributiviteit van } \cdot \text{ t.o.v. } + . \end{cases}$$

$$\left.\begin{array}{l} \exists \text{ ring met eenheidselement} \\ \exists \text{ commutatieve ring} \\ \text{Ringen kunnen nuldelers hebben} \end{array}\right\} \begin{array}{l} \text{Een commutatieve ring met} \\ \text{eenheidselement zonder nulde-} \\ \text{lers is een } \textbf{integriteitsgebied}. \end{array}$$

Voorbeelden van integriteitsgebieden: $\mathbb{Q}, +, \cdot \quad \mathbb{R}, +, \cdot \quad \mathbb{C}, +, \cdot$
Voorbeelden van andere ringen: $\mathbb{Z}_m, \oplus, \otimes \quad \mathbb{R}^{n\times n}, +, \cdot$

Inverteerbare elementen in een ring

Analoge definitie als in $\mathbb{Z}_m$. Ring R, notatie $U(R)$ voor de verzameling van alle inverteerbare elementen uit de ring R.
Stelling: $U(R), \cdot$ is een groep (+Bewijs).
$\Rightarrow |U(\mathbb{Z}_m), \cdot| = \Phi(m)$ want invert. $\Leftrightarrow ggd(r, m) = 1$

7.2 Lichamen en velden

Lichaam: waar $U(F) = F^*$. Alles is inverteerbaar, er is een invers element.
Veld: commutatief lichaam.
Een eindig integriteitsgebied is noodzakelijk een lichaam en dus een veld.

Voorbeeld van een oneindig lichaam dat geen veld is: de Quaternionen (Hamilton).

7.3 Veeltermringen

$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ is een veelterm of polynoom waarin a_i de coëfficiënten zijn en x een onbepaalde variabele is (onbelangrijk, ook wel $(a_0, a_1, \ldots, a_n)$.
$R[x]$ is de verzameling van alle veeltermen in de onbepaalde variabele x, waarbij de coëfficiënten $\in R$. $R_3[x]$: graad ten hoogste 3.
Er wordt een optelling en vermenigvuldiging gedefinieerd. De coëfficiënten kunnen $\in \mathbb{Z}_m$ zijn, waardoor bv. $3x \cdot 2x^2 = 0$ in $\mathbb{Z}_6$.
Delingsalgoritme: Voor gegeven $a(x)$ en $b(x)$ bestaan er $q(x)$ en $r(x)$ waarvoor $a(x) = b(x)q(x) + r(x)$ met gr $r(x) <$ gr $b(x)$.
Analoog met natuurlijke getallen worden delers (*factoren*) gedefinieerd, en een *ggd*. $\exists \lambda(x), \mu(x) : \quad \lambda(x)a(x) + \mu(x)b(x) = ggd\,(a(x), b(x))$. Algoritme van Euclides levert die $\lambda(x)$ en $\mu(x)$.
Reduceren (= ontbinden in irreduciebele factoren) is niet eenvoudig. Best zoeken naar lineaire factoren $(x - \alpha)$ door α in te vullen en nul te bekomen. Hogeregraadsfactoren met methode van onbepaalde coëfficiënten.

7.4 Eindige velden of Galoisvelden

Stel je $\mathbb{Z}_p[x]$ voor met p = karakteristiek, orde van de additieve deelgroep $\langle 1 \rangle$ en dus kleinste waarde waarvoor $p \cdot x = 0$ (additief). Uiteraard priem.
Freshmen dream: kar $p \Rightarrow (a + b)^p = a^p + b^p$. (+Bewijs) $\mathbb{F}_q$ eindig veld met $q = p^h$.
Stelling: $\mathbb{F}_q$ eindig veld kar $p \Rightarrow \mathbb{F}_q, +$ elementair abelse groep van orde $q = p^h$ en $\mathbb{F}_q^*$ cyclische groep van orde $q - 1$. (+Bewijs)

Visualisatie en primitieve wortels

- $\mathbb{F}_8 = GF(8) \cong (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2), + = \{(a_0, a_1, a_2) | a_i \in \mathbb{Z}_2\}$
  De elementen uit dit eindig veld zijn van de vorm $(1, 0, 1)$ of $1t^2 + 0t + 1$ en zijn gemakkelijk op te tellen en iets trager te vermenigvuldigen.
- $\mathbb{F}_8^* = GF(8) \backslash 0 \cong C_7$, dus $\exists \alpha : C_7 = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7 = 1\}$.
  De elementen uit dit veld zijn dezelfde als in dat hierboven, maar anders geschreven. Ze zijn gemakkelijk te vermenigvuldigen maar moeilijk op te tellen. α heeft de orde $q - 1$ en is een primitief element. Alle α^k zijn ook primitief element $\Leftrightarrow$ ggd$(k, q - 1) = 1$. Zo bestaan er dus $\Phi(q - 1)$ primitieve elementen. Merk op: α is prim wortel van $\mathbb{Z}_m \Leftrightarrow$ orde van $\alpha = \Phi(m)$ of $m - 1$ als m priem.
- Primitieve elementen zijn niet gemakkelijk te vinden in een eindig veld.

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

Vind een irreduc veelterm $f(t)$ van graad h.
Stel $\mathbb{F}_q$ gelijk aan $\{(a_0 + a_1t + a_2t^2 + \ldots + a_{h-1}t^{h-1})|a_i \in \mathbb{Z}_p\}$ en definieer de voor de hand liggende optelling en normale vermenigvuldiging, maar *modulo* de irreduc veelterm. t of $(0, 1, 0, 0, \cdots)$ is niet altijd een primitief element. Als $f(t)$ zo gekozen dat t wel primitief is, dan is $f(t)$ een **primitieve irreduciebele veelterm**.

Voorbeelden van eindige velden

In de cursus Cayleytabellen van $\mathbb{F}_4, \mathbb{F}_8, \mathbb{F}_9$. Stel als oefening de tabel op voor $\mathbb{F}_{25}, \mathbb{F}_{27}$ of $\mathbb{F}_{32}$.

De Zech-logtabel

Het is moeilijk om met de (a_0, a_1, a_{h-1})-notatie te vermenigvuldigen en nog veel moeilijker om met de $\alpha, \alpha^2, \ldots$-notatie op te tellen. Het wordt daarentegen heel simpel als je de functie kent die een bepaalde macht van α afbeeldt op de α-macht van het element bekomen door 1 op te tellen bij het vertrekelement. $(i \mapsto j \Leftrightarrow \alpha^j = \alpha^i + 1)$. Eenmaal al dit werk geleverd is, is optellen simpel.
Stelling: In $\mathbb{F}_q$ is -1 een kwadraat $\Leftrightarrow q \equiv 1 \bmod 4$. (+Bewijs)

Oplossen van vergelijkingen

Lineaire vgl: simpel, mbv inverse.
Kwadratische: hoogstens 2 opl

Oneven kar: zoals in $\mathbb{R}$, bepaal $\Delta = b^2 - 4ac \rightarrow \begin{cases} \Delta = 0 & \Rightarrow 1 \text{ opl } -\frac{b}{2a} \\ \Delta \neq \square & \Rightarrow \nexists \text{ opl} \\ \Delta = d^2 & \Rightarrow 2 \text{ opl } \frac{-b \pm d}{2a} \end{cases}$

Kwadratische vergelijkingen in even kar, $\mathbb{F}_{2^h}$

$$ax^2 + bx + c = 0$$

Hierin zijn a, b en $c \neq 0$ (waarom?)
Vermenigvuldig de vgl met $\frac{a}{b^2}$ zodat $\frac{a^2x^2}{b^2} + \frac{ax}{b} + \frac{ac}{b^2} = 0$. Dit is evenwaardig met $y^2 + y + \delta = 0$ als $y = \frac{ax}{b}$ en $\delta = \frac{ac}{b^2}$. Merk op, als s opl $\Rightarrow s + 1$ ook opl.

$$\mathrm{Tr}(z) = z + z^2 + z^4 + \ldots + z^{2^{h-1}}$$

$\mathrm{Tr}^2(z) + \mathrm{Tr}(z) = 0 \quad$ en $\quad \mathrm{Tr}(\delta) = 0$ of 1.
Als $\mathrm{Tr}(\delta) = 1 \Rightarrow$ geen oplossingen.

Als $\mathrm{Tr}(\delta) = 0 \Rightarrow$ 2 oplossingen, namelijk s en $s+1$, met $k \in \mathbb{F}_q | \mathrm{Tr}(k) = 1$, en

$$s = k\delta^2 + (k + k^2)\delta^4 + (k + k^2 + k^4 +)\delta^8 + \ldots + (k + \ldots + k^{2^{h-2}})\delta^{2^{h-1}}$$

Invullen met aandacht voor $\mathrm{Tr}(\delta) = 0$ en $\mathrm{Tr}(k) = 1$ leert dat s een oplossing is. Omgekeerd, als s een oplossing is, en dus $s^2 + s = \delta$, dan is $\mathrm{Tr}(s^2 + s) = 0$. Het is duidelijk dat Tr een partitie maakt in de elementen van $\mathbb{F}_q$: C_0 en C_1.
Als $q = 2^{2m+1}$, dan $1 \in C_1$, en voor k kan je 1 kiezen.

Samenvatting

$ax^2 + bx + c = 0$ heeft 2 oplossingen $\Leftrightarrow \mathrm{Tr}(\frac{ac}{b^2}) = 0$.